Demostracions

1 Demostració directa

Considerem $A_1, A_2, \ldots, A_n$ un conjunt d'hipòtesis, i una afirmació B. Volem demostrar que si $A_1, \ldots, A_n$, llavors B.
Es procedeix acceptant les hipòtesis. Es raona amb les hipòtesis, les definicions i resultats previs. Finalment s'acaba justificant B.

Estructura

Demostració. Suposem $A_1, \ldots, A_n$.
Arguments.
Per tant B. □

1.0.1 Exemples

Proposició 1.1. Siguin $a, b, c \in \mathbb{Z}$. Si $a|b$ i $b|c$, llavors $a|c$.
Demostració. Suposem que $a, b, c \in \mathbb{Z}$ i $a|b$ i $b|c$. Es vol veure que $a|c$.
Si $a|b$, llavors $b = an$ per $n \in \mathbb{Z}$. De la mateixa manera, $b|c$ vol dir $c = mb$ per $m \in \mathbb{Z}$. Per tant, $c = amn$. Com que $mn \in \mathbb{Z}$, llavors es conclou que $a|c$. □

Proposició 1.2. Si $n \in \mathbb{Z}$ és parell, llavors n^2 també és parell.

Demostració. Suposem que n és parell. Per tant $n = 2a$ per $a \in \mathbb{Z}$.

$$n^2 = (2a)^2 = 4a^2 = 2(2a^2)$$

Com que $2a^2 \in \mathbb{Z}$, llavors n^2 és parell. □

2 Demostracions per contrarecíproc

Demostracions basades en $A \to B \equiv \neg B \to \neg A$. Suposem $\neg B$ i mostrem que llavors $\neg A$.

2.0.1 Exemples

Proposició 2.1. Si n^2 és parell, llavors n també és parell.

Demostració. Suposem que n no és parell. Llavors n és senar, per tant es pot expressar com a $n = 2k + 1$ per $k \in \mathbb{Z}$.

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

Per tant n no és parell si n^2 tampoc ho és. Es conclou que si n^2 és parell, llavors n també ho és. □

Proposició 2.2. Si $a, b \in \mathbb{R}$ són tals que $a \cdot b \notin \mathbb{Q}$, llavors o $a \notin \mathbb{Q}$ o $b \notin \mathbb{Q}$.

Demostració. Suposem que a i b són racionals, llavors es poden escriure com $a = \frac{p}{q}$ i $b = \frac{r}{s}$ per $p, q, r, s \in \mathbb{Z}$ i $q, s \neq 0$. Llavors, $a \cdot b = \frac{p \cdot r}{q \cdot s}$ amb $q \cdot s \neq 0$. Per tant $a \cdot b \in \mathbb{Q}$. □

3 Demostracions per reducció a l'absurd

Volem demostrar A. Per fer-ho, suposem $\neg A$. Es raona fins que s'arriba a una contradicció. Per tant es conclou que $\neg A$ és impossible i per tant A.

També es pot aplicar a condicionals. Volem demostrar que $A \to B$. Suposem que $\neg(A \to B) \equiv (A \wedge \neg B)$. Es raona fins que es troba una contradicció. Per tant $A \to B$.

3.0.1 Exemples

Proposició 3.1. El nombre $\sqrt{2}$ és irracional.

Demostració. Per contradicció. Suposem que $\sqrt{2} \in \mathbb{Q}$. Llavors $\sqrt{2} = \frac{p}{q}$ per $p, q \in \mathbb{Z}$ coprimers.

$$(\sqrt{2})^2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$$

Per tant p^2 és parell i p també ho és. Llavors podem $p = 2a$ per $a \in \mathbb{Z}$.

$$(\sqrt{2})^2 = \frac{(2a)^2}{q^2} \Rightarrow 2q^2 = 4a^2 \Rightarrow q^2 = 2a^2$$

Per tant q^2 és parell i q també ho és. Tant p com q són parells, cosa que contradiu la hipòtesi inicial que q i p són coprimers. S'arriba a una contradicció, per tant $\sqrt{2} \notin \mathbb{Q}$. □

Definició 3.1 (Nombre primer)**.** Un nombre natural n és primer si i només si $n \geq 2$ i els únics divisors de n són 1 i n mateix.

Fet 3.1. Tot nombre natural major o igual que 2 té com a mínim un divisor primer.

Fet 3.2. Si $x|a$ i $x|a + b$, llavors $x|b$.

Proposició 3.2. Hi ha un nombre infinit de nombres primers.

Demostració. Suposem que hi ha un nombre finit de primers. Llavors els podem posar en una llista finita $p_1, p_2, \ldots, p_k$. Considerem el número $a = p_1 p_2 p_3 \cdots p_k + 1$. És sap que A té un divisor p que és primer. Donat a que els únics primers són els de la llista, existeix un $i \in [1, k]$ tal que $p = p_i$. Llavors $p|p_1 p_2 \cdots p_k$ i $p|a$. Llavors p ha de dividir el nombre 1, per tant $p = 1$ i p no és primer. S'arriba a una contradicció i per tant hi ha un nombre infinit de nombres primers. □

4 Tipus d'enunciats i les estratègies de demostració

4.1 Demostració d'un bicondicional

Enunciats del tipus, A i B són equivalents, A és condició necessària i suficient de B. L'estratègia és descomposar l'enunciat. $(A \leftrightarrow B) \equiv (A \to B) \wedge (B \to A)$. Per tant es demostra en dues parts.
($\to$) Es suposa A i es demostra B.
($\leftarrow$) Es suposa B i es demostra A.

4.2 Enunciats equivalents

A vegades es vol demostrar que una serie d'enunciats $A_1, A_2, A_3, \ldots$ són equivalents. Es sol fer un cercle d'implicacions.

$$A_1 \to A_2 \to \cdots \to A_{n-1} \to A_n \to A_1$$

. Per qüestions de facilitat a l'hora de demostrar implicacions també es poden fer sub-cercles.

4.3 Enunciats amb conjunció

Enunciats de la forma $(A \wedge B)$.
Es demostra A, a continuació és demostra B.

4.4 Enunciats amb disjunció

Demostració d'enunciats de la forma $(A \vee B)$. Hi ha més d'una manera. En general no és viable demostrar A o B individualment.

- Reducció a l'absurd. Suposem que $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$.
  Es desenvolupa fins a arribar a una contradicció.
- $(A \vee B) \equiv (\neg A \to B) \equiv (\neg B \to A)$.

4.5 Ús d'una disjunció en una demostració com a resultat intermedi

Com s'utilitza en una demostració una disjunció com a informació o resultat intermedi. S'obren dos casos.
Sabem que $A \vee B$, volem demostrar P.

- **Cas 1:** Si A, llavors P.
- **Cas 2:** Si B, llavors P.

Cal demostrar els dos casos per determinar que P és cert.

4.5.1 Exemples

Proposició 4.1. $\forall n \in \mathbb{N}, \quad n^2 + n$ és parell.

Demostració. **Cas 1:** Si n és parell, n^2 és parell. Un nombre parell més un altre, és parell. Per tant, $n^2 + n$ és parell.
Cas 2: Si n és senar, n^2 és senar. Un nombre senar més un altre senar, és senar. Per tant $n^2 + n$ és senar.
Per tant, per qualsevol $n \in \mathbb{N}$ el nombre $n^2 + n$ és parell. □

5 Inferències, equivalències i estratègies importants

5.1 Inferències

- Si A i B, llavors $(A \wedge B)$.
- Si $(A \wedge B)$, llavors A. (I B).

- Si A, llavors $(A \vee B)$.
- Si $(A \vee B)$ i $\neg A$, llavors B.
- Si $(A \to B)$ i A, llavors B.
- Si $(A \to B)$ i $\neg B$, llavors $\neg A$.

5.2 Equivalències

- $(A \vee B) \equiv (B \vee A)$. (Commutativa).
- $(A \wedge B) \equiv (B \wedge A)$. (Commutativa).
- $(A \leftrightarrow B) \equiv (A \to B) \wedge (B \to A)$.
- $\neg\neg A \equiv A$.
- $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$ (Llei de DeMorgan).
- $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$ (Llei de DeMorgan).

5.3 Estratègies

1. Demostració directa d'un condicional $(A \to B)$:
   - Es suposa A i es demostra B.
2. Reducció a l'absurt de A:
   - Es suposa $\neg A$ i s'arriba a una contradicció.
3. Demostració per casos. Es vol demostrar C amb hipòtesi $(A \vee B)$:
   - Es suposa A i es demostra C.
   - Es suposa B i es demostra C.

6 Demostració d'enunciats amb quantificadors

- $\forall x \quad A(x)$ (Com a dada en una demostració):
  - Si $\forall x \quad A(x)$, llavors $A(t)$ sigui la t que sigui.
- $\forall x \quad A(x)$ (Demostració):
  - Demostrar que per un x genèric $A(x)$ es compleix.
- $\exists x \quad A(x)$ (Com a dada):
  - No hi ha cap inferència associada.
  - Estratègia: Introduir una variable nova que refereixi a alguna cosa amb la propietat A.
- $\exists x \quad A(x)$ (Demostració):
  - Cal trobar un element x tal que $A(x)$.

6.0.1 Exemples

Proposició 6.1. $\forall n \in \mathbb{Z}\ \exists m \in \mathbb{Z}\quad n|m$.(Tot enter és divisor de com a mínim un enter).

Demostració. Sigui $n \in \mathbb{Z}$. Volem veure que hi ha un enter m tal que $n|m$ per qualsevol n. Prenem $n = m$ i clarament $n|m$. □

Proposició 6.2. $\exists n \in \mathbb{Z}\ \forall m \in \mathbb{Z}\quad n|m$. (Hi ha un enter que divideix tots els enters).

Demostració. Prenem $n = 1$. Llavors $\forall m \in \mathbb{Z}$ es compleix que $n|m$. □

Proposició 6.3. $\exists m \in \mathbb{Z}\ \forall n \in \mathbb{Z}\quad n|m$. (Existeix un enter que és divisible per tots els enters).

Demostració. Prenem $m = 0$. Llavors $n|m\quad \forall n \in \mathbb{Z}$. □

Proposició 6.4. $\forall m \in \mathbb{Z}\ \exists n \in \mathbb{Z}\quad n|m$. (Qualsevol enter té un divisor enter).

Demostració. Prenem $n = m$. Llavors clarament $n|m$. □

6.1 Demostració d'unicitat

Demostració de enunciats del tipus "Existeix un únic x que compleix P. Cal demostrar per un costat l'existència d'aquest element i d'altre banda que és únic. Per demostrar que un element és únic hi ha dues estratègies:

- Un cop determinat un x que ho compleix, demostrar que qualsevol x' que també ho compleixi és $x = x'$.
- Prendre dues solucions arbitràries x_1, x_2 i demostrar que $x_1 = x_2$.