Lògica, raonament i demostració

Miquel Angel Perelló
aprendes.com

Versió 2021

1 Introducció

No ens estranyaria gens veure que molts estudiants del batxillerat científic o tecnològic i del social coneixem la paraula demostració o prova, però en el fons no saben què significa, o, senzillament, encara no s'han adonat que sense aprendre a fer demostracions no s'avança correctament en matemàtiques.

A batxillerat, les matemàtiques probablement s'expliquen com una disciplina principalment computacional; s'aprèn a resoldre equacions, calcular derivades i integrals, multiplicar matrius i trobar determinants, i es veu com aquests conceptes i procediments poden donar resposta a qüestions pràctiques del món real. Però poques vegades es plantegen qüestions com: per què es pot aplicar aquest procediment i no un altre?, per què aquest resultat és cert? Les respostes a aquestes preguntes són el que importa sobretot a matemàtiques. Si apliquem aquest procediment o aquest resultat és perquè es compleixen les hipòtesis i s'ha demostrat abans que a partir d'elles s'obté com a conclusió el procediment o el resultat aplicat.

Aquest document va destinat als estudiants de batxillerat. Volem explicar com es construeixen les demostracions a matemàtiques. Per portar a terme aquest objectiu començarem aprenent d'una manera molt informal la lògica del llenguatge de les matemàtiques. Conèixer aquesta lògica és fonamental per comprendre el desenvolupament de les demostracions. Després donarem els mètodes de demostració més comuns a matemàtiques. Finalment, tractarem dues teories axiomàtiques: la geometria euclidiana en el pla i l'aritmètica dels nombres naturals.

Volem advertir que, en aquest document, s'assumeix coneixements bàsics de teoria de conjunts i un nivell de matemàtiques 4rt ESO avançat.

2 Variables i constants

Quan escrivim a la pissarra una expressió com $x + y = y + x$, a molta gent se li acut de seguida la propietat commutativa de la suma. És clar que sí, i a més, d'aquesta manera no hem d'escriure a la pissarra que l'ordre dels sumands no altera el resultat de la suma. Hem aconseguit sintetitzar una idea amb una expressió simbòlica fent ús de dues variables x i y. Si després escrivim $x+2 = 2+x$, tothom s'adona que aquesta igualtat és un cas particular de l'anterior substituint y per la constant el nombre

2. Podríem afegir molts més exemples, però no cal, tots recordeu el plantejament de problemes per equacions i la seva resolució, fet als cursos de l'ESO. Tot això seria molt més difícil de fer sense l'ajut de variables i constants. En resum, heu de tenir molt present que en el llenguatge de les matemàtiques és imprescindible l'ús de variables i constants.

Com hem dit, la formalització d'enunciats amb l'ajut de variables i constants es fa indispensable per a continuar endavant. En l'exemple següent es veu com es fa molt més senzill i alhora més rigorós treballar amb enunciats matemàtics si introduïm variables i constants. És habitual prendre com a variables les últimes lletres de l'abecedari i com a constants les primeres, però això és irrellevant.

Exemple 1. Amb l'ajut de variables i constants expressa els següents enunciats:

1. La mitja geomètrica de dos nombres positius és menor o igual que la mitja aritmètica.

   Si x, y són dos nombres positius, aleshores es compleix $\sqrt{x \cdot y} \leq \dfrac{x+y}{2}$.

2. El quadrat d'un nombre senar és senar.

   Si x és un nombre senar, aleshores x^2 és senar.

3. Donat un nombre real positiu, busqueu els nombres reals el quadrat dels quals és més petit o igual que el nombre donat.

   Sigui $a > 0$, aleshores hem de resoldre la inequació $x^2 \leq a$.

4. Trobar tres nombres parells consecutius que sumen 12.

   Busqueu un nombre parell x tal que $x + x + 2 + x + 4 = 12$.

3 Proposicions i predicats

És evident que l'enunciat 'si els elefants volen, existeix el nombre π' no és matemàtic perquè hi apareixen termes que no estan definits dins de les matemàtiques; en canvi, '161 és múltiple de 7' sí que és un enunciat matemàtic. Aquí no volem definir en rigor què és un enunciat matemàtic, només ens interessa que tingueu una idea intuïtiva clara sobre com distingir un enunciat matemàtic d'aquell que no ho és, i això creiem que ho podem assumir sense cap problema.

Hi han enunciats de les matemàtiques que són proposicions i altres, predicats. Una **proposició** és un enunciat que és o vertader o fals. Per exemple, els enunciats següents són proposicions vertaderes:

- Si un cercle té un radi de r unitats, aleshores la seva àrea és πr^2 unitats quadrades.
- Tot nombre parell és divisible per 2.
- $2 \in \mathbb{Z}$, que es llegeix '2 pertany als nombres enters'.
- $\sqrt{2} \notin \mathbb{Q}$, que es llegeix '$\sqrt{2}$ no pertany als nombres irracionals'.

- $\mathbb{N} \subseteq \mathbb{Z}$, que es llegeix 'els nombres naturals és un subconjunt dels nombres enters'.
- El conjunt $\{a, b, c\}$ té 3 elements.
- Alguns triangles rectangles són isòsceles.

En canvi, les proposicions següents són falses:

- $1 = 2$.
- $\sqrt{2} \notin \mathbb{R}$.
- Per a tot nombre real x, es té que $x^2 + 1 \leq 0$.
- $\{1, 2, 3\} \cap \mathbb{N} = \varnothing$, que es llegeix 'la intersecció dels conjunts $\{1, 2, 3\}$ i $\mathbb{N}$ és el conjunt vuit'.
- La suma dels angles de qualsevol quadrilàter val 180^o.
- Si $x = 2$, aleshores $x^2 = 9$.
- 6 és un nombre primer.

Volem observar que hi ha proposicions que tenen variables. Per exemple, l'enunciat 'Si x és un nombre enter, $2x + 1$ és senar' és una proposició vertadera. L'enunciat 'Per a tots els nombres reals x, y es compleix $(x - y)(x + y) = x^2 - y^2$' és una proposició verdadera coneguda com a identitat o producte notable. També hi ha proposicions falses amb variables com, per exemple, 'Per a tot nombre real x es té $\sqrt{x^2} = x$'.

Hi han enunciats que encara no sabem si són certs o no, però són proposicions o també anomenats **conjectures**. Per exemple, la conjectura de Goldbach diu: Tot enter parell superior a 2 és una suma de dos nombres primers. També tenim la conjectura de Fermat segons la qual per a tots els nombres naturals a, b, c, n i $n > 2$ es té $a^n + b^n \neq c^n$, però en aquest cas, a 1993, el matemàtic Andrew Wiles va demostrar que la conjectura era certa.

Finalment, els enunciats següents no són proposicions:

- x és un nombre parell.
- Una recta paral·lela a la recta d'equació $x + y = 1$.
- Els nombres enters parells més gran que un nombre irracional donat.
- La funció f és la funció inversa de la funció g.
- $2x + 1$.

Els **predicats** són enunciats oberts perquè contenen variables i són vertaders o falsos depenent dels valors assignats a les variables. Aquí denotem els predicats per lletres majúscules, com per exemple $P(x)$ o $Q(m,n)$, afegint les variables que estan presents entre parèntesis. Per exemple, l'enunciat 'n és un nombre primer' és un predicat que representem per $P(n)$, i l'enunciat 'm és més gran o igual que n', o abreujadament, '$m \geq n$' per $Q(m,n)$. Llavors, $P(2)$ és la proposició '2 és un nombre primer' que és vertadera, i $Q(3,4)$ és la proposició '$3 \geq 4$' que és falsa.

Dels cinc últims enunciats anteriors que no són proposicions els quatre primers són predicats. El primer és el predicat 'ser un nombre parell', que si el denotem per P, aleshores l'enunciat és $P(x)$. El segon és el predicat 'ser una recta paral·lela a $x+y=1$', que si el simbolitzem per Q i escrivim una recta del pla com $ax+by=c$, aleshores l'enunciat és $Q(a,b,c)$; per exemple, $Q(2,2,-1)$ és la proposició '$2x+2y=-1$ és una recta paral·lela a $x+y=1$' que és verdadera. De fet el tercer és una família de predicats que depèn del paràmetre a que és un nombre irracional. En concret, si el designem per P_a i considerem que la variable x pren valors a $\mathbb{Z}$, aleshores l'enunciat és $P_a(x)$; per exemple, $P_{\sqrt{2}}(4)$ és la proposició '4 és un nombre enter parell més gran que el nombre irracional $\sqrt{2}$' que és falsa. Finalment, l'últim és el predicat 'f és la funció inversa de g', que si el denotem per S i f,g són variables que denoten funcions, aleshores l'enunciat és $S(f,g)$; per exemple, $S(\sqrt[3]{x},x^3)$ és la proposició '$\sqrt[3]{x}$ és la funció inversa de x^3' que és vertadera. En canvi, l'últim no és un predicat perquè al substituir la variable x per un número s'obté un altre número, però en cap cas una proposició; diem que és una expressió algebraica. Aquestes expressions estan compostes per variables, constants numèriques i els símbols de les quatre operacions fonamentals de l'aritmètica.

Para acabar aquesta secció volem advertir que hem d'escriure

$$\text{'}3 \geq 4\text{' és falsa}$$

i no

$$3 \geq 4 \text{ és falsa}$$

perquè els termes 'vertadera' i 'falsa' no formen part del llenguatge de les matemàtiques (mireu l'observació següent). De fet hauríem d'escriure "$3 \geq 4$' es falsa perquè el nombre enter 3 no és més gran o igual que el nombre enter 4'. No és el nostre objectiu ser el màxim de rigorosos, però és important aquesta distinció perquè si no la fem, surten paradoxes, o sigui, enunciats que condueixen a fets contradictoris, que no es poden donar alhora. Aquí usem el català ampliat amb alguns símbols (per exemple, abans hem vist: $\in, \notin$ i $\subseteq$) que serveixen d'abreujadors per descriure el llenguatge de les matemàtiques; de fet això no és nou, ja que per aprendre la gramàtica anglesa podem fer ús del català.

Observació 1. Considerem una proposició p, aleshores l'enunciat "p és falsa" és una proposició? Suposem que p és una proposició, llavors p és vertadera o falsa. Si p és vertadera, llavors el que diu p és vertader i això contradiu el que diu l'enunciat, que p és falsa. Si p és falsa, llavors el que diu p és fals, però com el que diu l'enunciat és que p és falsa, llavors el que diu p és vertader que és contradictori amb supòsit que p és falsa. Per tant, l'enunciat 'p és falsa' no és una proposició.
Aquesta paradoxa també es pot presentar d'una manera més quotidiana: Un home afirma que està mentint. El que diu és vertader o fals? Suposem que l'home es

diu Joan. D'aquesta manera l'enunciat és "Joan diu: Ell està mentint."Destaquem l'enunciat "Joan està mentint". Aleshores, quan en Joan diu mentida, vol dir que l'enunciat "Joan està mentint"és falsa, i quan diu veritat, "Joan està mentint"és vertader. Tornem a trobar el cas d'abans on p és "Joan està mentint".
Aquesta paradoxa es dona també en el context dels conjunts, coneguda com a paradoxa de Russell, i diu: El conjunt de les coses que no són elements de si mateixes, és un conjunt? Denotem simbòlicament aquest conjunt per A, aleshores es té

$$A = \{x : x \notin x\}.$$

Segons la lògica clàssica, $A \in A$ o bé $A \notin A$. Com A és un conjunt, és una cosa, i per tant, (1) si $A \in A$, aleshores $A \notin A$ i això és una contradicció; (2) si $A \notin A$, aleshores $A \in A$ que també és una contradicció. En conseqüència, A no és conjunt. La base d'aquestes paradoxes està en el fet que no és correcte l'autoreferència des d'un mateix llenguatge. El mentider no pot dir que menteix si no vol contradir-se. Per evitar aquests problemes distingim entre llenguatge-objecte i metallenguatge. Es diu metallenguatge al llenguatge que usem per estudiar a un altre llenguatge, anomenat en aquest cas llenguatge-objecte.

4 Connectives lògiques

En teoria de conjunts combinem o modifiquem els conjunts amb operacions com la unió o la intersecció. De la mateixa manera, en aritmètica modifiquem nombres amb operacions com la suma o la multiplicació. Això també passa en lògica. Tenim algunes operacions per combinar o modificar proposicions o predicats; aquestes operacions es tradueixen en el llenguatge de les matemàtiques per les paraules 'i', 'o', 'no', 'si ... llavors ...' i '... si i només si ... '. És habitual simbolitzar aquestes operacions amb els símbols característics del llenguatge de la lògica. Aquí ho farem per una qüestió d'economia sintàctica. Cal tenir present que a matemàtiques, aquestes paraules tenen significats precisos, que donarem a l'apartat següent. En alguns casos, el significat matemàtic d'aquestes paraules difereix lleugerament o són més precisos que l'ús comú que fem en la vida quotidiana.

En general, la regla sintàctica és que a partir de dues proposicions p i q podem formar altres proposicions mitjançant les operacions lògiques, també anomenades **connectives lògiques**. La regla semàntica és que la veritat o falsedat d'aquestes noves proposicions dependrà de la veritat o falsedat de p i q, i serà definida per les anomenades **taules de veritat**. A una proposició se l'assigna el valor de veritat que simbolitzem per V quan la proposició és vertadera, i F quan és falsa.

4.1 Conjunció

Si p i q són dues proposicions, llavors la **conjunció** d'aquestes dues proposicions és la proposició 'p i q', simbolitzada per $p \wedge q$, i que es defineix de la següent manera:

- És vertadera, quan p i q són ambdues vertaderes;
- És falsa, quan p és falsa o q és falsa o ambdues són falses.

Per exemple, la proposició '$1 < \sqrt{2} < 2$' és la conjunció de les proposicions '$\sqrt{2} > 1$' i '$\sqrt{2} < 2$', que són totes dues vertaderes i, per tant, és vertadera.
D'acord amb la definició anterior, s'obté la taula de veritat de la conjunció lògica:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

.

Observem que la conjunció de dues proposicions només és vertadera quan les dues proposicions són vertaderes.

4.2 Disjunció

Si p i q són dues proposicions, llavors la **disjunció** d'aquestes dues proposicions és la proposició 'p o q', simbolitzada per $p \vee q$, i que es defineix de la següent manera:

- És vertadera, quan almenys una de les dues proposicions és vertadera;
- És falsa, quan p i q són ambdues falses.

Per exemple, la proposició '$\pi \in (-\infty, -1) \cup (1, +\infty)$' és la disjunció de les proposicions '$\pi < -1$' o '$\pi > 1$', la primera és falsa i la segona és vertadera i, per tant, és vertadera. La taula de veritat d'aquesta connectiva és

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

.

Observem que la disjunció de dues proposicions és falsa quan les dues proposicions són falses. Destaquem l'ús **inclusiu** que fem d'aquesta connectiva respecte de l'exclusiu que fem servir habitualment a la vida quotidiana i que fa que la proposició sigui vertadera quan només una de les proposicions és vertadera.

4.3 Negació

Si p és una proposició, llavors la **negació** d'aquesta proposició és la proposició 'no p', simbolitzada per $\neg p$, que es defineix de la següent manera:

- És vertadera, quan p és falsa;
- És falsa, quan p és vertadera.

Per exemple, la proposició '$\sqrt{3} \notin (0, 1)$' és la negació de la proposició '$\sqrt{3} \in (0, 1)$', que és falsa i, per tant, és vertadera. La taula de veritat d'aquesta connectiva és

p	$\neg p$
V	F
F	V

.

4.4 Condicional

Si p i q són dues proposicions, llavors el **condicional** d'aquestes dues proposicions és la proposició 'si p, llavors q', simbolitzada per $p \longrightarrow q$, i que es defineix de la següent manera:

- És vertadera, quan p i q són ambdues vertaderes o p és falsa;
- És falsa, quan p és vertadera i q és falsa.

Una proposició condicional 'si p, llavors q' també se'n diu **implicació** i diem que "p implica q", i que p és l'**antecedent** i q és el **conseqüent** de la implicació. La interpretació que fem d'aquesta connectiva sorprèn una mica en el seu ús doncs, per exemple, en l'enunciat 'Si hi ha dues rectes en el pla que són paral·leles, llavors 2 és un nombre primer' no hi ha cap relació entre l'antecedent 'hi ha dues rectes en el pla que són paral·leles' i el conseqüent '2 és un nombre primer', i, és matemàticament correcte, independentment de si l'antecedent és vertader o fals.
Segons la definició que hem donat, la taula de veritat d'aquesta connectiva és

p	q	$p \longrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

.

Observem que només és falsa quan l'antecedent és vertader i el conseqüent és fals.
El condicional de dues proposicions p i q podem trobar-lo en proposicions escrites al català de moltes maneres: (1) q si p; (2) si p, q; (3) p només si q; o (4) q sempre que p.
Per exemple, la proposició '700 és divisible per 4 perquè el nombre acaba amb dos zeros' és el condicional: '$P(700)$ implica $Q(700)$, on P és el predicat 'tenir zero a les decenes i també a les unitats' i Q és 'ser divisible per 4'.

4.5 Bicondicional

Si p i q són dues proposicions, llavors el **bicondicional** d'aquestes dues proposicions és la proposició 'p si i només si q', simbolitzada per $p \longleftrightarrow q$, i que es defineix de la següent manera:

- És vertadera, quan p i q són ambdues vertaderes o falses;
- És falsa, quan p és vertadera i q és falsa, o p és falsa i q és vertadera.

Una proposició bicondicional 'p si i només si q' també se'n diu **doble implicació** i diem que "p implica q i q implica p". La taula de veritat d'aquesta connectiva és

p	q	$p \longleftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

.

Per exemple, la proposició '98 és múltiple de 6 si i només si 98 és divisible per 2 i també per 3' és el bicondicional '$P(98)$ si i nomes si $Q(2)$ i $R(3)$, on P és el predicat 'ser múltiple de 6', Q és 'ser divisible per 2' i R és 'ser divisible per 3'.

Exemple 2. Escriu fent ús de les connectives les proposicions següents: (1) $-4 \leq -1$; (2) $|-3| = |2|$; (3) $-1 \in [0,1]$; (4) $2 \notin [0,1]$; (5) $\sqrt{2} < 2 < 2\sqrt{2}$ si $1 < \sqrt{2} < 2$; (6) $\sqrt[3]{1331} = 11$ si i només si $11^3 = 1331$.

Solució: (1) La proposició $-4 \leq -1$ es pot expressar com la disjunció: '$-4 < -1$' o '$-4 = -1$'. (2) La proposició $|-3| = |2|$ és la disjunció: '$-3 = 2$' o'$-3 = -2$'. (3) La proposició $-1 \in [0,1]$ és la conjunció: '$-1 \geq 0$' i '$-1 \leq 1$'. (4) La proposició $2 \notin [0,1]$ és la negació: 'no $2 \in [0,1]$'. (5) La proposició '$\sqrt{2} < 2 < 2\sqrt{2}$ si $1 < \sqrt{2} < 2$' és el condicional '$1 < \sqrt{2} < 2$ implica $\sqrt{2} < 2 < 2\sqrt{2}$'. (6) La proposició '$\sqrt[3]{1331} = 11$ si i només si $11^3 = 1331$' és el bicondicional ' $11^3 = 1331$ implica $\sqrt[3]{1331} = 11$ i $\sqrt[3]{1331} = 11$ implica $11^3 = 1331$'. □

5 Proposicions elementals i compostes

Proposicions **elementals** són aquelles que no posseeixen cap operador lògic. Les proposicions **compostes** estan formades per altres proposicions i operadors lògics. Per exemple, a partir de dues proposicions elementals p i q, podem formar com hem vist $\neg q$ i $p \vee q$. Però també $p \wedge \neg q$, i finalment, $(p \vee q) \longrightarrow (p \wedge \neg q)$. Hem utilitzat els parèntesis per evitar ambigüetats. De fet, també hem utilitzat la convenció estàndard segons el qual el símbol de negació $\neg$ té prioritat sobre les altres quatre connectives, però cap d'aquestes té prioritat sobre les altres.
Volem ara formalitzar l'enunciat següent: 'Es realitza una gran festa només si faig bé aquest deure o els meus amics estan d'acord'. Identifiquem les següents proposicions simples: p = 'Es realitza una gran festa', q = 'Faig bé aquest deure', i r = 'Els meus amics estan d'acord'. Llavors l'enunciat s'escriu simbòlicament d'aquesta manera tenint en compte les connectives lògiques: $(q \vee r) \longrightarrow p$. Un altre exemple és la proposició '273 és divisible per 91, si 273 és múltiple de 7 i múltiple de 13' és el condicional: '$P(273) \longrightarrow (Q(273) \wedge R(273))$', on P és el predicat 'ser divisible per 91', Q és 'ser mútiple de 7' i R és 'ser múltiple de 13'.

Donada una proposició composta, volem determinar el seu valor de veritat coneixent el valor de veritat de les proposicions simples que la conformen. Suposem la interpretació segons la qual les proposicions simples p i q són vertaderes i r i s són falses. Llavors, quin és el significat de la proposició composta $\neg(p \vee q) \longrightarrow (r \wedge \neg s)$?

p	q	r	s	$\neg s$	$p \vee q$	$\alpha = \neg(p \vee q)$	$\beta = (r \wedge \neg s)$	$\alpha \longrightarrow \beta$
V	V	F	F	V	V	F	F	V

La taula deduïm que la propocisió és falsa.

Donat el valor de veritat d'una proposició composta, ara volem determinar el valor de veritat de les proposicions simples que la conformen. Suposem que la proposició composta $(p \wedge \neg q) \longrightarrow r$ és falsa. Llavors, com la connectiva principal d'aquesta proposició és el condicional. Atès que aquesta implicació té un valor de veritat fals únicament quan l'antecedent és vertader i el conseqüent és fals, s'obté que $p \wedge \neg q$ és vertadera, i r ha de ser falsa. Ara bé $p \wedge \neg q$ és falsa només si p i q són vertadera i falsa, respectivament. Per tant, p és vertadera i, q i r, false

6 Formes proposicionals

Com hem fet fins ara les lletres $p, q, r, \ldots$ s'usen com a variables que representan a proposicions. El valor de veritat de p, per exemple, és desconegut mentre no s'especifica la seva interpretació, és a dir, no és coneix el significat de la proposició que representa.

Anomenem **formes proposicionals** a les expressions formals constituïdes per variables proposicionals i les connectives lògiques que les relacionen. Per exemple, $A(p,q,r) = ((p \wedge q) \longrightarrow (r \vee \neg p)) \wedge r$ és una forma proposional que conté tres variables p, q i r. Les formes proposicionals no són proposicions, però si cada variable proposicional és reemplaçada per una proposició simple o composta, la forma proposicional es converteix en una proposició. Si reemplacem les variables proposicionals per proposicions vertaderes o falses, el nombre de proposicions que es generen és 2^n, sent n el nombre de variables proposicionals. A la taula de veritat que es genera se l'anomena a vegades **matriu** de la forma proposicional. La matriu de la forma $A(p,q,r)$ té $2^3 = 8$ interpretacions posibles:

p	q	r	$\neg p$	$\alpha = p \wedge q$	$\beta = r \vee \neg p$	$\alpha \longrightarrow \beta$	$(\alpha \longrightarrow \beta) \wedge r$
V	V	V	F	V	V	V	V
V	V	F	F	V	F	F	F
V	F	V	F	F	V	V	V
V	F	F	F	F	F	V	F
F	V	V	V	F	V	V	V
F	V	F	V	F	V	V	F
F	F	V	V	F	V	V	V
F	F	F	V	F	V	V	F

La forma es converteix en una proposició vertadera quan les variables proposicionals p, q i r s'interpreten respectivament com a proposicions que són vertadera, falsa i vertadera (fila 3 de la matriu).

Exemple 3. Construeix la matriu de la forma $A(p,q) = (p \vee q) \longrightarrow (p \wedge \neg q)$. Quina interpretació permet assegurar que la forma es converteix en una proposició vertadera?

Solució: La forma té dues variables proposicionals i, per tant, $2^2 = 4$ interpretacions possibles. La matriu de la forma és:

p	q	$\neg q$	$p \vee q$	$p \wedge \neg q$	$(p \vee q) \longrightarrow (p \wedge \neg q)$
V	V	F	V	F	F
V	F	V	V	V	V
F	V	F	V	F	F
F	F	V	F	F	V

Observem que una proposició d'aquesta forma només serà vertadera quan substituïm q per una proposició falsa. $\square$

7 Tautologies i contradiccions

Una **tautologia** és una proposició que és vertadera per necessitat lògica. Una tautologia característica de la lògica clàssica és la proposició 'p o no p', sent p

qualsevol proposició. Aquesta tautologia se la coneix també amb el nom de **principi del tercer exclòs**, segons el qual la disjunció d'una proposició i la seva negació és sempre vertadera. En efecte, la taula de veritat d'aquesta proposició és

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

,

on veiem que l'última columna hi ha només el valor V com era d'esperar. Es evident que la tautologia no té cap interés matemàtic perquè no informa de res, però permet simplificar a vegades les demostracions com veurem més endavant.

Ara bé, el concepte de tautologia té més sentit quan en lloc de tractar amb proposicions treballem en formes. Una forma és tautologia quan la matriu de la forma només genera proposicions vertaderes; en unes altres paraules, quan és certa en totes les circumstàncies possibles. Per exemple, la forma $A(p,q) = (p \wedge q) \longrightarrow (p \vee q)$ és tautologia perquè la seva taula és:

p	q	$p \wedge q$	$p \vee q$	$(p \wedge q) \longrightarrow (p \vee q)$
V	V	V	V	V
V	F	F	V	V
F	V	F	V	V
F	F	F	F	V

D'aquí surt el fet següent: qualsevol proposició composta de la forma '$(p \wedge q) \longrightarrow (p \vee q)$' és una tautologia, independentment del que siguin les proposicions p i q.

Una **contradicció** és una proposició que és falsa per necessitat lògica. De fet, tota contradicció és la negació d'una tautologia i, al contrari, tota tautologia és la negació d'una contradicció. La negació del principi del tercer exclòs és una contradicció coneguda com el **principi de contradicció**, segons el qual la conjunció d'una proposició i la seva negació és una proposició sempre falsa. És la proposició 'p i no p', sent p qualsevol proposició. La taula de veritat d'aquesta proposició és

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

,

i veiem que l'última columna només té el valor F. De la mateixa manera que la tautologia, la contradicció té més sentit quan s'aplica a formes proposicionals. Una forma és contradicció quan la seva matriu només genera proposicions falses. Per exemple, segons el principi de contradicció la forma $(p \longrightarrow q) \wedge \neg(p \longrightarrow q)$ és una contradicció. Podem comprovar-ho fent la seva matriu:

p	q	$p \longrightarrow q$	$\neg(p \longrightarrow q)$	$(p \longrightarrow q) \wedge \neg(p \longrightarrow q)$
V	V	V	F	F
V	F	F	V	F
F	V	V	F	F
F	F	V	F	F

.

Per acabar, quan una forma proposicional no és tautologia ni contradicció es diu que és **contingència**; en unes altres paraules, quan admet algunes proposicions vertaderes i altres falses per als valors de veritat de les variables proposicionals. Un exemple de contingència és la forma $(p \vee q) \longrightarrow (p \wedge q)$ perquè la seva matriu és:

p	q	$p \vee q$	$p \wedge q$	$(p \vee q) \longrightarrow (p \wedge q)$
V	V	V	V	V
V	F	V	F	F
F	V	V	F	F
F	F	F	F	V

.

Les formes proposicionals poden ser connectades amb operadors lògics per a formar noves formes proposicionals. D'aquesta manera, si A i B són formes, llavors $\neg A$, $A \wedge B$, $A \vee B$, $A \longrightarrow B$ i $A \longleftrightarrow B$ representen noves formes proposicionals. Per exemple, si $A(p,q) = \neg p \longrightarrow q$ i $B(p,r,s) = s \longrightarrow (p \vee \neg r)$, aleshores $C(p,q,r,s) = A(p,q) \longrightarrow B(p,r,s)$, és a dir, $C(p,q,r,s) = (\neg p \longrightarrow q) \longrightarrow (s \longrightarrow (p \vee \neg r))$. Observem que A té $2^2 = 4$ interpretacions, B en té $2^3 = 8$ interpretacions, i C en té $2^4 = 16$ interpretacions.

Exemple 4. Si p, q i r són variables proposicionals, llavors $((\neg p \vee q) \wedge (\neg r \longrightarrow q)) \longrightarrow (p \longrightarrow r)$ és una forma proposicional tautològica?

Solució: La forma conté 3 variables i per tant la matriu de la forma té $2^3 = 8$ interpretacions possibles. En lloc de fer la taula, podem raonar suposant que la forma s'interpretés com a contradicció. Aleshores existeix una valoració de les variables segons la qual l'implicación és falsa i, per tant, l'antecedent $(\neg p \vee q) \wedge (\neg r \longrightarrow q)$ és vertader i el conseqüent $p \longrightarrow r$ és fals. Ara bé, l'antecedent és vertader quan $\neg p \vee q$ i $\neg r \longrightarrow q$ són ambdues vertaderes, i el conseqüent és fals quan p és vertader i r és fals. Però si prenem aquesta interpretació, aleshores $\neg p \vee q$ i $\neg r \longrightarrow q$ no poden ser ambdues vertaderes perquè $\neg p \vee q$ és vertadera només si q és vertadera, però $\neg r \longrightarrow q$ és aleshores falsa i, per tant, això no és possible. Com a conseqüència, concluïm que la forma no pot prendre el valor fals i, per tant, és tautologia.
Alternativament, si construïm la matriu de la forma es té:

p	q	r	$\neg p$	$\neg r$	$\alpha = \neg p \vee q$	$\beta = \neg r \vee q$	$\gamma = p \longrightarrow r$	$\alpha \wedge \beta$	$(\alpha \wedge \beta) \longrightarrow \gamma$
V	V	V	F	F	V	V	V	V	V
V	V	F	F	V	V	V	F	F	V
V	F	V	F	F	F	F	V	F	V
V	F	F	F	V	F	V	F	F	V
F	V	V	V	F	V	V	V	V	V
F	V	F	V	V	V	V	V	V	V
F	F	V	V	F	V	F	V	F	V
F	F	F	V	V	V	V	V	V	V

i surt que és tautologia com era d'esperar. $\square$

8 Implicació lògica

Si A i B són dues formes proposicionals, llavors es diu que A **implica lògicament** B quan la forma $A \longrightarrow B$ és tautologia. Cal destacar que la implicació lògica és una

relació entre formes proposicionals, que denotem per $\Longrightarrow$. D'aquesta manera, quan escrivim $A \Longrightarrow B$, que llegim "A implica B", significa que $A \longrightarrow B$ és tautologia. A la pràctica, el fet de tenir la implicació $A \Longrightarrow B$ permet fer el següent argument: si $A \Longrightarrow B$ i A és tautologia, aleshores necessariàment B és tautologia. D'aquí surt una interpretació molt comú en matemàtiques: quan $A \Longrightarrow B$, aleshores B es diu que és **condició necessària** per A, i també, que A és **condició suficient** per B. Per exemple, suposem que n és un enter positiu, aleshores l'enunciat 'si n és divisible per 4, llavors n és divisible per 2', és cert i pot escriure's com $P(n) \longrightarrow Q(n)$, on P = 'és divisible per 2' i Q = 'és divisible per 4'. La condició 'n és divisible per 4' és suficient perquè 'n sigui divisible per 2', és a dir, basta que n sigui divisible per 4 perquè sigui divisible per 2. En canvi, la condició 'n és divisible per 2' és necessària perquè 'n és divisible per 4', o sigui, si n no fos divisible per 2, aleshores no seria divisible per 4.
Més endavant veurem que les implicacions seran extremadament útils per construir raonaments vàlids. En particular, s'utilitzaran àmpliament les següents implicacions: Si A, B i C són formes proposicionals, aleshores

1. $(A \longrightarrow B) \wedge A \Longrightarrow B$
2. $(A \longrightarrow B) \wedge \neg B \Longrightarrow \neg A$
3. (i) $A \wedge B \Longrightarrow A$; (ii) $A \wedge B \Longrightarrow B$
4. (i) $A \Longrightarrow A \vee B$; (ii) $B \Longrightarrow A \vee B$
5. (i) $(A \vee B) \wedge \neg B \Longrightarrow A$; (ii) $(A \vee B) \wedge \neg A \Longrightarrow B$
6. (i) $A \longleftrightarrow B \Longrightarrow A \longrightarrow B$; (ii) $A \longleftrightarrow B \Longrightarrow B \longrightarrow A$
7. $(A \longrightarrow B) \wedge (B \longrightarrow A) \Longrightarrow A \longleftrightarrow B$
8. $(A \longrightarrow B) \wedge (B \longrightarrow C) \Longrightarrow A \longrightarrow C$

Per veure que $(A \longrightarrow B) \wedge A \Longrightarrow B$ hem de comprovar que $((A \longrightarrow B) \wedge A) \longrightarrow B$ és tautologia. Construïm la taula de veritat corresponent:

A	B	$A \longrightarrow B$	$(A \longrightarrow B) \wedge A$	$((A \longrightarrow B) \wedge A) \longrightarrow B$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

i observem que efectivament és tautologia. Anàlogament es fa per les altres.

9 Equivalència lògica

Si A i B són dues formes proposicionals, llavors es diu que A i B són **equivalents lògicament** quan la forma $A \longleftrightarrow B$ és tautologia. Com la implicació lògica, l'equivalència és una relació entre formes proposicionals que denotem per $\Longleftrightarrow$. D'aquesta manera, quan escrivim $A \Longleftrightarrow B$, que llegim "A és equivalent a B"o "A i B són equivalents", significa que $A \longleftrightarrow B$ és tautologia.

A la pràctica, el fet de tenir l'equivalència $A \Longleftrightarrow B$ permet fer el següent argument: Si $A \Longleftrightarrow B$, i A (resp. B) és tautologia, aleshores necessàriament B (resp. A) és tautologia, i també, d'aquí surt una interpretació molt comuna en matemàtiques: quan $A \Longleftrightarrow B$, aleshores es diu que A és **condició necessària i suficient** per B o a l'inrevés. De fet, això es dedueix de l'equivalència següent: $A \longleftrightarrow B \Longleftrightarrow (A \longrightarrow B) \wedge (B \longrightarrow A)$ perquè

A	B	$\alpha = A \longrightarrow B$	$\beta = B \longrightarrow A$	$\gamma = A \longleftrightarrow B$	$\alpha \wedge \beta$	$\gamma \longleftrightarrow (\alpha \wedge \beta)$
V	V	V	V	V	V	V
V	F	F	V	F	F	V
F	V	V	F	F	F	V
F	F	V	V	V	V	V

A continuació s'enumeren algunes equivalències que seran particularment útils i al seu costat el nom pel qual són conegudes:

1. $\neg(\neg A) \Longleftrightarrow A$ (llei de la doble negació)
2. $A \wedge B \Longleftrightarrow B \wedge A$ (llei commutativa de $\wedge$)
3. $A \vee B \Longleftrightarrow B \vee A$ (llei commutativa de $\vee$)
4. $(A \wedge B) \wedge C \Longleftrightarrow A \wedge (B \wedge C)$ (llei associativa de $\wedge$)
5. $(A \vee B) \vee C \Longleftrightarrow A \vee (B \vee C)$ (llei associativa de $\vee$)
6. $A \vee (B \wedge C) \Longleftrightarrow (A \vee B) \wedge (A \vee C)$ (llei distributiva de $\vee$ respecte de $\wedge$)
7. $A \wedge (B \vee C) \Longleftrightarrow (A \wedge B) \vee (A \wedge C)$ (llei distributiva de $\wedge$ respecte de $\vee$)
8. $A \longrightarrow B \Longleftrightarrow \neg A \vee B$
9. $A \longrightarrow B \Longleftrightarrow \neg B \longrightarrow \neg A$ (llei del contrarecíproc)
10. $A \longleftrightarrow B \Longleftrightarrow (A \longrightarrow B) \wedge (B \longrightarrow A)$ (llei del bicondicional)
11. $(A \vee B) \longrightarrow C \Longleftrightarrow (A \longrightarrow C) \wedge (B \longrightarrow C)$
12. $A \longrightarrow (B \wedge C) \Longleftrightarrow (A \longrightarrow B) \wedge (A \longrightarrow C)$
13. $\neg(A \wedge B) \Longleftrightarrow \neg A \vee \neg B$ (llei de De Morgan)
14. $\neg(A \vee B) \Longleftrightarrow \neg A \wedge \neg B$ (llei de De Morgan)

Algunes d'aquestes lleis tenen molt d'interès quan volem fer demostracions. La llei de la doble negació a la pràctica es usa de la següent manera: volem provar que p és vertadera. Per a fer-ho, suposem com hipòtesi que $\neg p$ és vertadera, i deduïm contradicció, i, per tant, $\neg(\neg p)$ és vertadera. Ara bé, $\neg(\neg p)$ i p són equivalents i, per tant, p és vertadera. Aquesta manera de demostrar un enunciat matemàtic serà tractada amb més detall més endavant.

Es diu **recíproc** de la proposició $p \longrightarrow q$ a la proposició $q \longrightarrow p$, i **contrarecíproc** a la proposició $\neg q \longrightarrow \neg p$. La llei del contrarecíproc també és la base de moltes demostracions. A la pràctica es usa de la següent manera: volem provar que p implica q. Per a fer-ho, observem que és més senzill provar que $\neg q$ implica $\neg p$, i, per tant, és cert que p implica q. Tractarem aquesta forma de demostració més en detall més endavant.

Finalment, fem alguns comentaris sobre la llei del bicondicional. Quan s'ha de demostrar una equivalencia $p \longleftrightarrow q$, la llei del bicondicional permet fer-ho de la següent manera: primer, provem que p implica q, i després, el recíproc, es a dir, que q implica p. Es habitual en matemàtiques dir-ho d'alguna d'aquestes maneres: (1) p és condició necessària i suficient per q o (2) si p, llavors q, i recíprocament.

Per a completar aquesta secció provarem les lleis 10 i 12. Per demostrar 10 hem de comprovar que $(A \longleftrightarrow B) \longleftrightarrow (A \longrightarrow B) \wedge (B \longrightarrow A)$ és tautologia. En efecte, construiïm la matriu i s'obté tautologia

A	B	$\alpha = A \longrightarrow B$	$\beta = B \longrightarrow A$	$\gamma = A \longleftrightarrow B$	$\alpha \wedge \beta$	$\gamma \longleftrightarrow (\alpha \wedge \beta)$
V	V	V	V	V	V	V
V	F	F	V	F	F	V
F	V	V	F	F	F	V
F	F	V	V	V	V	V

.

Per demostrar 11 hem de comprovar que $\neg(A \wedge B) \longleftrightarrow (\neg A \vee \neg B)$ és tautologia. En efecte, construiïm la matriu i s'obté tautologia

A	B	$A \wedge B$	$\neg A$	$\neg B$	$\alpha = \neg(A \wedge B)$	$\beta = \neg A \vee \neg B$	$\alpha \longleftrightarrow \beta$
V	V	V	F	F	F	F	V
V	F	F	F	V	V	V	V
F	V	F	V	F	V	V	V
F	F	F	V	V	V	V	V

.

Les altres és demostran de la mateixa manera.

Exemple 5. Escriu fent ús de les connectives les proposicions següents: (1) S'ha de revisar. Per exemple, la proposició 'un nombre natural és parell si i només si el seu quadrat és parell' és el bicondicional: $P(n)$ si i nomes si $P(n^2)$, on P és el predicat 'ser un nombre natural parell'. (2) És necessàri que x sigui un nombre real no negativo perquè $\sqrt{x}$ sigui real; (3) És suficient que $n = 3$ perquè $n^2 - 5n + 6 = 0$; (4) $n^2 - 5n + 6 = 0$ precisament si $n = 2$ o $n = 3$; (5) $|a| = |b|$ sii $a = \pm b$.

Solució: La proposició (1) es pot expressar com la implicació: $\sqrt{x}$ és real $\Longrightarrow x$ real i $x \geq 0$; la proposició (2) és la implicació: $n = 3 \Longrightarrow n^2 - 5n + 6 = 0$; la proposició (3) és el bicondicional: $n^2 - 5n + 6 = 0 \Longleftrightarrow n = 2$ o $n = 3$, i, la proposició (4) és també un bicondicional: $|a| = |b| \Longleftrightarrow a = \pm b$. $\square$

10 Inferència lògica

Molts cops veieu com en resoldre exercicis a matemàtiques se us demana que raoneu o justifiqueu la resposta. Ara volem tractar aquest assumpte. Què es vol dir que raoneu la vostra resposta? És clar, heu de fer un raonament vàlid que justifiqui allò que se us demana demostrar. Això té dues parts, una és conduir correctament el vostre raonament des del punt vista lògic, i l'altra, és comprendre correctament els conceptes que estan presents en el raonament des del punt de vista matemàtic. Aquí tractarem el primer punt perquè el segon depèn dels coneixements que cadascú té de les matemàtiques.

Suposem que la proposició condicional '$p \to q$' és vertadera. Llavors sabem (recordeu la taula de veritat d'aquesta connectiva) que si 'p' és vertadera, necessàriament ho serà 'q'. Ara bé, només pel fet que '$p \to q$' sigui vertadera no es té que 'p' i 'q' siguin vertaderes, perquè podrien ser totes dues falses, o 'p' falsa i 'q' vertadera. Per tant, si '$p \to q$' i 'p' són vertaderes, llavors sí que 'q' ha de ser vertadera. En aquest últim cas es diu que 'q' és **conseqüència lògica** de '$p \to q$' i 'p' o també que 'q' s'**infereix lògicament** de '$p \to q$' i 'p'. És habitual representar aquesta inferència lògica seguint el següent format:

$$\begin{array}{l} p \longrightarrow q \\ \underline{p \qquad\qquad} , \\ q \end{array}$$

on la linea horitzontal separa les proposicions que es diuen **premisses**, de la proposició que es diu **conclusió**.
Per exemple: Si $x \in A$, llavors $|x| \leq 1$; sabem que $x \in A \cap B$. En conseqüència, $|x| \leq 1$. La regla d'inferència anterior ens permet assegurar que aquest argument és vàlid i perquè sabem que $x \in A \cap B$ implica $x \in A$.

Observem doncs, que la conseqüència lògica és una relació entre les premisses i la conclusió. De fet, pel raonament que hem fet abans aquesta inferència pot també escriure's com '$(p \to q) \wedge p$' $\Longrightarrow$ 'q', és a dir, com una implicació lògica. És clar que també podríem reescriure aquesta implicació lògica en termes de formes proposicionals com $(A \longrightarrow B) \wedge A \Longrightarrow B$, on A i B són formes, i també com a inferència lògica seguint el format anterior:

$$\begin{array}{l} A \longrightarrow B \\ \underline{A \qquad\qquad} . \\ B \end{array}$$

En general, des del punt de vista lògic un **raonament** és un condicional que té com antecedent la conjunció de proposicions $P_1, ..., P_n$, anomenades premisses, i com a conseqüent una proposició C, anomenada conclusió.

$$(P_1 \wedge \cdots \wedge P_n) \longrightarrow C$$

Es diu que el raonament és **vàlid** si la conclusió necessàriament es deriva de les premisses, o sigui, si $(P_1 \wedge \cdots \wedge P_n) \longrightarrow C$ és tautologia, o equivalentment, si $(P_1 \wedge \cdots \wedge P_n) \Longrightarrow C$. Pensant en la noció d'implicació lògica, podem dir que un raonament és vàlid si no podem assignar valors de veritat a les proposicions que s'utilitzen en el raonament de manera que les premisses siguin vertaderes i la conclusió sigui falsa.

No hem d'oblidar que la lògica s'ocupa només d'analitzar la validesa dels raonaments, no ens pot dir si la informació continguda en una hipòtesi és vertadera o falsa. Els termes vàlid i no vàlid es refereixen a l'estructura del raonament, no a la veritat o falsedat de les proposicions què depèn dels nostres coneixements de matemàtiques.

Tenint en compte l'última manera d'escriure el nostre argument, podríem intentar demostrar que és vàlid, mostrant que $(P_1 \wedge \cdots \wedge P_n) \longrightarrow C$ és tautologia, utilitzant una taula de veritat. Aquest mètode realment funcionaria, però no seria gens eficaç. En primer lloc, atès que si hi ha m proposicions implicades, la taula de veritat hauria de tenir 2^m files, la qual cosa seria molt feixuga si m és gran. En segon lloc, l'ús d'una taula de veritat no proporciona cap visió intuïtiva de per què l'argument és vàlid.
Per a aquests motius, en lloc d'utilitzar taules de veritat, intentarem justificar la validesa dels raonaments fent ús de les implicacions lògiques que hem donat. Si volem demostrar una implicació lògica complicada, és recomanable fer-ho descomponent-la en una col·lecció d'implicacions més senzilles, preses d'una en una. Si ja es coneixen les implicacions més simples, podrien ser blocs per a la implicació més complicada. Algunes de les implicacions senzilles que fem servir, conegudes com a **regles d'inferència** de la lògica proposicional, es detallen a continuació.

$\begin{array}{l} A \longrightarrow B \\ A \\ \hline B \end{array}$	MP: Modus Ponens	$\begin{array}{l} A \longrightarrow B \\ \neg B \\ \hline \neg A \end{array}$	MT: Modus Tollens
$\begin{array}{l} A \\ \hline\hline \neg\neg A \end{array}$	DN: Doble Negació	$\begin{array}{l} A \\ \hline\hline A \end{array}$	R: Repetició
$\begin{array}{l} A \wedge B \\ \hline A \end{array}$	EC: Eliminació Conjunctor	$\begin{array}{l} A \wedge B \\ \hline B \end{array}$	EC: Eliminació Conjunctor
$\begin{array}{l} A \\ B \\ \hline A \wedge B \end{array}$	IC: Introducció conjunctor	$\begin{array}{l} A \\ \hline A \vee B \end{array}$	IC: Introducció disjunctor
$\begin{array}{l} B \\ \hline A \vee B \end{array}$	ID: Introducció Disjunctor	$\begin{array}{l} A \vee B \\ \neg A \\ \hline B \end{array}$	ED: Eliminació Disjunctor
$\begin{array}{l} A \vee B \\ \neg B \\ \hline A \end{array}$	ED: Eliminació Disjunctor	$\begin{array}{l} A \longleftrightarrow B \\ \hline A \longrightarrow B \end{array}$	EB: Eliminació Bicondicional
$\begin{array}{l} A \longleftrightarrow B \\ \hline B \longrightarrow A \end{array}$	EB: Eliminació Bicondicional	$\begin{array}{l} A \longrightarrow B \\ B \longrightarrow A \\ \hline A \longleftrightarrow B \end{array}$	IB: Introducció Bicondicional
$\begin{array}{l} A \longrightarrow B \\ B \longrightarrow C \\ \hline A \longrightarrow C \end{array}$	TC: Transitivitat Condicional	$\begin{array}{l} A \longrightarrow B \\ C \longrightarrow D \\ A \vee C \\ \hline B \vee D \end{array}$	DC: Dilema constructiu
$\begin{array}{l} \neg (A \vee B) \\ \hline\hline \neg A \wedge \neg B \end{array}$	DM: De Morgan	$\begin{array}{l} \neg (A \wedge B) \\ \hline\hline \neg A \vee \neg B \end{array}$	DM: De Morgan

En aquesta taula hem utilitzat el conveni de representar per una línia horitzontal doble dues regles d'inferència com s'indica a continuació:

$$\begin{array}{c} A \\ \hline\hline B \end{array} \qquad \text{està en lloc de} \qquad \begin{array}{c} A \\ \hline B \end{array} \quad \text{i} \quad \begin{array}{c} B \\ \hline A \end{array}$$

on A i B són formes proposicionals. No sols hem tingut present les implicacions lògiques de la secció 8, també les equivalències lògiques de la secció 9 com, per exemple, les lleis de De Morgan.

Exemple 6. Volem determinar si el següent raonament és vàlid: "Si en Pau va rebre l'e-mail, llavors va agafar l'avió i serà aquí al migdia. Pau no va agafar l'avió. Per tant, Pau no va rebre l'e-mail".

Solució: Primer procedim a identificar les proposicions simples:

$p =$ 'Pau va rebre l'e-mail'

$q =$ 'Pau va agafar l'avió'

$r =$ 'Pau serà aquí al migdia'

Després, expressem formalment el raonament:

$$\begin{array}{ll} P_1: & p \longrightarrow (q \wedge r) \\ P_2: & \neg q \\ \hline C: & \neg p \end{array}$$

Per provar la validesa d'aquest argument utilitzarem les regles d'inferència:

$$\begin{array}{lll} 1. & p \longrightarrow (q \wedge r) & P_1 \\ 2. & \neg q & P_2 \\ 3. & \neg q \vee \neg r & \text{ID } 2 \\ 4. & \neg (q \wedge r) & \text{DM } 3 \\ \hline 5. & \neg p & \text{MT } (1,4) \end{array}$$

Observem que la fila 3 s'ha deduït de la fila 2 mitjançant la regla ID; la fila 4 s'ha deduït de la fila 3 fent ús de la llei de De Morgan i, finalment, la fila 5 que és la conclusió s'ha obtingut de les files 1 i 4 per la regla MT. □

Exemple 7. Volem determinar si el següent raonament és vàlid: "Si robes un banc, vas a la presó. Si anem a la presó, no ens divertim. Si tenim vacances, ens divertim. Robem un banc o tenim vacances. Per tant, anem a la presó o ens divertim"

Solució: Les proposicions simples d'aquest raonament són:

$p =$ 'Robem un banc'

$q =$ 'Anem a la presó'

$r =$ 'Ens divertim'

$s =$ 'Tenim vacances'

Expressem el raonament simbòlicament:

$$\begin{array}{ll} P_1: & p \longrightarrow q \\ P_2: & q \longrightarrow \neg r \\ P_3: & s \longrightarrow r \\ P_4: & p \vee s \\ \hline C: & q \vee r \end{array}$$

Intentem provar la validesa d'aquest argument utilitzant les regles d'inferència:

$$\begin{array}{lll} 1. & p \longrightarrow q & P_1 \\ 2. & q \longrightarrow \neg r & P_2 \\ 3. & s \longrightarrow r & P_3 \\ 4. & p \vee s & P_4 \\ \hline 5. & q \vee r & \text{DC } (1,3,4) \end{array}$$

Observem, però que no hem fet ús de la hipòtesi 2. Llavors, la conclusió $q \vee r$ és vertadera si q i r ho són, però en canvi la hipòtesi 2, $q \longrightarrow \neg r$, és falsa i això no és possible. Per tant, el raonament no és vàlid. $\square$

En tot raonament se'ns presenten dues qüestions molt importants: Una és la seva validesa, i l'altra, és la seva deduïbilitat. La primera qüestió fa referència a les taules de veritat, i la segona, a les regles d'inferència. Quina relació hi ha entre aquestes dues nocions? Tot i que no és absolutament obvi ni fàcil de demostrar, resulta molt remarcable que les dues nocions, una de naturalesa semàntica i l'altre sintàctica, sempre donen el mateix resultat, és a dir, un raonament és vàlid si i només si és deduïble. Per tant, si volem demostrar que un argument donat és vàlid, n'hi haurà prou amb demostrar que és deduïble i viceversa. L'equivalència d'aquests dos enfocaments és un resultat important en la lògica. El fet que la validesa implica la deduïbilitat es coneix com a **teorema de completesa** de la lògica proposicional, i el fet que la deduïbilitat implica la validesa es coneix com a **teorema de la correcció** de la lògica proposicional. Aquests resultats i les seves demostracions podem trobar-se en qualsevol text de lògica proposicional.

Per les consideracions anteriors veiem que per provar que un raonament és vàlid, simplement hem de trobar una deducció, que sovint és una tasca molt més agradable que mostrar directament la seva validesa. En canvi, per provar que un raonament no és vàlid, les deduccions no són de gran ajuda, perquè hauríem de demostrar que no és possible trobar cap deducció, i això no podrem assegurar-ho mai, sempre podria haver-hi una deducció que funcionés. En aquests casos és millor fer servir la definició de validesa directament i trobar valors de veritat per als quals les proposicions que són premisses del raonament siguin vertaderes i la conclusió falsa.

Exemple 8. Volem determinar la validesa del següent raonament: "Si el crim va ocórrer després de les 4, llavors en Pep no va poder haver-lo comès. Si el crim va ocórrer a les 4 o abans, llavors en Carles no va poder haver-lo comès. El crim involucra a dues persones, si en Carles no el va cometre. Per tant, el crim involucra a dues persones".

Solució: Primer procedim a identificar les proposicions simples:

$p =$ 'El crim va ocórrer després de les 4'

$q =$ 'Pep podia haver comès el crim'

$r =$ 'Carles podia haver comès el crim'

$s =$ 'El crim involucra a dues persones'

Després expressem el raonament simbòlicament:

$$\begin{array}{ll} P_1: & p \longrightarrow \neg q \\ P_2: & \neg p \longrightarrow \neg r \\ P_3: & \neg r \longrightarrow s \\ \hline C: & s \end{array}$$

Intentem provar la validesa d'aquest argument utilitzant les regles d'inferència:

$$
\begin{array}{lll}
1. & p \longrightarrow \neg q & P_1 \\
2. & \neg p \longrightarrow \neg r & P_2 \\
3. & \neg r \longrightarrow s & P_3 \\
4. & \neg p \longrightarrow s & \text{TC } (2,3) \\
5. & p \vee \neg p & \text{Tautologia} \\
\hline
6. & \neg q \vee s & \text{DC } (1,4,5)
\end{array}
$$

No hem deduït s sinó $\neg q \vee s$. Això fa pensar que si q és falsa i s també, hi ha una interpretació (una fila de la taula de veritat) que farà les premisses vertaderes i la conclusió, falsa; es pot comprovar que això passa si prenem p i r ambdues vertaderes. Per tant, aquest raonament no és vàlid. A continuació mostrem la interpretació esmentada:

p	$\longrightarrow$	$\neg$	q	$\neg$	p	$\longrightarrow$	$\neg$	r	$\neg$	r	$\longrightarrow$	s	s
V	V	V	F	F	V	V	F	V	F	V	V	F	F

Volem destacar el fet què construir una taula de veritat per veure que hi ha una valoració que prova el que hem dit, portaria molta feina perquè la taula tindria 16 files. □

Hi ha raonaments que quan intentem provar la seva validesa deduïm una contradicció, és a dir, deduïm una proposició i la seva negació. Llavors es diu que el conjunt de premisses d'aquest raonament és **inconsistent**. Quan les premisses d'un raonament no són inconsistents es diu que les premisses són **consistents**. No és que hi hagi res lògicament erroni amb premisses inconsistents, senzillament que no serveixen per res, perquè aleshores podem deduir qualsevol proposició. Volem destacar també que, des del punt de vista semàntic, un raonament té un conjunt de premisses inconsistent quan no hi ha cap interpretació (cap fila de la taula de veritat) que faci a totes les premisses vertaderes.

Exemple 9. Volem determinar si les premisses del següent raonament és o no consistent: "Miquel no toca la piano o Maria toca la guitarra. Si Carla no toca el violí, Maria no toca la guitarra. Miquel toca el piano i Carla no toca el violí. Per tant, Jaume toca l'acordió".

Solució: Procedim a formalitzar el raonament, identificant les seves proposicions simples:

$p =$ 'Miquel toca la piano'

$q =$ 'Maria toca la guitarra'

$r =$ 'Carla toca el violí'

$s =$ 'Jaume toca l'acordió'

Llavors el raonament formalitzat és

$$
\begin{array}{ll}
P_1 : & \neg p \vee q \\
P_2 : & \neg r \longrightarrow \neg q \\
P_3 : & p \wedge \neg r \\
\hline
C : & s
\end{array}
$$

Per un costat, utilitzant les regles d'inferència, s'obté:

1.	$\neg p \vee q$	P_1
2.	$\neg r \longrightarrow \neg q$	P_2
3.	$p \wedge \neg r$	P_3
4.	p	EC 3
5.	$p \vee s$	ID 4
6.	$\neg r$	EC 3
7.	$\neg q$	MP (2,6)
8.	$\neg p$	ED (1,7)
9.	s	ED (5,8)

Per un altre, es té també

1.	$\neg p \vee q$	Hipòtesis
2.	$\neg r \longrightarrow \neg q$	Hipòtesis
3.	$p \wedge \neg r$	Hipòtesis
4.	p	EC 3
5.	$p \vee \neg s$	ID 4
6.	$\neg r$	EC 3
7.	$\neg q$	MP (2,6)
8.	$\neg p$	ED (1,7)
9.	$\neg s$	ED (5,8)

Observem que hem deduït s en el primer cas, i $\neg s$, en el segon. Com a conseqüencia, podem deduïr $s \wedge \neg s$, que és una contradicció. Per tant, el conjunt de premisses és inconsistent.
També podem provar la inconsistència de les premisses comprovant si és possible que hi hagi una interpretació que faci totes les premisses vertaderes:

$\neg$	p	$\vee$	q	$\neg$	r	$\longrightarrow$	$\neg$	q	p	$\wedge$	$\neg$	r
		V				V !				V		
F	V		V	V	F	F !	F	V	V		V	F

Observem que no és possible excepte que acceptem que una proposició sigui vertadera i falsa alhora, cosa que no pot ser. □

Per acabar aquesta secció, volem tractar els raonaments que a vegades es consideren com a vàlids i no ho són, sovint coneguts com a **fal·làcies**. En primer lloc tractarem els que tenen a veure amb un mal ús de les regles d'inferència. Són arguments que poden semblar vàlids a primera vista, però que són fal·làcies. Considerem el següent raonament: "Si l'Albert menja un bon dinar, beurà una cervesa. L'Albert va beure una cervesa i, per tant, va menjar un bon dinar". Podríem pensar que aquest raonament és vàlid per MP, però no és així. En efecte, si formalitzem l'argument es té:

$p =$ 'Albert menja un bon dinar'

$q =$ 'Albert beurà una cervesa'

i, aleshores,

$$\begin{array}{ll} P_1: & p \longrightarrow q \\ P_2: & q \\ \hline C: & p \end{array}$$

És evident que no poden aplicar MP i, a part, no és vàlid, perquè pot haver begut una cervesa sense haver tingut un bon sopar. De fet, si fem la interpretació següent

$$\begin{array}{ccc||c||c} p & \longrightarrow & q & q & p \\ \hline \text{F} & \text{V} & \text{V} & \text{V} & \text{F} \end{array}$$

comprovem el que hem dit.

Considerem ara el següent raonament: "Si en Joan va en bicicleta a primera hora del matí, aleshores menja un bon esmorzar. En Joan no va en bicicleta. Per tant, en Joan no menja un bon esmorzar". Podríem pensar que aquest raonament és vàlid per MT, però no és així. En efecte, si formalitzem l'argument es té:

$p =$ 'Joan va en bicicleta a primera hora del matí'

$q =$ 'Joan menja un bon esmorzar'

i, aleshores,

$$\begin{array}{ll} P_1: & p \longrightarrow q \\ P_2: & \neg p \\ \hline C: & \neg q \end{array}$$

És evident que no poden aplicar MT i, a part, no és vàlid, perquè pot haver menjat un bon esmorzar sense haver anat en bicicleta. De fet, si fem la interpretació següent

$$\begin{array}{ccc||c|c||cc} p & \longrightarrow & q & \neg & p & \neg & q \\ \hline \text{F} & \text{V} & \text{F} & \text{V} & \text{F} & \text{F} & \text{V} \end{array}$$

comprovem el que hem dit.

En segon lloc, hi ha raonaments que no són vàlids perquè es fan suposicions que no estan justificades per les premisses. Per exemple, considerem el següent raonament: "Si en Dídac té febre, esternuda molt. Per tant, Dídac esternuda molt". És clar que podríem aplicar MP per concloure que en Dídac esternuda molt, però no sabem per les hipòtesis que en Dídac té febre.

Aquests exemples de fal·làcies poden semblar molt senzills, però quan el raonament és més extens i complex, i no s'escriu sinó que es parla, a vegades aquests errors lògics passen desapercebuts. Cal doncs tenir cura de no cometre'ls.

11 Quantificadors

En la secció 'Variables i constants' hem escrit

$$x + y = y + x,$$

reconeixent en aquesta expressió la llei commutativa de l'aritmètica. Si assumim que les variables designen nombres reals, aquest enunciat afirma que tots els nombres

reals compleixen aquesta propietat i, en general, tots els enunciats d'aquest tipus que afirmen que objectes arbitraris d'una classe compleixen una determinada propietat, s'anomenen **proposicions universals**.
A vegades també ens trobem enunciats com

$$x^2 - 3x + 2 = 0$$

reconeixent en aquesta expressió que hi ha dos nombres que compleixen aquesta equació. En aquests casos diem que són **proposicions existencials** perquè afirmen l'existència d'objectes (en aquest cas, els nombres 1 i 2) que compleixen una certa propietat.

Fins ara, mitjançant els símbols lògics $\wedge, \vee, \neg, \longrightarrow$ i $\longleftrightarrow$, hem vist com podem formalitzar molts enunciats de les matemàtiques i com podem conèixer que dos enunciats diferents tenen el mateix significat si són equivalents. També hem vist com la formalització ens pot ajudar a comprendre l'estructura lògica dels raonaments, i com els raonaments són vàlids amb l'ajut d'implicacions lògiques o regles d'inferència. Però amb tot això no n'hi ha prou per captar la totalitat del significat de molts enunciats de les matemàtiques. A l'inici d'aquesta secció hem vist com hi ha uns enunciats molt comuns a matemàtiques que cal estudiar amb més detall.

En efecte, imaginem que estem tractant un conjunt infinit X de nombres enters. Considerem ara l'enunciat 'Tots els elements de X són senars'. Si volem formalitzar aquest enunciat, hauríem d'escriure

$$P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \cdots,$$

on $P(x)$ és el predicat 'x és senar'. I si volem formalitzar l'enunciat 'Hi ha almenys un element de X que és senar', hauríem d'escriure

$$P(x_1) \vee P(x_2) \vee P(x_3) \vee \cdots.$$

El problema d'aquestes dues expressions és que no s'acaben mai. Per superar-lo introduirem dos nous símbols $\exists$ i $\forall$. El símbol $\exists$, anomenat **quantificador existencial**, està en lloc de frases com 'existeix' o 'hi ha un'. D'aquesta manera l'enunciat 'Hi ha elements de X que són senars' podem escriure'l així

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

El símbol $\forall$, anomenat **quantificador universal**, està en lloc de frases com 'per a tots' o 'per a cadascun'. D'aquesta manera l'enunciat 'Tots els elements de X són senars' podem escriure'l així

$$\forall x \in X, P(x).$$

Els exemples que hem donat a l'inici d'aquesta secció podem ara expressar-los d'aquesta manera:

$$(\forall x, y)\,(x, y \in \mathbb{R} \longrightarrow x + y = y + x)$$

que constitueix una proposició universal, i l'altre

$$(\exists x)\,\big(x \in \mathbb{R} \wedge\ x^2 - 3x + 2 = 0\big)$$

que és una proposició existèncial.

Observació 2. En teoria de conjunts la proposició $\exists x \in X, P(x)$ podem escriure-la d'aquesta manera:

$$\{x \in X : P(x)\} \neq \emptyset,$$

indicant que el conjunt dels elements que compleixen la propietat P és no vuit; i la proposició $\forall x \in X, P(x)$, com

$$\{x \in X : P(x)\} = X,$$

indicant que el conjunt dels elements que compleixen la propietat P és tot el conjunt X.

L'enunciat 'el quadrat d'un nombre real més petit o igual que 4' és un predicat. Si x és un nombre real, aleshores '$x^2 \leq 4$' és el predicat abreujat. L'enunciat '$x^2 \leq 4$' no és una proposició perquè no podem afirmar que sigui vertadera o falsa llevat que assignem a la varible lliure x un valor real. Si representem per $P(x)$ aquest predicat, llavors $P(1)$ és una proposició vertadera, en canvi, $P(3)$ és falsa.
Hi ha una altra manera de fer que un predicat es converteixi en una proposició. Es fent que les seves variables lliures quedin lligades per quantificadors. Considerem que $P(x)$ el predicat anterior, aleshores '$\forall x \in \mathbb{R},\ P(x)$' és una proposició falsa, i en canvi, '$\exists x \in \mathbb{R},\ P(x)$' és vertadera.

Podem construir enunciats amb més d'un quantificador. Per exemple, considerem el predicat $Q(m, n) =$ '$m < n$', on $m, n \in \mathbb{Z}$. Llavors, la proposició '$\forall m \in \mathbb{Z}\ \exists n \in \mathbb{Z}, m < n$', escrita en català com 'per a tot nombre enter m existeix algun altre enter n tal que $m < n$', és vertadera. En efecte, donat qualsevol enter m, existeix $n = m + 1$, també és enter i compleix la condició $m < n$.

L'ordre dels quantificadors és molt important perquè per exemple, canviant l'ordre de l'enunciat anterior, o sigui '$\exists m \in \mathbb{Z}\ \forall n \in \mathbb{Z}, m < n$' es té una proposició falsa. És important també observar el paper que fan les variables lliures en una proposició que també en té de lligades. Amb relació al predicat anterior, considerem la proposició '$\exists m \in \mathbb{Z},\ m < n$', què és vertadera perquè només cal prendre $m = n - 1$. Si ara posem x en lloc de m en la proposició, es té '$\exists x \in \mathbb{Z},\ x < n$' que té el mateix significat que l'anterior; de fet, els valors de m o x depenen sempre del valor que assignem a la variable lliure n, i, per tant, si aquesta expressió formés part d'una expressió més llarga, aquesta última no canviaria en el seu significat. En canvi, si substituïm la variable lliure n per una altra q, la proposició '$\exists m \in \mathbb{Z},\ m < q$' pot canviar el significat d'una expressió més llarga de la qual en forma part, doncs ara m depèn de q i no de n.

Ara volem veure la negació de proposicions amb quantificadors. Per exemple, considerem el predicat $Q =$ 'tenir els ulls blaus'. Llavors, si suposem que la variable x té per domini el conjunt de totes les persones, l'enunciat 'Totes les persones tenen els ulls blaus' s'escriu així: $(\forall x)\, Q(x)$. La negació d'aquest enunciat és 'No totes les persones tenen els ulls blaus' que s'escriu com $\neg\, (\forall x)\, Q(x)$. És clar que aquest últim enunciat també el podem escriure com 'Hi ha alguna persona que no te els ulls blaus', que simbòlicament ho escrivim així: $(\exists x)\, \neg Q\,(x)$.
Considerem ara el cas d'una proposició existencial. Considerem l'enunciat 'Existeix una solució real en l'equació $x^3 + x = 0$'. Si suposem que el domini de la variable x són

els nombres reals, aleshores escrivim aquesta proposició així: $(\exists x)\,(x^3+x=0)$. La negació d'aquesta proposició és 'Cap nombre real és solució de l'equació $x^3+x=0$', que s'escriu així: $(\forall x)\,(x^3+x\neq 0)$.

Podem resumir els dos casos anteriors d'aquesta manera: Si $P(x)$ és un predicat i el domini de la variable x és el conjunt U, aleshores es compleixen les següents equivalències:

- $\neg\,(\forall x\in U, P(x)) \Longleftrightarrow \exists x\in U, \neg P\,(x)$
- $\neg\,(\exists x\in U, P\,(x)) \Longleftrightarrow \forall x\in U, \neg P\,(x)$

A diferència de les equivalències discutides a la secció ???, no podem utilitzar taules de veritat per verificar aquestes equivalències, tot i que són certes, basant-se en els significats dels quantificadors. Podem utilitzar les equivalències anteriors per negar proposicions amb més d'un quantificador. Per exemple, suposem que f és una funció real de variable i considerem l'enunciat 'Per a cada nombre real x, existeix un nombre real y tal que $f(x)=y$'; simbòlicament s'escriu com $(\forall x)\,(\exists y)\,(f(x)=y)$. La seva negació és

$$\begin{aligned}\neg\,((\forall x)\,(\exists y)\,(f(x)=y)) &\Longleftrightarrow (\exists x)\,(\neg\,(\exists y)\,(f(x)=y))\\ &\Longleftrightarrow (\exists x)\,((\forall y)\,(f(x)\neq y))\,,\end{aligned}$$

i, reformulant aquesta última expressió en català es té: 'Existeix un nombre real x tal que per a tot nombre real y es compleix $f(x)\neq y$'.

Finalment, passem a les regles d'inferència amb quantificadors. Hi ha quatre regles d'inferència d'aquest tipus i, tot i que el seu ús requereix una mica més de cura que les regles d'inferència de la secció ???, s'utilitzen amb el mateix propòsit, que és mostrar la validesa dels raonaments lògics.

EQU: $\dfrac{(\forall x\in U)\,P(x)}{P(a)}$ (Eliminació Quantificador Universal)

on a és qualsevol element de U.

IQU: $\dfrac{P(b)}{(\forall x\in U)\,P(x)}$ (Introducció Quantificador Universal)

on b és un element arbitrari de U.

EQE: $\dfrac{(\exists x\in U)\,P(x)}{P(c)}$ (Eliminació Quantificador Existencial)

on c és un element de U però el símbol 'c' no ha d'haver aparagut en el argument abans.

IQE: $\dfrac{P(d)}{(\exists x\in U)\,P(x)}$ (Introducció Quantificador Existencial)

on d és un element de U.

En la regla EQE volem destacar el fet que c no fa referència a cap símbol que ja s'ha utilitzat en l'argument. Per tant, hem de triar una lletra nova, en lloc d'una que ja s'utilitzi per a una altra cosa.

Un exemple de raonament lògic senzill que implica quantificadors és el següent:

> 'A cada gat simpàtic i intel·ligent li agrada el fetge picat. Tots els gats siamesos són agradables. Hi ha un gat siamès al qual no li agrada el fetge picat. Per tant, hi ha un gat estúpid.'

Formalitzem els enunciats del raonament. Per facilitar l'escriptura, considerem que la variable x té per domini el conjunt de tots els gats. Denotem per S, I, F i G els predicats 'és simpàtic o agradable', I, 'és intel·ligent', F, 'agrada el fetge picat', i G, 'és gat siamès', respectivament. Aleshores, el raonament podem simbolitzar-lo d'aquesta manera:

$$\begin{array}{rl} P_1: & (\forall x)\,(S(x) \wedge I(x) \longrightarrow F(x)) \\ P_2: & (\forall x)\,(G(x) \longrightarrow S(x)) \\ P_3: & (\exists x)\,(G(x) \wedge \neg F(x)) \\ \hline C: & (\exists x)\,\neg I(x) \end{array}$$

Fem ara la deducció per provar la seva validesa:

$$\begin{array}{lll} 1. & (\forall x)\,(S(x) \wedge I(x) \longrightarrow F(x)) & P_1 \\ 2. & (\forall x)\,(G(x) \longrightarrow S(x)) & P_2 \\ 3. & (\exists x)\,(G(x) \wedge \neg F(x)) & P_3 \\ 4. & G(a) \wedge \neg F(a) & \text{EQE } 3 \\ 5. & G(a) \longrightarrow S(a) & \text{EQU } 2 \\ 6. & S(a) \wedge I(a) \longrightarrow F(a) & \text{EQU } 1 \\ 7. & G(a) & \text{EC } 4 \\ 8. & \neg F(a) & \text{EC } 4 \\ 9. & S(a) & \text{MP } (5,7) \\ 10. & \neg\,(S(a) \wedge I(a)) & \text{MT } (6,8) \\ 11. & \neg S(a) \vee \neg I(a) & \text{DM } 10 \\ 12. & \neg\neg S(a) & \text{DN } 9 \\ 13. & \neg I(a) & \text{ED } (11,12) \\ \hline 14. & (\exists x)\,\neg I(x) & \text{IQE } 13 \end{array}$$

Tinguem en compte que a la línia (4) hem escollit alguna lletra com 'a' que no s'utilitzava abans d'aquesta línia, perquè apliquem la regla EQE.

Exemple 10. Considereu el raonament formalitzat següent:

$$\begin{array}{rl} P_1: & (\exists x \in U)\,(P(x) \wedge Q(x)) \\ P_2: & (\exists x \in U)\,M(x) \\ \hline C: & (\exists x \in U)\,(M(x) \wedge Q(x)) \end{array}$$

Es proposa la prova següent per a provar la seva validessa, és correcte?

$$\begin{array}{lll} 1. & (\exists x \in U)\,(P(x) \wedge Q(x)) & P_1 \\ 2. & (\exists x \in U)\,M(x) & P_2 \\ 3. & P(a) \wedge Q(a) & \text{EQE } 1 \\ 4. & Q(a) & \text{EC } 3 \\ 5. & M(a) & \text{EQE } 2 \\ 6. & Q(a) \wedge M(a) & \text{IC } (4,5) \\ 7. & (\exists x \in U)\,(M(x) \wedge Q(x)) & \text{IQE } 6 \end{array}$$

Solució: No és correcte, perquè en el pas 5 el símbol 'a' ha aparagut abans. $\square$

12 Definicions i la identitat

Quan, per exemple, en el conjunt dels nombres enters diem que x és divisible per y si i només si existeix un nombre enter k tal que $x = ky$, simbòlicament

$$x \mid y \Longleftrightarrow (\exists z)\,(z \in \mathbb{Z} \wedge x = ky)\,,$$

volem establir una definició del símbol '$|$' donant el seu significat amb ajuda de termes ja coneguts com 'nombre enter', 'producte' (o 'quocient'). De la mateixa manera, en el conjunt dels nombres reals diem que $x \leq y$ si i només si no és el cas que $x > y$, formalment,

$$(\forall x, y)\,(x \leq y \Longleftrightarrow \neg\,(x > y))\,,$$

establim la definició del símbol '$\leq$' donant el seu significat amb ajuda del predicat ja conegut '$>$'. En aquest últim cas, per exemple, podem substituir en qualsevol proposició el predicat '$x \leq y$' pel predicat 'no és el cas que $x > y$' sense que canvi el seu significat.

No volem donar una definició precisa de com cal construir correctament una definició, però tota definició pot adoptar la forma d'una equivalència lògica; el membre de l'esquerra ha de contenir allò que volem definir i, el de la dreta, allò que està ja ben definit o que el seu significat sigui comprensible immediatament, però mai hi ha d'aparèixer el que volem definir.

La noció d'identitat present en molts enunciats com "x és idèntic a y', 'x és el mateix que y', o senzillament, 'x és igual a y' i que abreugem simbòlicament per $x = y$ es pot definir des del punt de vista lògic amb l'ajut de la llei de Leibniz. D'acord amb aquesta llei, $x = y$ si i només si x i y tenen en comú totes les seves propietats. Observeu que aquest enunciat no pertany a la lògica proposicional perquè s'hauria de fer ús d'un quantificador sobre una variable que designa propietats d'objectes i no objectes com hem fet fins ara. Formalment, es té

$$x = y \Longleftrightarrow (\forall P)\,(Px \longleftrightarrow Py)$$

on Px designa una propietat que compleix x. Tot i això, a matemàtiques és més comú interpretar la relació d'identitat com una relació d'igualtat o de congruència dins d'un domini determinat d'objectes. Per exemple, en àlgebra diem que dos polinomis $A(x)$ i $B(x)$ són idèntitics si i només si $A(x)$ i $B(x)$ tenen el mateix grau i els coeficients dels monomis del mateix grau de cadascun dels polinomis són iguals. És evident que quan $x = y$ es vol significar que en tota proposició on aparegui x pot substituir-se per y si és necessari, i viceversa.
De la definició que hem donat s'obté de manera bastant evident que la relació d'igualtat compleix les tres propietats següents:

Reflexiva: Tot objecte és igual a si mateix: $x = x$.

Simètrica: Si $x = y$, llavors $y = x$.

Transitiva: Si $x = y$ i $y = z$, llavors $x = z$.

13 Demostracions

Entrem a la secció més important d'aquest document que són les demostracions a matemàtiques. És important ser conscients de les raons per les quals hem fet fins ara una petita introducció a la lògica. N'hi ha tres raons de molt significatives:

1. En primer lloc, les taules de veritat que hem estudiat ens indiquen els significats exactes de les paraules 'i', 'o', 'no', 'si ... llavors ...' i '... si i només si ...'. Per exemple, sempre que fem servir o llegim la construcció 'Si ..., llavors...' en un context matemàtic, la lògica ens indica exactament què es vol dir.

2. En segon lloc, les regles d'inferència proporcionen un camí pel qual podem construir nova informació (proposicions) a partir d'informació coneguda.

3. Finalment, les equivalències lògiques ens ajuden a canviar correctament certes proposicions en unes altres proposicions amb el mateix significat però molt més útils.

En resum, la lògica ens ajuda a entendre els significats dels enunciats i també a construir de nous. De fet és el llenguatge bàsic que ens permet escriure i comprendre bé els enunciats matemàtics. Però, malgrat el seu paper fonamental, el seu lloc queda en un segon pla. Els símbols $\wedge, \vee, \neg, \longrightarrow, \longleftrightarrow, \forall$ i $\exists$ poques vegades s'escriuen a la pissarra o en els llibres de text. Tot i això, hem de ser conscients dels seus significats constantment; quan llegim o escrivim una frase relacionada amb les matemàtiques, hem d'analitzar-la amb aquests símbols, sigui mentalment o sobre paper en brut, per tal d'entendre o comunicar bé el seu significat, que ha de ser sempre vertader i inequívoc.

A matemàtiques un raonament lògic és senzillament l'enunciat d'un teorema. La justificació que fa que un teorema sigui vàlid és la seva prova o demostració. Quan passem a la construcció de demostracions matemàtiques, ens centrem en el contingut matemàtic de les proposicions implicades en la prova i no ens referim explícitament a les regles d'inferència lògica discutides en les seccions anteriors; fer-ho seria una distracció de les qüestions matemàtiques. Tampoc utilitzem la notació lògica de les seccions anteriors. Tot i això, farem servir les regles d'inferència de manera implícita tot el temps, no oblidem que és el marc sobre el qual es basa tot.
Sovint passa que la nostra intuïció ens indica el que és important, el què creiem que pot ser cert, el què hem de provar després i més coses. Desafortunadament, els objectes matemàtics solen ser tan complicats o abstractes que la nostra intuïció fal-la. Per això construïm demostracions, per verificar que una afirmació determinada que ens sembla intuïtivament certa és realment certa, només així podem avançar a matemàtiques. Finalment, afegir també que ens interessa aprendre a fer demostracions perquè ens ajuda a entendre les nocions o fets relacionats amb el resultat que es vol demostrar.

Quan es té l'enunciat d'un teorema, primer s'ha de comprendre el que significa, segon s'ha de saber escriure amb rigor (seguint el llenguatge de la lògica) i finalment, amb l'ajut d'altres nocions, proposicions o teoremes, s'ha d'explorar els possibles camins per portar a terme la seva demostració. Per construir la prova, el primer que cal fer és especificar en rigor el què se suposa que es compleix, que anomenem les **hipòtesis,** i després el què s'intenta demostrar, que se'n diu **tesi**. A continuació, s'ha d'escollir una estratègia per a la prova. La següent etapa és obtenir la prova, fent ús de l'estratègia escollida. Si no es pot idear una prova amb l'estratègia escollida, potser s'hauria d'intentar una altra. No hi ha una manera fixa de trobar la prova; sempre requereix experimentar, jugar i provar coses diferents.

En els apartats següents tractarem les més importants.

13.1 Demostracions directes

Molts teoremes tenen la forma $A \Longrightarrow B$. El camí més senzill per provar $A \Longrightarrow B$ és fer-ho directament: suposem que A és vertadera i hem d'arribar a deduïr B mitjançant una seqüència de passos que comença en A i acaba en B. Aquest tipus de prova es diu **prova directa** per distinguir-la d'altres mètodes de demostració.

Exemple 11. Reformuleu simbòlicament cadascun dels teoremes següents en la forma $A \longrightarrow B$.

1. L'àrea d'un cercle de radi r és πr^2.

2. Donada una recta r i un punt P que no és de r, hi ha exactament una recta s que passa pel punt P i és paral·lela a r.

3. En tot triangle ABC, els costats del qual són a, b i c, llavors es compleix
$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}.$$

4. $e^x \cdot e^y = e^{x+y}$.

Solució: (1) Si $C(r) =$"C és un cercle del pla de radi r" i $A(x) =$" àrea de la figura x", aleshores es té $\forall r\,(C(r) \longrightarrow A(C(r)) = \pi r^2)$. De fet, si $r > 0$, aleshores $C(r) = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = r^2\}$.
(2) Si $R(x) =$"és una recta del pla", $P(x) =$"és un punt del pla" i $x \parallel y =$"x és paral·lel a y", aleshores
$$\forall x, y\,(R(x) \wedge P(y) \longrightarrow \exists z\,(R(z) \wedge y \in z \wedge z \parallel x))$$
(3) Si $T(x, y, z) =$"T és un triangle del pla de costats x, y, z" i $A(x) =$"angle oposat al costat x del triangle T". Aleshores
$$\forall x, y, z \left(T(x, y, z) \longrightarrow \frac{x}{\sin A(x)} = \frac{y}{\sin A(y)} = \frac{z}{\sin A(z)} \right).$$
De fet, $T(x, y, z) = \{(x, y, z) \in \mathbb{R}^3 : x \leq y + z\}$.
(4) $\forall x, y\,(x, y \in \mathbb{R} \longrightarrow e^x \cdot e^y = e^{x+y})$. □

Exemple 12. Considerem tres nombres enters qualssevol a, b i c. Si a divideix b i b divideix c, prova que a divideix c.

Solució: Primer observem que a l'enunciat hi apareix un predicat "x divideix y", que simbolitzem per $x \mid y$. La seva definició és: $x \mid y$ sii (abreujatura de "si i només si") existeix $k \in \mathbb{Z}$ tal que $kx = y$. Ara hem d'escollir una estrategia per la prova. En aquest escollim la prova directa: suposem que $a \mid b$ i $b \mid c$ (hipotèsis) i tenim que veure que $a \mid c$ (tesi).
Si $a \mid b$ i $b \mid c$, llavors existeixen $k_1, k_2 \in \mathbb{Z}$ tals que $k_1 a = b$ i $k_2 b = c$. D'aquí, per substitució es té: $k_2\,(k_1 a) = (k_1 k_2)\,a = c$. Per tant, existeix $k = k_1 k_2 \in \mathbb{Z}$ tal que $ka = c$ i, com a conseqüència, $a \mid c$. □

Exemple 13. Provar que per a qualssevol nombres positius x i y es compleix que la mitja aritmètica és més gran que la mitja geomètrica.

Solució: Primer observem que a l'enunciat hi apareixen dos conceptes: mitja aritmètica i geomètrica de dos nombres positius. La mitja aritmètica i geomètrica de x i y són respectivament: $\sqrt{xy}$ i $\dfrac{x+y}{2}$. Escollim una prova directa: com hipòtesi suposem $x, y \geq 0$, tenim que veure $\sqrt{xy} \leq \dfrac{x+y}{2}$ (tesi).
Si $x, y \geq 0$ aleshores $\sqrt{x}$ i $\sqrt{y}$ existeixen. És evident que $(\sqrt{x} - \sqrt{y})^2 \geq 0$. Desemvolupant aquesta última expressió i passant l'arrel quadrada a l'altre costat de la desigualtat, es té

$$\begin{aligned} x - 2\sqrt{xy} + y &\geq 0 \\ x + y &\geq 2\sqrt{xy} \end{aligned}$$

Finalment, dividind tots dos costats per 2, es té el resultat que voliem:

$$\frac{x+y}{2} \geq \sqrt{xy}.$$

□

13.2 Demostracions cap enrere

Un altre mètode de construir una demostració és treballant mentalment des de la tesi cap a les hipòtesis. Es diu **prova pensada cap enrere** per distingir-la de les demés. Tot i això, la prova finalment es construeix de forma directa. Mirem-ho construïnt la prova cap enrere de la següent proposició:

Exemple 14. Provar que per a qualssevol nombres reals x, y i $x < y$, es té que $4xy < (x+y)^2$.

Solució: L'hipòtesi és $x, y \in \mathbb{R}$ i $x < y$, i la tesi, $4xy < (x+y)^2$. La prova cap enrere surt de la tesi, i, per tant, podem fer es següent:

$$\begin{aligned} 4xy &< (x+y)^2 \\ 4xy &< x^2 + 2xy + y^2 \\ 0 &< x^2 - 2xy + y^2 \\ 0 &< (x-y)^2 \end{aligned}$$

De la última desigüaltat, s'obté $x - y \neq 0$ i, per tant, $x \neq y$. En particular, $x < y$. De fet, això que hem escrit s'havia d'haver pensat mentalment perquè la demostració real és una prova directa: Si $x < y$, llavors $x \neq y$ i, per tant, $x - y \neq 0$. D'aquí, es té $(x-y)^2 > 0$ i, per tant, $x^2 - 2xy + y^2 > 0$. Sumant a tots dos costats $4xy$ es té: $x^2 + 2xy + y^2 > 4xy$ i, per tant, $(x+y)^2 > 4xy$, com voliem demostrar. □

13.3 Demostracions per contrarecíproc

Recordem que el contrarecíproc de $A \longrightarrow B$ és $\neg B \longrightarrow \neg A$, i també l'equivalència lògica $(A \longrightarrow B) \longleftrightarrow (\neg B \longrightarrow \neg A)$, anomenada llei del contrarecíproc. Per això, si volem provar $A \longrightarrow B$, podem fer-ho de manera equivalent, construïnt una prova directa de $\neg B \longrightarrow \neg A$. L'estratègia és doncs pendre com hipòtesi que B és falsa i hem d'arribar a que A és també falsa (tesi). Aquest tipus de demostració es diu **prova per contrarecíproc**. Veiem-ho amb un exemple:

Exemple 15. Provar que per a qualsevol nombre enter n, si n^2 és parell, llavors n és parell.

Solució: Volem constuir una prova per contrarecíproc. Aleshores, les hipòtesis són que $n \in \mathbb{Z}$ i n no és parell. La tesi és que n^2 no és parell. Si n no és parell, n és senar i, per tant, existeix $k \in \mathbb{Z}$ i $n = 2k + 1$. Hem de veure que n^2 també és senar. En efecte, com $n = 2k + 1$, aleshores $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2\,(2k^2 + 2k) + 1$ i com $2k^2 + 2k \in \mathbb{Z}$, s'obté que n^2 és senar, com voliem demostrar. $\square$

13.4 Demostracions reducció a l'absurd

El principi del tercer no exclòs permet afirmar que una proposició o es vertadera o bé falsa. Aquest principi és la base del següent mètode de demostració. En concret, si volem demostrar que una proposició p és certa, aquest mètode proposar suposar el contrari, o sigui que $\neg p$ és certa, i llavors per regles d'inferència hem d'arribar a una contradicció com per exemple $q \wedge \neg q$, on q és una proposició qualsevol, per poder concluir que la suposició que A és falsa no és possible i, en conseqüència, A és certa.
A matemàtiques els teoremes tenen la forma $A \longrightarrow B$ i, per tant, hem d'adaptar el raonament anterior a aquest cas. Recordem l'equivalència lògica $\neg\,(A \longrightarrow B) \longleftrightarrow A \wedge \neg B$. Per tant, si volem construir una demostració de $A \longrightarrow B$, hem de suposar que $\neg\,(A \longrightarrow B)$ és certa. Això és equivalent a suposar que $A \wedge \neg B$ és certa, o sigui que A és certa i B és falsa i d'aquí hem de provar que s'arriba a una contradicció. Una vegada s'ha arribat a la contradicció, concluïm que $A \wedge \neg B$ és falsa i, per tant, $A \longrightarrow B$ és vertadera.
Aquest mètode de demostració es coneix com a **prova per reducció a l'absurd**. L'hipòtesi és $A \wedge \neg B$ i la tesi és una contradicció o absurd.

Exemple 16. Volem provar que $\sqrt{2}$ és un nombre irracional.

Solució: En primer lloc observem que l'enunciat no és un condicional. Però, recordem la definició de un nombre racional diferent de zero: $a \neq 0$ és racional sii existeixen enters no nuls m, n tals que $a = \dfrac{m}{n}$. Llavors, podem reformular l'enunciat com volem. En efecte, l'enunciat "$\sqrt{2}$ és un nombre irracional"és equivalent a la proposició següent escrita simbòlicament

$$(\forall m, n \in \mathbb{Z}) \left(n \neq 0 \wedge m \neq 0 \wedge \frac{m}{n} \neq \sqrt{2}\right).$$

Per demostrar aquesta proposició universal, considerem dos nombre enters no nuls m, n. Hem demostrar que no és possible que $\dfrac{m}{n} = \sqrt{2}$. L'estratègia serà fer la prova

per reducció a l'absurd: suposem m i n són enters no nuls i que $\dfrac{m}{n} = \sqrt{2}$ (hipòtesi), hem de trobar un contradicció (tesi). No és restrictiu suposar que la fracció $\dfrac{m}{n}$ és irreductible; cas contrari, escriuríem la fracció irreductible equivalent. Si $\dfrac{m}{n} = \sqrt{2}$, aleshores $m = \sqrt{2}n$ i, per tant, $m^2 = 2n^2$. D'aquí, deduïm que m^2 és un enter parell. Llavors m és parell com hem provat en l'exemple 15. Llavors, $m = 2k$, on $k \in \mathbb{Z}$. D'aquí, $m^2 = 4k^2 = 2n^2$ i, per tant, $n^2 = 2k^2$. Deduïm que n^2 és parell i, per tant, n també. Però, això és una contradicció perquè aleshores la fracció $\dfrac{m}{n}$ és reductible. En conseqüència, no és possible que $\dfrac{m}{n} = \sqrt{2}$, i, com m i n son arbitraris, $\sqrt{2}$ no és racional.
Aquí volem fer èmfasi en el fet següent: Hem pogut reformular l'enunciat pensant lògicament i això a part d'entendre millor l'enunciat ens ha permès fer una demostració per reducció a l'absurd. $\square$

Exemple 17. Volem provar que no existeix cap nombre real x tal que $x^2 + 1 = 0$.

Solució: Primer, escribim simbòlicament l'enunciat: $\neg\,(\exists x \in \mathbb{R})\,(x^2 + 1 = 0)$. Veiem que és la negació d'una proposició existencial. Fent ús de la següent equivalència lògica

$$\neg\,(\exists x \in \mathbb{R})\,\big(x^2 + 1 = 0\big) \iff (\forall x \in \mathbb{R})\,\big(x^2 + 1 \neq 0\big)\,,$$

i de la regla d'inferència IQU:

$$\begin{array}{l} P(b) \\ \hline (\forall x \in U)\,P(x) \end{array}\,,$$

llavors només cal provar que prenent un nombre real qualsevol b, es compleix que $b^2+1 \neq 0$. Però, això és immediat perquè $b^2 \geq 0$ i, per tant, $b^2+1 \geq 1$; en particular, $b^2 + 1 \neq 0$. $\square$

13.5 Demostracions per contraexemple

A matemàtiques també trobem enunciats amb quantificadors que rebutjant propietats. Però, de fet rebutjar una propietat enunciada per una proposició 'p' és el mateix que provar '$\neg p$'. Per exemple, per demostrar que no és el cas que $(\forall x \in U)\,P(x)$, primer cal pensar en la següent equivalència lògica:

$$\neg\,(\forall x \in U, P(x)) \iff \exists x \in U, \neg P\,(x)$$

i després recordar la regla d'inferencia IQE:

$$\begin{array}{l} \neg P(d) \\ \hline (\exists x \in U)\,\neg P(x) \end{array}\,.$$

Llavors, només cal trobar un exemple pel qual $P(x)$ és fals. Aquesta manera de fer la demostració és coneix com **prova per contraexemple**.

Exemple 18. Volem provar que no és veritat que la suma de dos nombres irracionals és irracional.

Solució: Per buscar una estratègia, primer haurem de reformular l'enunciat lògicament: si $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ és el conjunt dels nombres irracionals, aleshores

$$\neg\, (\forall x, y \in \mathbb{I})\, (x + y \in \mathbb{I})$$

Hem vist que aquest enunciat és equivalent al següent:

$$(\exists x, y \in \mathbb{I})\, (x + y \notin \mathbb{I})$$

Per tant, per demostrar l'enunciat només cal trobar dos nombres irracionals la suma dels quals no és irracional. □

13.6 Demostracions per casos

A vegades trobem enunciats que són de la forma $(C \vee D) \longrightarrow B$, és a dir, que inclouen una disjunció en l'antecedent. En aquests casos, la següent equivalència

$$(C \vee D) \longrightarrow B \iff (C \longrightarrow B) \wedge (D \longrightarrow B)\,,$$

proporciona l'estratègia que hem de seguir. En efecte, per demostrar que $(C \vee D) \longrightarrow B$ és certa és suficient demostrar que $C \longrightarrow B$ i $D \longrightarrow B$ són ambdues certes. De fet, la demostració la construïm per casos (en aquest cas, n'hi ha dos casos) segons la forma que tingui l'antecedent. La demostració de cadascun dels casos seguirà l'estratègia que faci falta. Aquest mètode de demostració es coneix com **prova per casos**.

Exemple 19. Volem provar que si n és un nombre enter, llavors $n^2 + n$ és parell.

Solució: Sabem que tot nombre enter n és o parell o bé senar. Aquesta idea proporciona l'estratègia de la demostració: construïr una prova per casos. Volem provar que (1) si n és parell, aleshores $n^2 + n$ és parell, i (2) si n és senar, aleshores $n^2 + n$ és senar.

Cas 1: Si n és parell, llavors per definició existeix $k \in \mathbb{Z}$ tal que $n = 2k$. Aleshores es té:

$$n^2 + n = 4k^2 + 2k = 2\left(2k^2 + k\right),$$

i, per tant, $n^2 + n$ és parell perquè $2k^2 + k \in \mathbb{Z}$.

Cas 2: Si n és senar, llavors per definició existeix $m \in \mathbb{Z}$ tal que $n = 2m + 1$. Aleshores es té:

$$\begin{aligned} n^2 + n &= (2m+1)^2 + 2m + 1 \\ &= 4m^2 + 6m + 2 = 2\left(2m^2 + 3m + 1\right), \end{aligned}$$

i, per tant, $n^2 + n$ és parell perquè $2m^2 + 3m + 1 \in \mathbb{Z}$.

□

Ara passem als teoremes de la forma $A \longrightarrow (C \vee D)$ on hi trobem una disjuntiva en el conseqüent. Una estratègia per a fer la demostració és fent ús primer de la llei del contrarecíproc i després una de les lleis de De Morgan:

$$\begin{aligned} A \longrightarrow (C \vee D) &\iff \neg\,(C \vee D) \longrightarrow \neg A \\ &\iff (\neg C \wedge \neg D) \longrightarrow \neg A \end{aligned}$$

A partir d'aquí, construïm la prova directa o per reducció al absurd. Veiem-ho en un exemple.

Exercici 1. Considerem dos nombres reals x i y. Volem provar que si xy és irracional, llavors x o y és irracional.

Solució: Segons el que hem vist anteriorment, aquest enunciat és equivalent al següent: Si x és racional i y també ho és, llavors xy és racional. Però això és evident perquè sabem que la multiplicació és una operación interna del cos dels racionals. $\square$

Després d'haver discutit sobre l'aparició de la connectiva $\vee$, anem ara a tractar els casos quan aprareix la connectiva $\wedge$ en els teoremes de la forma $A \longrightarrow B$. Per demostar un enunciat de la forma $A \longrightarrow (C \wedge D)$ fem ús de l'equivalència següent:

$$A \longrightarrow (C \wedge D) \Longleftrightarrow (A \longrightarrow C) \wedge (A \longrightarrow D)$$

A partir d'aquí, la demostració consisteix en provar que $A \longrightarrow C$ i $A \longrightarrow D$ són certes.
Si l'enunciat és de la forma $(C \wedge D) \longrightarrow B$, llavors l'estratègia és prendre com hipòtesis que C i D són certes i com a tesi que B és certa. La prova pot ser directe o per reducció a l'aburd.
Finalment, volem tractar una altra forma lògica que presenten molts teoremes. Són els teoremes de la forma $A \longleftrightarrow B$ i que ens donen condicions necessàries i suficients. La llei del bicondicional ens dona la resposta per construir proves d'aquest teoremes:

$$A \longleftrightarrow B \Longleftrightarrow (A \longrightarrow B) \wedge (B \longrightarrow A)\,.$$

Per tant, és suficient provar $A \longrightarrow B$ i $B \longrightarrow A$, cadascun dels quals es pot demostrar mitjançant qualsevol dels mètodes que hem vist fins ara.

Exemple 20. Volem provar que si x i y son dos nombres reals, llavors $xy = 0$ sii $x = 0$ o $y = 0$.

Solució: L'enunciat expressat formalment és:

$$(\forall x, y \in \mathbb{R})\,(xy = 0 \longleftrightarrow x = 0 \vee y = 0)\,.$$

Per tant, si x, y són nombres reals arbitraris, hem de demostrar $xy = 0 \longleftrightarrow x = 0 \vee y = 0$. Segons hem dit abans, això és equivalent a demostrar cadascun del teoremes següents: (1) $xy = 0 \longrightarrow x = 0 \vee y = 0$ i (2) $x = 0 \vee y = 0 \longrightarrow xy = 0$.
(1) Demostrem que la condició necessària perquè $xy = 0$ és $x = 0$ o $y = 0$. Això és equivalent a provar que si $x \neq 0$ i $y \neq 0$ aleshores $xy \neq 0$. No és restrictiu suposar que $x \leq y$; cas contrari, faríem que $x > y$ i la prova es contrueix de forma anàloga. Ara l'estratègia és fer la demostració per casos: si $x \neq 0$, llavors o $x > 0$ o bé $x < 0$.

Cas 1: Si $0 < x \leq y$, llavors $xy > 0$ i, per tant, $xy \neq 0$.

Cas 2: Si $x < 0$ i $y \geq x$, llavors apareixen dos subcasos: (2.1) $x < 0$ i $y > 0$ (2.2) $x < 0$ i $y < 0$ i $y \geq x$.

Subcas 2.1: Si $x < 0$ i $y > 0$, llavors $xy < 0$ i, per tant, $xy \neq 0$.

Subcas 2.2: Si $x < 0$ i $y < 0$ i $y \geq x$, llavors $xy > 0$ i, per tant, $xy \neq 0$.

Com a conseqüència, concluïm el que volíem demostrar.
(2) Demostrem que la condició suficient perquè $xy = 0$ és que $x = 0$ o $y = 0$. Això és evident perquè si $x = 0$ aleshores $0 \cdot y = 0$ i si $y = 0$, $x \cdot 0 = 0$. $\square$

13.7 Demostracions d'existència i unicitat

És molt freqüent trobar demostracions que impliquin l'existència d'un objecte que compleix una determinada propietat i també la seva unicitat. Quant a la prova d'existència només cal trobar l'objecte en concret que compleix la propietat. Quant a la unicitat, l'estratègia més comuna és suposar que x i y són dos objectes que satisfan la propietat donada, llavors hem de demostrar que $x = y$.

Exemple 21. Volem provar que la proporció entre dos nombres reals a i b, $a > b > 0$, que compleixen la propietat

$$\frac{a}{b} = \frac{a+b}{a}$$

és un nombre irracional i a més és únic.

Solució: Primer hem de provar l'existència, buscant aquest nombre que representa la proporció donada. Suposem que existeix, aleshores es compleix

$$\frac{a}{b} = \frac{a+b}{a} \Longleftrightarrow \frac{a}{b} = \frac{\frac{a}{b}+1}{\frac{a}{b}}$$

Fent que $\frac{a}{b} = x$, llavors tenim

$$x = \frac{x+1}{x} \Longleftrightarrow x^2 - x - 1 = 0$$

i, resolent l'equació de segon grau i sabent que $x > 0$, es té la solució

$$\Phi = \frac{1}{2}\left(1+\sqrt{5}\right)$$

Ara, hem de veure que Φ és irracional. Considerem el conjunt $A = \Big\{a \in \mathbb{N}\colon\ \exists b \in \mathbb{N}$ i $a > b > 0$ i $\Phi =$
$A = \emptyset$, llavors Φ és irracional. Suposem ara que no és el vuit. Aleshores, com A és un subconjunt de $\mathbb{N}$, A té primer element, que denotem per m. Llavors es té $\Phi = \frac{m}{b}$ i $m > b > 0$, per tant, $m + b > m$ i

$$\frac{m}{b} < \frac{m+b}{b}$$

però, això és una contradicció perquè

$$\frac{m}{b} = \frac{m+b}{b} = \Phi.$$

Deduïm que Φ és irracional.
Finalment, hem de demostrar la unicitat. Suposem que Φ_1 i Φ_2 compleixen la propietat. Llavors, de (13.8) es té

$$\begin{aligned}
\Phi_1^2 - \Phi_1 - 1 &= \Phi_2^2 - \Phi_2 - 1 \\
\Phi_1^2 - \Phi_2^2 - \Phi_1 + \Phi_2 &= 0 \\
(\Phi_1 - \Phi_2)(\Phi_1 + \Phi_2 - 1) &= 0
\end{aligned}$$

i, per tant, $\Phi_1 - \Phi_2 = 0$ o $\Phi_1 + \Phi_2 - 1 = 0$ però, $\Phi_1 + \Phi_2 > 1$ perquè $a > b > 0$. Per tant, $\Phi_1 = \Phi_2$. $\square$

13.8 Demostracions per inducció

La inducció matemàtica és una tècnica útil per demostrar enunciats sobre nombres naturals. Considerem, per exemple, l'enunciat següent: "Si n és parell, llavors n^2 és divisible per 4". Volem provar que aquest enunciat és correcte. Com ho fem? Aplicant inducció sobre n, que vol dir provar els dos passos següents:

1. Primer hem de provar que la propietat és vertadera pel primer element. En aquest cas el primer element és 2 perquè tractem amb nombres naturals parells. La propietat es certa perquè $2^2 = 4$ que és divisible per 4.

2. Per a tot nombre natural n (no sabem quin és), si la propietat és certa per n, llavors hem de provar que també ho és per el següent element: Suposem n és parell i que n^2 és divisible per 4, aleshores hem de provar que el següent parell $(n+2)^2$ és divisible per 4. En efecte, $(n+2)^2 = n^2 + 4n + 4 = 4k + 4n + 4 = 4(k + n + 1)$, on $n^2 = 4k$ i $k \in \mathbb{N}$.

Concluïm que la propietat és vàlida per a tot nombre natural parell.
Intuïtivament, aquestes dues condicions permeten assegurar que la propietat es compleix per tots els naturals. En efecte, $P(2)$ és vertadera, $P(2) \longrightarrow P(4)$ és vertadera i, per tant, $P(4)$ també ho és; $P(4) \longrightarrow P(6)$ és certa i, per tant, $P(6)$ també. I així succesivament.

La base d'aquest mètode de demostració és el principi d'inducció que, de fet és un dels axiomes que defineixen els nombres naturals. Aquest principi diu: Si $P(n)$ és un enunciat sobre els naturals i es compleixen les dues condicions següents: A la primera part, anomenada **cas base**, mostrem que $P(1)$ és es compleix (el primer element no necessàriament és 1, depèn de cada cas). A la segona part, anomenada pas inductiu, suposem que n és un natural tal que $P(n)$ és certa, tot i que no sabem què és n, i hem de deduïr que $P(n + 1)$ és certa. La suposició que $P(n)$ és vertadera es diu **hipòtesi d'inducció**. La conclusió d'aquest raonament és que $P(n)$ és vàlida per a tot n natural. Aquest mètode de demostració es coneix com **prova per inducció** sobre n.

Veiem en detall aquest mètode en un exemple:

Exemple 22. Volem demostrar que per a tot n natural es compleix

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Solució: Construïm una prova d'inducció sobre n, sent $P(n) =$ '$1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$'.

Cas base: $P(1)$ és $1 = \frac{1(1+1)}{2}$ i, evidentment és veritat.

Hipòtesi d'inducció: Suposem que $P(n)$ és certa, o sigui que $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Tesi: Hem de demostrar que $P(n+1) =$'$1 + 2 + \cdots + n = \dfrac{(n+1)(n+2)}{2}$' és certa.

En efecte, aplicant l'hipòtesi d'inducció, es té

$$\begin{aligned} 1+2+\cdots+n+n+1 &= \frac{n(n+1)}{2}+n+1 \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

que és el que volíem veure.

Conclusió: Pel principi d'inducció sobre n, deduïm que $P(n)$ és certa per a tot $n \in \mathbb{N}$.

□

Exemple 23. Volem demostrar que per a tot nombre natural n es compleix que $8^n - 3^n$ és divisible per 5.

Solució: El cas base és per $n = 1$: $8-3 = 5$ que és divisible per 5. Suposem ara que per a tot nombre natural n es té que $8^n - 3^n$ és divisible per 5 (hipòtesi d'inducció), hem de demostrar que $8^{n+1} - 3^{n+1}$ també és divisible per 5. En efecte, tenim

$$\begin{aligned} 8^{n+1} - 3^{n+1} &= 8 \cdot 8^n - 3 \cdot 3^n \\ &= 8 \cdot 8^n - (8-5) \cdot 3^n \\ &= 8 \cdot (8^n - 3^n) + 5 \cdot 3^n \end{aligned}$$

però, per hipòtesi d'inducció, $8^n - 3^n = 5k$, sent $k \in \mathbb{N}$. Per tant,

$$8^{n+1} - 3^{n+1} = 5 \cdot (8k + 3^n)$$

i, d'aquí, s'obté que $8^{n+1} - 3^{n+1}$ és divisible per 5 perquè $8k + 3^n \in \mathbb{N}$. Com a conseqüència, $8^n - 3^n$ és divisible per 5 per a tot nombre natural n. □

Les definicions **inductives** estan implícites en les definicions de diverses funcions molt comuns que impliquen nombres enters no negatius. Per exemple, el factorial d'un nombre enter no negatiu n, designat per $n!$, es defineix inductivament d'aquesta manera:

- $0! = 1$;
- $(n+1)! = (n+1) \cdot n!$.

Un altre exemple son les definicions per **recursió**. La successió de Fibonacci és un bon exemple: $1, 1, 2, 3, 5, 8, 13, ...$, que podem definir per recursió d'aquesta manera:

- $u_1 = 1$,
- $u_2 = 1$,
- $u_{k+1} = u_{k-1} + u_k$ per $k \in \mathbb{N}$ i $k \geq 2$.

14 Teories axiomàtiques

Resulta que, per demostrar alguna cosa, es necessita el coneixement d'algunes veritats anteriors. La lògica només proporciona les maneres que podem deduir una afirmació d'altres, però necessitem algunes afirmacions per començar. Aquestes afirmacions inicials s'anomenen **axiomes** o **postulats** d'ençà que Euclides va escriure els seus Elements cap al 300 aC. Per exemple, el primer postulat d'Euclides diu 'donats dos punts, existeix una única línea recta que passa per ells', enunciat que la majoria de la gent considera evident. Tot i això, en l'enfocament axiomàtic modern els axiomes no es veuen necessàriament com a veritats evidents per si mateixos, sinó simplement com a afirmacions que suposem que són certes. Fem matemàtiques explorant el que es deriva de la veritat d'aquests axiomes mitjançant les regles de deducció de la lògica.

Les matemàtiques modernes es basen en la teoria de conjunts i la lògica. La majoria dels objectes matemàtics, com ara punts, línies, nombres, funcions, successions, grups, etc., són realment conjunts. Per tant, és necessari començar a coneixer els axiomes de la teoria de conjunts. Aquí no tractarem aquest punt però es pot trobar en qualsevol text de teoria de conjunts de nivell avançat.
A més, tenim els axiomes que defineixen cadascuna de les teories. Per exemple, com hem comentat abans, en geometria euclidiana tenim l'axioma que afirma que existeix una i només una recta que passa per dos punts diferents. En les matemàtiques modernes no té cap sentit discutir aquest axioma. Si no s'assumeix, simplement no podem anomenar al objectes amb els noms 'línia recta' i 'punt'. Els axiomes serveixen aquí com a definicions que caracteritzen aquest sistema matemàtic. De fet, una teoria matemàtica és com un joc d'escacs i els axiomes corresponen a les regles del joc. Si no accepteu una regla, el joc deixa de ser escacs i és un altre cosa.

Les matemàtiques s'ocupen de sistemes abstractes de diversos tipus, definits cadascun per un conjunt adequat d'axiomes, que serveixen per caracteritzar la seva estructura. Però tot i que, des del punt de vista de les matemàtiques pures, cada estructura es considera autònoma, l'esquema matemàtic sol tenir una o més realitzacions concretes; és a dir, l'estructura sol trobar-se (possiblement només fins a un cert grau d'aproximació) en un sistema més concret. La geometria euclidiana abstracta de tres dimensions, per exemple, té una de les seves realitzacions l'estructura de l'espai ordinari.

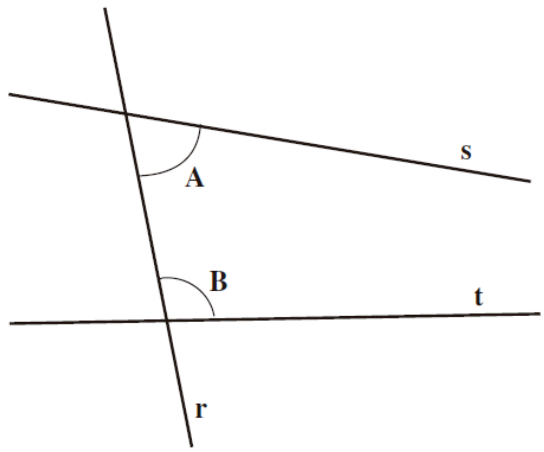
Per acabar aquest document presentem dues teories axiomàtiques clàssiques de les matemàtiques.

14.1 Teoria axiomàtica de la geometria plana

La geometria euclidiana plana es pot considerar com el conjunt de resultats que s'obtenen a partir dels cinc postulats d'Euclides per deducció lògica. Com es pot observar de seguida, els postulats d'Euclides estan pensats per fer geometria en el pla fent ús de la regla i el compàs. Aquests postulats són:

1. Es pot traçar una línia recta entre dos punts qualsevol i el resultat és un segment de línia recta.

2. Qualsevol segment de línia recta es pot ampliar indefinidament.
3. Donat un punt i un segment de línia de recta que comencen pel punt, podeu dibuixar un cercle centrat en el punt donat amb el segment de línia donat com a radi.
4. Tots els angles rectes són iguals.
5. Si dues rectes en un pla es troben amb una altra recta i si la suma dels angles interns d'un costat és inferior a dos angles rectes, les rectes es reuniran si s'estenen prou al costat on es suma la suma dels angles és inferior a dos angles rectes.

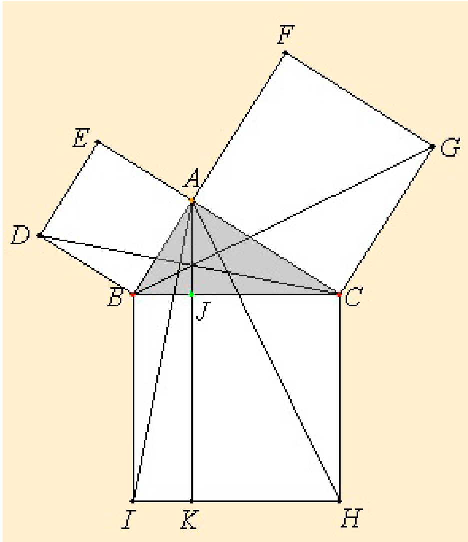


El cinquè axioma és conegut com l'**axioma de les paral·leles** quan és reformulat d'aquesta manera: 'Donada qualsevol recta i un punt que no estigui sobre aquesta recta, existeix una única recta que passa pel punt i és paral·lela a la recta donada'. De fet, la geometria clàssica euclidiana es distingeix per aquest axioma. Si no acceptem aquest resultat, surt per exemple l'**axioma de Lobachevsky**: Donada una recta i un punt exterior a ella, existeixen almenys dues rectes que passen per aquest punt i que no tallen la recta donada. La geometria caracteritzada pels quatre primers postulats d'Euclides i l'axioma de Lobachevsky distingeix la geometria anomenada hiperbòlica.

Per completar aquest apartat provarem el teorema de Pitàgores:

Teorema 1 (Teorema de Pitàgores)**.** *En tots els triangles rectangles es compleix que el quadrat del costat oposat a l'angle recte és igual a la suma dels quadrats dels costats que comprenen a l'angle recte.*

Demostració: En efecte, considerem un triangle rectangle qualsevol ABC, on hi suposem l'angle $\angle BAC$ recte. Podem construir un quadrat sobre cada segment del triangle, i obtenir d'aquesta manera una construcció com la de la figura següent.



Observem primer que els triangles DCB i ABI són iguals, perquè $AB = BD$, $BI = BC$ i $\angle DBC = \angle ABI$. Llavors, l'àrea del quadrat $ABDE$ és el doble de l'àrea del triangle DCB, perquè les dues figures tenen la mateixa base i es troben entre les mateixes paral·leles. Per la mateixa raó l'àrea del rectangle $BIJK$ és el doble de l'àrea del triangle ABI. D'aquestes dues conclusions, obtenim que l'àrea del rectangle $BIJK$ és igual que l'àrea del quadrat $ABDE$. Anàlogament, s'obté que l'àrea del rectangle $CHKJ$ és igual que l'àrea del quadrat $ACGF$. Per tant, com l'àrea del quadrat $BIHC$ és igual a la suma de les àrees dels rectangles $BIKJ$ i $CHKJ$, per les igualtats demostrades tenim que l'àrea del quadrat $BIHC$ de catet oposat a l'angle recte, és igual a la suma de les àrees dels quadrats $ABDE$ i $ACGF$, que tenen per catets els segments que comprenen l'angle recte. $\square$

14.2 Teoria axiomàtica de l'aritmètica

A partir dels postulats de Peano, és possible demostrar totes les propietats esperades dels nombres naturals i, a partir del nombres naturals, és possible construir primer els enters, després els nombres racionals i després els nombres reals. El conjunt dels nombres naturals és el conjunt $\mathbb{N}$, l'existència del qual ve donada per als postulats de Peano que són:

1. Existeix un element 1 que pertany al conjunt dels nombres naturals $\mathbb{N}$.
2. Existeix una funció $s : \mathbb{N} \longrightarrow \mathbb{N}$ tal que compleix les propietats següents:
   (a) No hi ha cap nombre natural n tal que $s(n) = 1$.
   (b) Per a tots $m, n \in N$, si $s(m) = s(n)$, llavors $m = n$.
   (c) Per a cada subconjunt $K \subseteq \mathbb{N}$, si $1 \in K$ i per a cada nombre natural $n \in K$ es té que $s(n) \in K$, llavors tot nombre natural és de K.

Si pensem intuïtivament en la funció s com la que assigna a cada nombre natural el seu **següent**, llavors la part (a) dels postulats diu que 1 és el **primer element** o número en $\mathbb{N}$, perquè no és el successor de res. També es diu que $\mathbb{N}$ és un **conjunt ben ordenat**. La part (c) es coneix com a principi d'inducció i constitueix la base de les demostracions per inducció que hem tractat en l'apartat 13.8.

La pregunta que ens fem de seguida és com sabem que hi ha un conjunt i un element del conjunt i una funció del conjunt en si mateix, que satisfan els postulats de Peano? La resposta no la tractarem aquí. Com hem assenyalat més amunt la teoria de conjunts és la base de les matemàtiques modernes, llavors no és necessari suposar addicionalment que els postulats de Peano es compleixen, perquè l'existència d'alguna cosa que compleixi els postulats de Peano es pot deduir dels axiomes de la teoria de conjunts.

Per a completar aquest apartat proposem demostrar una propietat característica del conjunt dels nombres naturals: tot subconjunt K no vuit de $\mathbb{N}$ està ben ordenat, és a dir, que K té primer element.

Teorema 2. *Qualsevol conjunt no buit de nombres naturals té un primer element.*

Demostració: La demostració la farem per reducció a l'absurd utilitzant alhora el principi d'inducció: Considerem un conjunt no vuit de nombres naturals K sense cap primer element. Considerem la propietat que per a qualsevol n de K, n no és següent de cap nombre de K. Fem inducció sobre n. El cas base és $1 \notin K$, i això és evident, perquè K és un subconjunt de nombres naturals i 1 és el primer element de $\mathbb{N}$. La hipòtesi d'inducció és suposar que per a qualsevol n, no hi ha cap element de K del qual n sigui el seu següent. Hem de provar que això també es compleix per $n+1$. És clar que $n+1$ és el següent de n. Si $n \in K$, per hipòtesi d'inducció, n és el primer element, però això és contradictori amb el fet que K no té cap primer element. Per tant, $n+1 \notin K$, i en conseqüència $K = \mathbb{N}$, és a dir, K té primer element. $\square$