Métodos de demostración

IIC1253 - Matemáticas Discretas
Clase 06

Prof. Fernando Florenzano Hernández
faflorenzano@ing.puc.cl

¿Qué es una demostración?

Definición

Una **demostración** es un argumento válido
para establecer la verdad de una **afirmación matemática**.

¿Qué **afirmaciones matemáticas** conocen?

Afirmaciones matemáticas

Ejemplos

1. Todo número natural cumple que
   si es par, entonces su sucesor es impar.

$$\forall x.\ x \text{ es par} \to \text{el sucesor de } x \text{ es impar}$$

2. Todo número natural cumple que
   es par si, y solo si, el número al cuadrado es par.

$$\forall x.\ x \text{ es par} \leftrightarrow x^2 \text{ es par}$$

3. Existe una cantidad infinita de números primos.

?

afirmación matemática $\approx$ proposición en lógica de predicados

Tipos de afirmaciones matemáticas

- Definición.
- Axioma.
- Proposición.
- Lema.
- Teorema.
- Corolario.
- Conjetura.
- Problema abierto.

¿Qué es una demostración?

Definición

Una **demostración** es un argumento válido
para establecer la verdad de un **afirmación matemática**.

Un argumento válido es
una **secuencia de argumentos** que puede estar compuesta por:

- axiomas.
- aplicación de definiciones.
- hipótesis o supuestos (si existe).
- afirmaciones previamente demostradas.

Cada argumento en la secuencia de argumentos esta conectado con el anterior por una **regla de inferencia** (consecuencia lógica).

El **último paso** de la secuencia establece la verdad de la afirmación.

¿Qué NO es una demostración?

- Una secuencia de símbolos.
- Una secuencia disconexa de argumentos.

IMPORTANTE

La secuencia de argumentos debe ser lo más **clara**, **precisa** y **completa** posible de tal manera de **convencer** al lector u oyente sin dejarle ninguna duda sobre la correctitud de la demostración.

¿Cómo comenzar a escribir una demostración?

Una demostración **debe** seguir un **orden** lógico de argumentos.

Pero, a la hora de **escribir** la demostración, es difícil hacerlo en ese mismo orden.

Es recomendable que comiencen escribiendo el **inicio** de la demostraciones (las **hipótesis**) y sus **definiciones**. Así tendrán claro con que pueden partir.

Inmediatamente después escriban el **fin** de la demostración (el **objetivo** a demostrar) y sus **definiciones**. Así tendrán claro a dónde tienen que llegar.

Luego, **rellenen**.

Ejemplo

Sea Σ un conjunto de fórmulas proposicionales y α una fórmnula proposicional. Demuestre:

$$\text{Si } \Sigma \cup \{\neg\alpha\} \text{ es inconsistente, entonces } \Sigma \vDash \alpha$$

Ejemplo demostración

(Hip.) Si $\Sigma \cup \{\neg\alpha\}$ es inconsistente

(Def.) Entonces no existe valuación $v_1, \ldots, v_n$ tal que haga verdadero a todas las fórmulas en $\Sigma \cup \{\neg\alpha\}$.

(Objetivo.) $\Sigma \vDash \alpha$

Ejemplo demostración

(Hip.) Si $\Sigma \cup \{\neg\alpha\}$ es inconsistente

(Def.) Entonces no existe valuación $v_1, \ldots, v_n$ tal que haga verdadero a todas las fórmulas en $\Sigma \cup \{\neg\alpha\}$.

(Def. de Obj.) Para toda valuación que hace verdad a las fórmulas de Σ, entonces esa valuación hace verdad a α.

(Objetivo.) $\Sigma \models \alpha$

Ejemplo demostración

(Hip.) Si $\Sigma \cup \{\neg\alpha\}$ es inconsistente

(Def.) Entonces no existe valuación $v_1, \ldots, v_n$ tal que haga verdadero a todas las fórmulas en $\Sigma \cup \{\neg\alpha\}$.

(Arg.) Es decir, para **cualquier** valuación, hay al menos una fórmula en $\Sigma \cup \{\neg\alpha\}$ que evalua a **falso**.

(Def. de Obj.) Para toda valuación que hace verdad a las fórmulas de Σ, entonces esa valuación hace verdad a α.

(Objetivo.) $\Sigma \vDash \alpha$

Ejemplo demostración

(Hip.) Si $\Sigma \cup \{\neg\alpha\}$ es inconsistente

(Def.) Entonces no existe valuación $v_1, \ldots, v_n$ tal que haga verdadero a todas las fórmulas en $\Sigma \cup \{\neg\alpha\}$.

(Arg.) Es decir, para **cualquier** valuación, hay al menos una fórmula en $\Sigma \cup \{\neg\alpha\}$ que evalua a **falso**.

(Arg.) Suponga que una valuación $v'_1, \ldots, v'_n$ hace verdad solo a las fórmulas de Σ. Sabemos que si agregamos $\neg\alpha$ al conjunto, se dejan de cumplir todas las fórmulas.

(Def. de Obj.) Para toda valuación que hace verdad a las fórmulas de Σ, entonces esa valuación hace verdad a α.

(Objetivo.) $\Sigma \vDash \alpha$

Ejemplo demostración

(Hip.) Si $\Sigma \cup \{\neg\alpha\}$ es inconsistente

(Def.) Entonces no existe valuación $v_1, \ldots, v_n$ tal que haga verdadero a todas las formulas en $\Sigma \cup \{\neg\alpha\}$.

(Arg.) Es decir, para **cualquier** valuación, hay al menos una fórmula en $\Sigma \cup \{\neg\alpha\}$ que evalua a **falso**.

(Arg.) Suponga que una valuación $v'_1, \ldots, v'_n$ hace verdad solo a las fórmulas de Σ. Sabemos que si agregamos $\neg\alpha$ al conjunto, se dejan de cumplir todas las fórmulas.

(Arg.) Entonces $(\neg\alpha)(v'_1, \ldots, v'_n) = 0$. Es decir, $\alpha(v'_1, \ldots, v'_n) = 1$.

(Def. de Obj.) Para toda valuación que hace verdad a las fórmulas de Σ, entonces esa valuación hace verdad a α.

(Objetivo.) $\Sigma \vDash \alpha$

¿Cómo encontramos una secuencia de argumentos para demostrar un teorema?

1. Experiencia.
2. Intuición.
3. Creatividad.
4. Perseverancia.
5. **Métodos de demostración**.

Contenidos

Contenidos

Demostración directa

Supongan que queremos demostrar una afirmación como:

$$\forall x.\, P(x) \rightarrow Q(x)$$

Método directo

Suponemos que $P(n)$ es verdadero para un n **cualquiera** (genérico) y demostramos que $Q(n)$ también es verdadero.

¿Qué sucede cuando $P(n)$ es **falso**?

Ejemplo de una demostración directa

Definición

- Un entero n en $\mathbb{Z}$ se dice **par** si existe k en $\mathbb{Z}$ tal que $n = 2k$.
- Un entero n en $\mathbb{Z}$ se dice **impar** si existe k en $\mathbb{Z}$ tal que $n = 2k + 1$.

Teorema

Si n es un entero impar, entonces n^2 es impar.

Demostración

Suponemos que n es impar.
Por definición, existe un $k \in \mathbb{Z}$ tal que $n = 2k + 1$.

$$\begin{aligned} n^2 &= (2k+1)^2 && \text{(definición de } n\text{)} \\ &= 4k^2 + 4k + 1 && \text{(multiplicación } (2k+1)(2k+1)\text{)} \\ &= 2 \cdot (2k^2 + 2k) + 1 && \text{(factorización por 2)} \end{aligned}$$

Si definimos k' como $k' = 2k^2 + 2k$, entonces se tiene que $n^2 = 2k' + 1$.
Por definición de un número impar, concluimos que n^2 es impar. $\square$

Contenidos

Demostración por contrapositivo

Supongan que queremos demostrar:

$$\forall x. P(x) \to Q(x) \quad \equiv \quad \forall x.\ \neg Q(x) \ \to \ \neg P(x)$$

Método por contrapositivo

Suponemos que $Q(n)$ es **falso** para un n cualquiera (genérico) y demostramos que $P(n)$ también es **falso**.

Ejemplo de demostración por contrapositivo

Teorema

Suponga a y b son positivos. Si $n = ab$, entonces $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

¿Es posible hacer una demostración directa?

Demostración (por contrapositivo)

PD: Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $n \neq ab$.

Suponga que $a > \sqrt{n}$ y $b > \sqrt{n}$ con n positivo.

$$\begin{aligned} n &= \sqrt{n} \cdot \sqrt{n} & \\ &< a \cdot \sqrt{n} & (\text{por } a > \sqrt{n}) \\ &< a \cdot b & (\text{por } b > \sqrt{n}) \end{aligned}$$

Entonces, $n < a \cdot b$ y, por lo tanto, $n \neq ab$. □

Contenidos

Demostración por análisis de casos

Supongan que queremos demostrar:

$$\forall x \in D.\ P(x)$$

Metodó de análisis de casos

Dividimos el dominio de posibilidades D a una cantidad **finita de casos** $D_1, D_2, \ldots, D_k$ tal que:

$$D = D_1 \cup D_2 \cup \ldots \cup D_k$$

Por último, demostramos para todo subdominio D_i se cumple:

$$\forall x \in D_i.\ P(x)$$

con i desde 1 hasta k.

Ejemplo de una demostración por casos

Teorema

Para todo entero n se cumple que $n^2 \geq n$.

Demostración

1. Si $n = 0$, entonces $0^2 = 0$. Por lo tanto, $0^2 \geq 0$.
2. Si $n \geq 1$, entonces:

$$\begin{array}{rcll} n & \geq & 1 & \\ n^2 & \geq & n & \text{(multiplicando ambos lados por } n > 0\text{)} \end{array}$$

3. Si $n \leq -1$, como $n^2 \geq 0$ entonces se tiene que $n^2 \geq n$.

$\square$

¿Cuál es la ventaja de demostrar por casos?

Recomendación

"Cuando todos los métodos anteriores han fallado y no se sabe por donde empezar, una "estrategia" es empezar demostrando casos simples para así ***ganar intuición*** *en la demostración general. "*

Contenidos

Demostración de **doble implicación**

Supongan que queremos demostrar una afirmación como:

$$\forall x.\, P(x) \leftrightarrow Q(x)$$

Demostración para doble-implicación

Debemos demostrar dos afirmaciones (**ambas direcciones**):

$$\forall x.\, P(x) \rightarrow Q(x) \quad \text{y} \quad \forall x.\, P(x) \leftarrow Q(x)$$

Ejemplo de una demostración de **doble-implicación**

Teorema

Para todo número natural n,
se tiene que n es impar si, y solo si, n^2 es impar.

Demostración

$(\Rightarrow)$ Si n es impar, entonces n^2 es impar. ✓

$(\Leftarrow)$ Si n^2 es impar, entonces n es impar.

PD: Si n es par, entonces n^2 es par.

...

Ejercicio: termine la demostración.

Contenidos

Demostración por contradicción

Supongan que queremos demostrar una afirmación R, pero demostramos:

$$(\neg R) \to (S \wedge \neg S)$$

donde S es una afirmación cualquiera.

¿Qué implica esto?

Metodó por contradicción

Suponemos que $\neg R$ es verdadero y inferimos una **contradicción**.
Si esto sucede, entonces R debe ser **verdadero**.

Demostración por contradicción (versión alternativa)

Supongan que queremos demostrar:

$$R \ := \ \forall x.\ P(x) \to Q(x)$$

Metodó por contradicción

$$\neg R \ := \ \exists x.\ P(x) \wedge \neg Q(x)$$

Suponemos que existe un n tal que $P(n)$ es **verdadero** y $Q(n)$ es **falso** y inferimos una **contradicción**.

> *"Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game."*

A mathematician's apology (G. H. Hardy).

Ejemplo de una demostración por contradicción

Definiciones

- Un número r en $\mathbb{R}$ se dice **racional** si existen enteros p y q tal que:

$$r = \frac{p}{q}$$

  con $q \neq 0$ y p, q no tienen divisores en común exceptuando el 1.

- Un número $r \in \mathbb{R}$ se dice **irracional** si no es racional.

Teorema

$\sqrt{2}$ es un número irracional.

Ejemplo de una demostración por contradicción

Demostración ($\sqrt{2}$ es un número irracional)

Suponga que $\sqrt{2}$ es racional.
Entonces, existen p y q en $\mathbb{Z}$, sin divisores en común, tal que $\sqrt{2} = \frac{p}{q}$.

$$\begin{aligned} \sqrt{2} &= \frac{p}{q} \\ 2 \cdot q^2 &= p^2 \end{aligned}$$

Por lo tanto, p^2 es par y, entonces, p **es par** (¿por qué?).
Como p es par, entonces $p = 2k$ para algún k en $\mathbb{Z}$.

$$\begin{aligned} 2 \cdot q^2 &= p^2 \\ 2 \cdot q^2 &= (2k)^2 \\ q^2 &= 2 \cdot k^2 \end{aligned}$$

Por lo tanto, q^2 es par y, entonces, q **es par**.

¡Contradicción! (¿Por qué?)

$\square$

Contenidos

Demostración por **contra-ejemplo**

Supongan que deseamos demostrar que la siguiente afirmación es **falsa**:

$$\forall x.\ P(x)$$

Demostración por contra-ejemplo

Encontrar un elemento n (**cualquiera**) tal que $P(n)$ es **falso**.

Ejemplo de una demostración por **contra-ejemplo**

Teorema

Es falso que todo número mayor a 1 es la suma de dos cuadrados perfectos.

Demostración

Probamos con los primeros números mayor a 1:

$$\begin{aligned} 2 &= 1^2 + 1^2 \\ 3 &\neq 1^2 + 1^2 \\ &\neq 2^2 + 1^2 \end{aligned}$$

Por lo tanto, 3 no es la suma de dos cuadrados perfectos. $\square$

¿cómo buscar/encontrar el contra-ejemplo?

Recomendaciones

1. Probar primero los ejemplos más "**pequeños**".
2. Seguir con los ejemplos más "**comunes**".
3. Intentar con muchos ejemplos.

Contenidos

Demostración **existencial**

Supongan que queremos demostrar:

$$\exists x.\, P(x)$$

Demostración de existencia

Debemos demostrar que **existe** un elemento n tal que $P(n)$ es **verdadero**. Notese que NO es estrictamente necesario mostrar n explicitamente.

Ejemplo de una demostración **existencial**

Teorema

Existen dos números irracionales a y b tal que a^b es racional.

Demostración

Como $\sqrt{2}$ es irracional considere $\sqrt{2}^{\sqrt{2}}$.

1. Si $\sqrt{2}^{\sqrt{2}}$ es **racional** , entonces $a = \sqrt{2}$ y $b = \sqrt{2}$ es suficiente.
2. Si $\sqrt{2}^{\sqrt{2}}$ es **irracional** , entonces considere $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$.

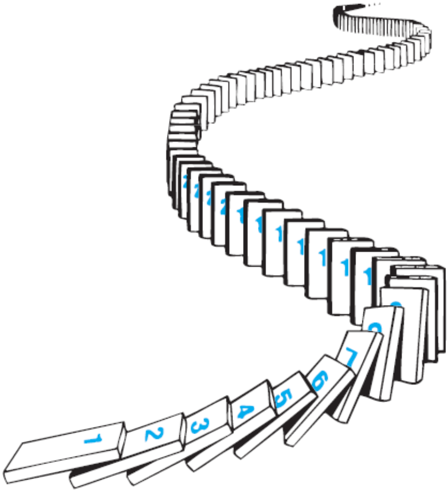
$$\begin{aligned} \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} &= \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} \\ &= \sqrt{2}^{2} \\ &= 2 \end{aligned}$$

Por lo tanto, a^b es racional.

$\square$

Contenidos

Demostración por inducción



Demostración por inducción

Suponga que deseamos demostrar una afirmación $\forall x.\ P(x)$ sobre $\mathbb{N}$.

Principio de inducción

Para una afirmación $P(x)$ sobre los naturales, si $P(x)$ cumple que:

1. $P(0)$ es verdadero,
2. si $P(n)$ es verdadero, entonces $P(n+1)$ es verdadero,

entonces para todo n en los naturales se tiene que $P(n)$ es verdadero.

Notación

- $P(0)$ se llama el **caso base**.
- En el paso 2.
  - $P(n)$ se llama la **hipótesis de inducción**.
  - $P(n+1)$ se llama la **tesis de inducción** o paso inductivo.

Ejemplo de demostración por inducción

Teorema

La suma de los primeros n números naturales es igual a $\frac{n \cdot (n+1)}{2}$.

Demostración

Demostramos que se cumple para $n = 0$:

$$\textbf{Caso base } (n = 0): \qquad 0 = \frac{0 \cdot (0+1)}{2} = 0$$

Ejemplo de demostración por inducción

Demostración (continuación)

Suponemos que se cumple para un n cualquiera y demostramos para $n+1$:

$$
\begin{array}{lrcl}
\textbf{Hipótesis:} & 0+1+\ldots n & = & \dfrac{n\cdot(n+1)}{2} \\[2ex]
\textbf{Inducción:} & 0+1+\ldots+n+(n+1) & = & \underbrace{0+1+\ldots+n}_{\text{caso n}}+(n+1) \\[2ex]
 & & = & \dfrac{n\cdot(n+1)}{2}+(n+1) \\[2ex]
 & & = & \dfrac{(n+1)\cdot((n+1)+1)}{2}
\end{array}
$$

$\square$

¿Cuál método de demostración ocupar?

¡No existe un método infalible para demostrar!

Recomendaciones

1. Escribir definiciones e hipótesis
2. Escribir el objetivo
3. Probar con distintos métodos.
4. Ganar intución intentando con casos o ejemplos mas sencillos.
5. Revisar demostraciones similares.
6. Sean creativos.