Cómo hacer demostraciones

Lic. Ramiro Choque C.

April 5, 2007

Contenido

1 Introducción **2**

2 Elementos de un problema por demostrar **2**
2.1 Hipótesis y tesis 2
2.2 Interpretación simbólica 3

3 Demostración **4**
3.1 Vacuidad 4
3.2 Trivial 5
3.3 Directa 5
3.4 Contrarrecíproca 6
3.5 Bicondicional 7
3.6 Contradicción 8
3.7 Casos: $p \vee q \Rightarrow r$ 9
3.8 $p \Rightarrow q \vee r$ 9

4 Demostraciones cuantificadas **10**
4.1 Movimiento de cuantificadores 10
4.2 Existenciales 11
4.2.1 Pruebas constructivas 11
4.2.2 Pruebas no constructivas 11
4.3 Existencia y unicidad 12
4.4 Contraejemplos 12
4.5 Reducción del radio de acción 13
4.6 Especificación universal 14

4.7 Inducción Matemática 15
4.8 Prueba empleando razonamiento regresivo 16

1 Introducción

En Matemática esencialmente existen dos tipos de problemas a saber, problemas por resolver y problemas por demostrar. Las demostraciones están asociadas a los problemas por demostrar. Una demostración es un proceso con el cual justificamos una cierta afirmación. Por ello uno debe poder leer, entender y escribir demostraciones. Para poder realizar demostraciones se debe aplicar razonamiento natural basado en la lógica, principios y algunas técnicas llamados "métodos de demostración".

Lo que se demuestra son afirmaciones en una cierta teoría que tiene principios (axiomas, definiciones, teoremas, etc.)

2 Elementos de un problema por demostrar

Los objetos con los que procesamos en los problemas por demostrar son las afirmaciones, enunciados o proposiciones. Lo que se desea establecer es que cierta afirmación P es válida es una cierta teoría mediante razonamientos válidos. Si se logra este hecho, decimos que el enunciado P es un *teorema*, y a la sucesión de razonamientos que se realiza para establecer P, es llamado *demostración*, la sucesión mencionada es utilizando la regla de inferencia *Modus Ponens*, que la forma estandar, natural y directo de razonar. La proposición P esencialmente es de la forma simple p, o bien compuesta $p \wedge q$, $p \vee q$, $p \Rightarrow q$, $p \Leftrightarrow q$, que a excepción de la primera, las otras se pueden expresar como una implicación. En efecto, $p \vee q \equiv \sim p \Rightarrow q$, $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$.

Todo problema por demostrar se expresa en términos de hipótesis y tesis o conclusión, y esto son llamados elementos de un problema por demostrar.

2.1 Hipótesis y tesis

Si tenemos un enunciado P relativa a una teoría, la hipótesis de P es todo lo que se ha establecido previamente a P. El enunciado P es la tesis del problema, y en general, es lo que queremos demostrar, y cuando se logre esto será un *teorema*, esto es, un teorema es una afirmación que posee una

demostración. Cuando estamos inmerso en una teoría y construimos una afirmación el cual se mantiene como cierta y se utiliza sin demostración, lo llamaremos una *conjetura*.

Veamos algunos ejemplos donde el objetivo es identificar la hipótesis y la tesis.

Teorema 1. $1 > 0$

¿Cuál es la hipótesis? ¿Cuál es la tesis?

La hipótesis a este teorema es toda la teoría desarrollada de los números reales que antecede. Lo que se debe demostrar es que teniendo los resultados previos como hipótesis concluir que $1 > 0$.

2.2 Interpretación simbólica

Muchos afirmaciones están en lenguaje usual, ellas para ser demostrados deben ser si es necesario expresados en forma simbólica. Además la forma simbólica ayuda a identificar el método de prueba que se puede emplear.

Observe el siguiente teorema en $\mathbb{R}$

Ejemplo 1. El cuadrado de un entero impar es impar.

Ahora simbolizaremos. El enunciado significa que,

$$\text{si } n \text{ es entero impar, entonces } n^2 \text{ es impar.}$$

que también podemos escribir en la forma

$$\begin{gathered}\text{Hipótesis: } n = 2k - 1, \text{ con } k \in \mathbb{Z} \\ \text{Tesis: } n^2 = 2k' - 1, \text{ con } k \in \mathbb{Z}\end{gathered}$$

3 Demostración

3.1 Vacuidad

Si se desea establecer que un enunciado de la forma $p \Rightarrow q$, es un teorema, entonces debemos recordar los valores de verdad de una implicación. Una implicación es falso si tiene antecedente verdadero y consecuente falso, en otro caso es siempre verdadero. Las pruebas de implicaciones se clasifica como sigue: Sea $\mathbb{F}$ un enunciado falso y $\mathbb{V}$ un enunciado verdadero. Nótese que $\mathbb{F} \Rightarrow q$ y $p \Rightarrow \mathbb{V}$ son proposiciones tautológicas.

Si presentamos una demostración de la forma $\mathbb{F} \Rightarrow q$, decimos que es una *prueba por vacuidad*, para ello lo único que hay que establecer es el antecedente falso.

Teorema 2. $\emptyset \subset A$.

Prueba. Como $x \in \emptyset \Rightarrow x \in A$, es cierto por vacuidad, entonces por definición de inclusión de conjuntos, $\emptyset \subset A$. ∎

Nota 1. Es útil conocer lo siguientes

1. $(\forall \varphi(x))\, P(x) = \forall x : \varphi(x) \Rightarrow P(x)$
2. $(\exists \varphi(x))\, P(x) = \exists x : \varphi(x) \wedge P(x)$

Por ejemplo

$$\forall \varepsilon > 0 : |a| < \varepsilon \quad \equiv \quad \forall \varepsilon : \varepsilon > 0 \Rightarrow |a| < \varepsilon.$$

Y

$$\exists x < 0 : x^3 + x < 1 \quad \equiv \quad \exists x : x < 0 \wedge x^3 + x < 1.$$

En los números reales

Teorema 3. El conjunto vació es un conjunto acotado

Prueba. Sea M un número positivo. $\forall x \in \emptyset : |x| \leq M$ es cierto por vacuidad, entonces el conjunto vacío $\emptyset$, es un conjunto acotada. ∎

3.2 Trivial

Si presentamos una demostración de la forma $p \Rightarrow \mathbb{V}$, decimos que es una *demostración trivial*. Para dar una prueba trivial lo único que hay que establecer es que el consecuente es verdadero.

Teorema 4. Límite de la función constante es la misma constante, esto es, $\lim_{x \to a} b = b$.

Prueba. Sea $\varepsilon > 0$ (suponemos verdadero), entonces como

$$0 < |x - a| < \delta \Rightarrow \underbrace{|b - b| < \varepsilon}_{\mathbb{V}}$$

es cierto trivialmente, entonces por definición de límite, $\lim_{x \to a} b = b$ ∎

3.3 Directa

Se presentamos una demostración en la forma $p \Rightarrow q$, estableciendo que si p es cierto, entonces razonado se sigue que q es cierto, o bien establecemos la verdad de q con la *hipótesis auxiliar* q como cierto, entonces decimos que hemos realizado una *demostración directa*. Así podemos dar dos demostraciones directas.

(1) Partimos de la hipótesis p, razonamos, hasta establecer la tesis, entonces decimos que es una *demostración directa*.

(2) Si establecemos q con la ayuda de la hipótesis p, es también una *demostración directa*.

Observación 1. Aclaramos el denominativo "hipótesis auxiliar"

Teorema. En $\mathbb{Z}$, si k^2 es un entero impar, entonces k es impar.

- *Hipótesis*: de esta afirmación es toda la teoría previamente desarrollada de los números enteros.
- *Hipótesis auxiliar*: k^2 es un entero impar
- *Tesis*: k es impar.
- En las demostraciones directas la *hipótesis del problema*, es la hipótesis y la hipótesis auxiliar.

Ahora presentamos las dos formas de realizar demostraciones directas.

Teorema 5. En $\mathbb{R}$, si $a + c = b + c$, entonces $a = b$.

Prueba. (1) Si $a + c = b + c$, entonces

$$(a + c) + (-c) = (b + c) + (-c)$$

ello por identidad (es como escribir $a = a$). Por asociatividad

$$a + (c + (-c)) = b + (c + (-c))$$

por la propiedad del inverso aditivo (que es axioma)

$$a + 0 = b + 0$$

y por la propiedad del neutro aditivo

$$a = b$$

∎

Prueba. (2)

$$\begin{array}{rcll} a & = & a + 0 & \text{Neutro aditivo} \\ & = & a + (c + (-c)) & \text{Inverso aditivo} \\ & = & (a + c) + (-c) & \text{Asociatividad} \\ & = & (b + c) + (-c) & \text{Hipótesis "auxiliar"} \\ & = & b + (c + (-c)) & \text{Asociatividad} \\ & = & b + 0 & \text{Inverso aditivo} \\ & = & b & \text{Neutro aditivo} \end{array}$$

∎

3.4 Contrarrecíproca

Como $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$ es una tautología, en lugar de probar $p \Rightarrow q$ podemos probar $\sim q \Rightarrow \sim p$ que es la contrarrecíproca de $p \Rightarrow q$. Cuando hacemos esto decimos que estamos realizando una *prueba por contrarrecíproca.*

En muchos problemas, esta es la alternativa adecuada, veamos esto con algunos ejemplos.

Teorema 6. Si n^2 es un entero par, entonces n es un entero par.

Prueba. Realizamos la prueba empleando la contrarrecíproca que también es una implicación. Hipótesis: n no es un entero par, Tesis: n^2 no es un entero par.

Si n no es un entero par, entonces (ahora empleamos razonamiento usual), n es impar, luego $n = 2k + 1$, con $k \in \mathbb{Z}$ ello por definición de entero impar. Al cuadrado

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k + 2) + 1 = 2k' + 1$$

donde $k' = 2k + 2$ es un entero. Teniendo $n^2 = 2k' + 1$, concluimos que n^2 no es entero par. ∎

Observación 2. Si en el teorema anterior, empleamos demostración directa, tendremos

$$n^2 = 2k.$$

Ahora lo que se nos puede ocurrir es $n = \sqrt{2k}$, con ello no podemos asegurar que es un número entero, mucho menos que es par.

3.5 Bicondicional

Como $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$, entonces para demostrar $p \Leftrightarrow q$ es suficiente demostrar que $p \Rightarrow q$ y $q \Rightarrow p$. Así para demostrar un teorema donde la conectiva es la bicondicional, "si, y sólo si", se debe demostrar dos implicaciones, la implicación directa ("si") $p \Rightarrow q$ y la recíproca ("sólo si") $q \Rightarrow p$. También decimos que "q es una condición necesaria para p" (q debe ocurrir necesariamente si p ocurre) y que "q es una condición suficiente para p".

Teorema 7. En $\mathbb{Z}$, n es un entero par si y solo si n^2 es par.

Prueba. ($p \Rightarrow q$) Si n es un entero par, entonces $n = 2k$, con k un entero. Su cuadrado es $n^2 = 4k^2 = 2(2k^2)$ que es par.

($q \Rightarrow p$) Ver la prueba del teorema 6 ∎

3.6 Contradicción

Sea $\mathbb{F}$ una afirmación falsa en un cierto ámbito, decimos también que es una contradicción. Por ejemplo $1 < 0$, 2 es impar, n es entero par y n es entero impar, $n^2 + 1 < 0$, etc. son contradicciones en $\mathbb{Z}$. Enunciados de la forma $p \wedge \sim p$ son ejemplos de contradicciones. Si p es falso, entonces $\sim p$ es verdadero. Por ejemplo, $1 < 0$ es falso, entonces $\sim (1 < 0) \equiv 1 \geq 0$ es verdadero.

Supongamos que deseamos demostrar la proposición p. Como

$$(\sim p \Rightarrow \mathbb{F}) \Rightarrow p$$

es una tautología, entonces para demostrar p es suficiente demostrar

$$\sim p \Rightarrow \mathbb{F}.$$

Es decir, para probar p es suficiente demostrar que de la negación de lo que se quiere demostrar, se deduce una contradicción (afirmación falsa)

Teorema 8. No existe un número racional a tal que $a^2 = 2$.

Prueba. Por contradicción. Supongamos que existe un número racional $a = \dfrac{p}{q}$ tal que $a^2 = 2$. Podemos simplificar la fracción y podemos suponer que $\dfrac{p}{q}$ es una fracción simplificada. Luego

$$\left(\frac{p}{q}\right)^2 = 2$$

entonces

$$p^2 = 2q^2 \tag{1}$$

es par. Por el teorema 6, se deduce que p es par, entonces $p = 2k$, para algún k entero. Reemplazando en (1), tendremos $(2k)^2 = 2q^2$, de donde $q^2 = 2k^2$ es par, luego q es par. Así la fracción $\dfrac{p}{q}$ no está simplificada ($\Rightarrow\Leftarrow$), que contradice a la suposición de que estaba simplificada. ∎

3.7 Casos: $p \vee q \Rightarrow r$

Considerando la tautología $p \vee q \Rightarrow r \equiv \underbrace{(p \Rightarrow r)}_{\text{caso I}} \wedge \underbrace{(q \Rightarrow r)}_{\text{caso II}}$, se deduce que para demostrar un enunciado de la forma $p \vee q \Rightarrow r$ es suficiente analizar dos casos. Hacemos notar que si ocurre que $p \Rightarrow \mathbb{F}$ cierto, entonces p tiene que ser falso, luego el problema se reduce a demostrar que $q \Rightarrow r$. Así, si en la prueba de uno de los casos obtenemos una contradicción, podemos olvidarnos de él y consideramos los casos que faltan.

Ejemplo 2. En $\mathbb{R}$, definamos $a * b = \max(a, b)$. Demostrar que esta operación es asociativa. Esto es $(a * b) * c = a * (b * c)$.

Prueba. Por ley de tricotomía para a,b y c (expresando dos de ellos, luego con el tercero)

ocurre las siguientes posibilidades: $a \leq b \leq c$, $a \leq c \leq b$, $c \leq a \leq b$, $b \leq a \leq c$, $b \leq c \leq a$ ó $c \leq b \leq a$. p.d. $(a * b) * c = a * (b * c)$

Caso I :Si $a \leq b \leq c$, entonces

$$(a * b) * c \quad = \quad b * c \quad = \quad c \quad \text{y} \quad a * (b * c) \quad = \quad a * c \quad = \quad c$$

luego $(a * b) * c = a * (b * c)$.

Caso II : Si $a \leq c \leq b$, entonces

$$(a * b) * c \quad = \quad b * c \quad = \quad b \quad \text{y} \quad a * (b * c) \quad = \quad a * b \quad = \quad b$$

luego $(a * b) * c = a * (b * c)$.

Los otros cuatro casos son análogos.

∎

3.8 $p \Rightarrow q \vee r$

Si tenemos mas hipótesis, tendremos mas argumentos con que demostrar, así es aceptable considerar la tautología

$$p \Rightarrow q \vee r \equiv p \wedge \sim q \Rightarrow r$$

Luego para demostrar $p \Rightarrow q \vee r$, incorporamos $\sim q$ como hipótesis, y probamos r a partir de p y $\sim q$.

Ejemplo 3. En $\mathbb{R}$, demostrar que si $ab = 0 \Rightarrow a = 0$ ó $b = 0$

Prueba. Si $ab = 0$ y $a \neq 0$, entonces existe a^{-1} y multiplicando a $ab = 0$, obtenemos $a^{-1}(ab) = a^{-1}0$, por asociatividad $(a^{-1}a)\,b = a^{-1}0$. Por la propiedad del inverso multiplicativo y el hecho de que cualquier número multiplicado por cero es cero, resulta $1 \cdot b = 0$, como 1 es neutro, entonces $b = 0$. ∎

4 Demostraciones cuantificadas

4.1 Movimiento de cuantificadores

Si el universo $U = \{x_1, \ldots, x_n\}$ es finito y $P(x)$ y $Q(x)$ son predicados, definimos

(1) $\forall x : P(x) \equiv P(x_1) \wedge \cdots \wedge P(x_n)$,

(2) $\exists x : P(x) \equiv P(x_1) \vee \cdots \vee P(x_n)$.

Luego un enunciado cuantificado universalmente es cierto si para cada $x \in U$, $P(x)$ es cierto, una proposición cuantificada existencialmente es cierto si es cierto $P(x)$ para al menos un $x \in U$. Este mismo principio vale para el caso infinito.

En este ámbito es fácil demostrar

1. $\forall x : Q(y) \equiv Q(y)$, donde se supone que x no figura en $Q(y)$.
2. $\sim \forall x : P(x) \equiv \exists x : \sim P(x)$,
3. $\sim \exists x : P(x) \equiv \forall x : \sim P(x)$,
4. $\forall x : P(y) \wedge Q(x) \equiv P(y) \wedge \forall x : Q(x)$,
5. $\exists x : P(y) \vee Q(x) \equiv P(y) \vee \exists x : Q(x)$,
6. $\forall x : P(x) \wedge Q(x) \equiv \forall x : P(x) \wedge \forall x : Q(x)$,
7. $\exists x : P(x) \vee Q(x) \equiv \exists x : P(x) \vee \exists x : Q(x)$,

Observación 3. No es posible demostrar que $\exists x : P(x) \wedge Q(x) \equiv \exists x : P(x) \wedge \exists x : Q(x)$, y no es dificil demostrar que

$$\exists x : P(x) \wedge Q(x) \Rightarrow \exists x : P(x) \wedge \exists x : Q(x)$$

Una observación análoga para el cuantificador universal, pero con la disyunción.

4.2 Existenciales

Las demostraciones de afirmaciones de la forma $\exists x : P(x)$ son llamados pruebas de existencia o demostraciones existenciales. Son de dos tipos, *constructivos* y *no constructivos*.

4.2.1 Pruebas constructivas

Dar una *prueba constructiva de existencia* del enunciado $\exists x : P(x)$ es establecer la afirmación exhibiendo una valor c tal que $P(c)$ es verdadera. Algunas veces, en vez de exhibir un valor específico c, una prueba constructiva de existencia especifica un algoritmo para obtener tal valor.

Ejemplo 4. En $\mathbb{R}$, demostrar que si $a < b$, entonces $\exists c \in \mathbb{R}^+$: $b = a + c$.

Prueba. Proporcionamos una demostración constructiva.

Como $a < b$, entonces $b - a > 0$. Sea $c = b - a \in \mathbb{R}^+$, y tenemos $b = a + c$. ∎

4.2.2 Pruebas no constructivas

Una prueba no constructiva de existencia establece la afirmación $\exists x : P(x)$ sin indicar cómo encontrar el valor c tal que $P(c)$ es cierta. Tal prueba más comúnmente involucra una prueba por contradicción o puede resultar de aplicar un teorema de existencia no constructiva.

Una prueba constructiva de existencia especifica un elemento, mientras que una prueba no constructiva no provee información de como hallar algún elemento y sólo da una afirmación de existencia. Algunos resultados en las matemáticas caen entre estos dos extremos. Demostraciones de existencia constructivas son común en análisis numérico.

En el ejemplo que sigue aplicamos el siguiente teorema.

Teorema 9. (de valor intermedio) Si $f : [a, b] \to \mathbb{R}$ es continua y k está entre $f(a)$ y $f(b)$ entonces $\exists c \in]a, b[$ tal que $f(c) = k$.

Ejemplo 5. Demostrar que la ecuación $x^3 + x + 1 = 0$ tiene una raíz.

Prueba. Proporcionamos una demostración no constructiva.

Sea $f(x) = x^3 + x + 1$. Todo polinomio es continuo. Como $f(0) = 1$, y $f(-1) = -1$, tenemos que $f(-1) < 0 < f(0)$, luego 0 es esta entre $f(-1)$ y $f(0)$. Por el teorema de valor intermedio, existe un número $c \in]-1, 0[$ tal que $f(c) = 0$, esto es $c^3 + c + 1 = 0$, de donde c es una raíz de la ecuación dada. ∎

Observación 4. Nótese que en este ejemplo no indicamos como encontrar el número c, por ello la demostración hecha es una prueba no constructiva de existencia.

4.3 Existencia y unicidad

Si demostramos la existencia de cierto valor, la pregunta inmediata es si es única. Para probar que un valor a es único que verifica el enunciado $P(x)$, se debe verificar

$$P(a) \wedge P(b) \Rightarrow a = b$$

Ejemplo 6. Probar que el conjunto vacío es único.

Sean $\emptyset$ y $\emptyset'$ son conjuntos vacíos. p.d. $\emptyset = \emptyset'$

Como $\emptyset$ es vacío, y $\emptyset'$ es conjunto, entonces como el vacío es subconjunto de cualquier conjunto, resulta $\emptyset \subset \emptyset'$. Ahora $\emptyset'$ es conjunto vacío, entonces $\emptyset' \subset \emptyset$. Luego $\emptyset = \emptyset'$

4.4 Contraejemplos

Las afirmaciones de la forma $\forall x : P(x)$, suele incorporar universo y cuantificador universal implícitos. Por ejemplo, en $\mathbb{R}$

Teorema 10. $a^2 \geq 0$

el universo y cuantificar son implícitos. El teorema expresa en realidad

$$\forall a \in \mathbb{R}\colon\ a^2 \geq 0.$$

Si presentamos un enunciado de la forma $\forall x : P(x)$, la pregunta es ¿es demostrable? Si se presenta una prueba será un teorema, luego será un

enunciado verdadero. Si afirmamos que no es demostrable, entonces estamos afirmando que $\forall x : P(x)$ es falso. Luego debemos demostrar su negación que será una prueba de existencia que puede ser constructiva o no. Si damos una prueba constructiva de existencia, debemos encontrar un valor c tal que $p(c)$ es falso. Cuando realizamos esto decimos que hemos hecho una *prueba por contraejemplo* y que el valor c es *contraejemplo de* $\forall x : P(x)$.

Este tipo de problemas suelen presentarse cuando analizamos un teorema de la forma $\forall x : P(x) \Rightarrow Q(x)$, y la pregunta suele ser, si la recíproca, $\forall x : Q(x) \Rightarrow P(x)$, es cierto. Entonces podemos presentar una demostración, en ese caso se constituirá en un teorema, o podemos dar un contraejemplo, en este caso debemos encontrar un valor c tal que $Q(c) \Rightarrow P(c)$ es falso.

Teorema 11. En $\mathbb{R}$, si $a > b$ y $b > c$, entonces $a > c$.

¿La recíproca de este teorema es cierto?

Solución. No. Para ello proporcionaremos un contraejemplo, encontrando valores de a,b y c para los que la recíproca es falso. Como $2 > 1 \Rightarrow 2 > 3$ y $3 > 1$ es falso. Entonces la recíproca no se verifica.

4.5 Reducción del radio de acción

En algunos problemas es necesario reducir el radio de acción de un cuantificador. El siguiente enunciado es útil

$$\forall x : P(x) \Rightarrow Q(y) \equiv (\forall x : P(x)) \Rightarrow Q(y) \qquad (*)$$

que es fácil verificar en el caso de universo finito, que también es válida en el caso no finito. En el primer miembro de la equivalencia (*), el radio de acción del cuantificador es $P(x) \Rightarrow Q(y)$, en cambio en el segundo miembro es $P(x)$. Así el radio de acción del cuantificador es mas pequeño en el segundo miembro de la equivalencia (*). Lo que (*) afirma es que si el consecuente esta libre de la variable cuantificada universalmente, su radio de acción se reduce al antecedente.

Ejemplo 7. En teoría de conjuntos, en el problema por demostrar

$$B \subset A \Rightarrow B = \emptyset.$$

¿Cuál es la hipótesis?

Como A y B son variables, en realidad, debemos demostrar que

$$\forall B\ \forall A : B \subset A \Rightarrow B = \emptyset.$$

Este es un enunciado como (*), como A no figura en el consecuente entonces la hipótesis es $\forall A : B \subset A$, que es una hipótesis mas significativo que tomar como hipótesis $B \subset A$.

Ejemplo 8. En $\mathbb{R}$, en el enunciado

$$\forall \varepsilon > 0 : |a| < \varepsilon \Rightarrow a = 0,$$

la hipótesis es $\forall \varepsilon > 0 : |a| < \varepsilon$, pues el consecuente $a = 0$ esta libre de ε.

En cambio en el enunciado $\forall \varepsilon > 0 : |a| < \varepsilon \Rightarrow \varepsilon^2 + a^2 \geq 2\varepsilon a$, la hipótesis es $|a| < \varepsilon$, y no podemos asumir como hipótesis $\forall \varepsilon > 0 : |a| < \varepsilon$, pues el consecuente no esta libre de ε.

4.6 Especificación universal

Si $\forall x : P(x)$ es cierto, entonces para un valor c del universo, será cierto $p(c)$. Este proceso es llamado *especificación o particularización universal.* Justamente este tipo de argumento suele ser útil en algunas demostraciones.

Ejemplo 9. En teoría de conjuntos, demostrar que $\forall A$: $B \subset A \Rightarrow B = \emptyset$.

Prueba. Analizando el alcance del cuantificador universal, notamos que la hipótesis es $\forall A$: $B \subset A$. Luego por especificación podemos tomar $A = \emptyset$, entonces tendremos $B \subset \emptyset$, pero esto implica que $B = \emptyset$. ∎

Ejemplo 10. En $\mathbb{R}$, demostrar que $\forall \varepsilon > 0 : |a| < \varepsilon \Rightarrow a = 0$.

Prueba. Observando el radio de acción del cuantificador universal, notamos que en el consecuente de la implicación no figura ε, luego su alcance es el antecedente. Así la hipótesis es $\forall \varepsilon > 0 : |a| < \varepsilon$. Queremos demostrar que $a = 0$. Procedemos por contradicción, Supongamos que $a \neq 0$, entonces $\varepsilon = \dfrac{|a|}{2} > 0$. Por especificación universal, concluimos que $|a| < \dfrac{|a|}{2}$. De donde $1 < \dfrac{1}{2}$ que es una contradicción. ∎

4.7 Inducción Matemática

Si el universo es finito es fácil demostrar que $\forall x : P(x)$ es cierto, puede ser resuelto por casos,

$$\forall x : P(x) = \underbrace{P(x_1)}_{\text{caso I}} \wedge \underbrace{P(x_2)}_{\text{caso II}} \wedge \cdots \wedge \underbrace{P(x_n)}_{\text{caso n}}$$

No podemos hacer lo mismo en el caso infinito. El caso infinito numerable, como $\mathbb{N}$, es posible explicar un método de prueba, veamos esto. Sea el problema de demostrar

$$\forall n \in \mathbb{N} : P(n)$$

que es equivalente a probar

$$P(1) \wedge P(2) \wedge P(3) \wedge \cdots$$

Lo usual seria probar, $P(1)$, ¿que falta demostrar?, $P(2)$, y una vez hecho esto, probar $P(3)$, etc. Podemos llegar a establecer digamos hasta $P(k)$ ¿Qué falta probar?, falta probar el siguiente, $P(k+1)$.

El método de inducción matemática expresa este hecho

Teorema 12. (Inducción Matemática) Sea $P(n)$ un enunciado que depende de $n \in \mathbb{N}$.

Si $P(1)$ es cierto y $\forall k \in \mathbb{N} : P(k) \Rightarrow P(k+1)$, entonces $\forall n \in \mathbb{N} : P(n)$ es cierto.

$P(k)$ es llamado *hipótesis de inducción.*

Ejemplo 11. En $\mathbb{R}$, demostrar que, si $0 < a < b$, entonces $\forall n \in \mathbb{N} : a^n < b^n$

Prueba. Supongamos que $0 < a < b$. p.d. $\forall n \in \mathbb{N} : a^n < b^n$. (*)

Como el enunciado que queremos demostrar depende de los números naturales, aplicamos inducción matemática, para ello sólo debemos probar dos resultados.

(1) (*) se verifica para $n = 1$. En efecto, como $0 < a < b$, entonces $a^1 = a < b = b^1$.

(2) Asumimos hipótesis de inducción. Supongamos que el enunciado (*) es cierto para $n = k$. Por demostrar que se verifica para $n = k + 1$.

Por hipótesis de inducción $a^k < b^k$. Entonces

$$a^{k+1} = a^k a < b^k a < b^k b = b^{k+1}$$

∎

Observación 5. ¿La recíproca del ejemplo anterior es cierto?, es decir $\forall n \in \mathbb{N} : a^n < b^n \Rightarrow 0 < a < b$, es cierto ?
No, un contraejemplo es

$$2^2 < (-3)^2 \Rightarrow 0 < 2 < -3$$

Ejemplo 12. En $\mathbb{R}$, demostrar que $\forall m \in \mathbb{N}, \forall n \in \mathbb{N} : a^m \cdot a^n = a^{m+n}$.

Prueba. Sea $m \in \mathbb{N}$, p.d. $\forall n \in \mathbb{N} : a^m \cdot a^n = a^{m+n}$.
Aplicamos inducción matemática. Recuerde la definición de exponente: $a^1 = a$, $a^n = a^{n-1}a$.

(1) $a^m \cdot a^1 = a^m a = a^{m+1}$, ello por definición de exponente.

(2) Hipótesis de inducción (H.I.) $a^m \cdot a^k = a^{m+k}$. p.d. $a^m \cdot a^{k+1} = a^{m+k+1}$.

Por definición de exponente,

$$a^m \cdot a^{k+1} = a^m \cdot a^k a = \left(a^m \cdot a^k\right) a \overset{\text{H.I.}}{=} a^{m+k} a = a^{m+k+1}.$$

∎

4.8 Prueba empleando razonamiento regresivo

Un proceso que ayuda a identificar lo que se desea demostrar es analizar la tesis o conclusión del problema por demostrar. El análisis de la tesis aproxima la hipótesis y la tesis, resulta ser un razonamiento regresivo. Luego presentar este razonamiento regresivo como prueba de la afirmación que desea demostrar no es correcto, puede resultar ser prueba de la recíproca. Así el razonamiento regresivo debe ser elemento aclaratorio de la tesis, y no la demostración del enunciado dando. Nosotros expresaremos el razonamiento regresivo mediante la abreviatura p.d., *por demostrar*, con color diferente

Ejemplo 13. Demostrar que $a^2 + b^2 \geq 2ab$.

Prueba. Lo que debemos demostrar es $a^2 + b^2 \geq 2ab$
esto es equivalente a demostrar $a^2 + b^2 - 2ab \geq 0$
esto es, p.d. $(a - b)^2 \geq 0$.
El número reales, el cuadrado de todo número es no negativo, entonces

$$(a - b)^2 \geq 0.$$

Desarrollando el binomio, resulta

$$a^2 + b^2 - 2ab \geq 0$$

sumando $2ab$, llegamos a estableces que

$$a^2 + b^2 \geq 2ab$$

∎

Observación 6. ¿Que de malo tiene la siguiente prueba del anterior ejemplo?

Prueba. Tenemos $a^2 + b^2 \geq 2ab$, sumando $-2ab$, obtenemos

$$a^2 + b^2 - 2ab \geq 0$$

el primer miembro es cuadrado de un binomio, luego

$$(a - b)^2 \geq 0.$$

que es siempre cierto, con lo cual queda demostrado. ∎

Lo que en realidad se ha demostrado es:

$$a^2 + b^2 \geq 2ab \Rightarrow (a - b)^2 \geq 0.$$

Y no se ha establecido la verdad de $a^2+b^2 \geq 2ab$. Por ello esta demostración no es válida.

Ejemplo 14. Demostrar que $\lim_{x\to\infty} x^n = \infty$, $\forall n \in \mathbb{N}$.

Prueba. Sea $n \in N$. p.d. $\forall \varepsilon > 0\ \exists \delta > 0 : x > \delta \Rightarrow x^n > \varepsilon$

Sea $\varepsilon > 0$ y $\delta = \max(1, \delta_1)$, donde $\boxed{\delta_1 = \varepsilon}$ (que es investigado según lo que se quiera obtener en la tesis). Si $x > \delta$, p.d. $x^n > \varepsilon$

entonces por transitividad $x > 1$ y $x > \delta_1$ (*)

Entonces, observando la tesis, debemos construir x^n. Como es $x > 1$, por el ejemplo 11, $x^{n-1} \geq 1$, Multiplicando por x, resulta

$$x^n > x$$

Transitividad con (*), $x^n > \delta_1 = \varepsilon$. ∎

References

[1] Ralph P. Grimaldi, Matemática Discreta y Combinatoria, tercera edición.

[2] Patrick Suppes, Teoría Axiomática de Conjuntos, ed. Norma, 1968

[3] Armando Rojo (1981), Algebra, Ed. El Ateneo.

[4] http://fsc729.ifreepages.com/proofs.html