

Apunts de
FONAMENTS MATEMÀTICS
amb exercicis

Part 1

Rafel Farré

01/09/2023

- Els exercicis en color negre són per fer a les classes de teoria.
- Els exercicis en color blau són per fer a les classes de taller. Els marcats amb (R) són recomanats.
- Els exercicis en color verd està resolt al document *Exercicis Resolts*.

0. SUMATORIS

$$\sum_{i=m}^n f(i) = f(m) + f(m+1) + \dots + f(n-1) + f(n)$$

Exemples:

- $\sum_{i=1}^{100} i = 1 + 2 + 3 + \dots + 99 + 100.$
- $\sum_{i=-2}^{50} 2i = -4 - 2 + 0 + 2 + 4 + \dots + 98 + 100.$
- $\sum_{i=5}^{1000} i^2 = 5^2 + 6^2 + 7^2 + \dots + 999^2 + 1000^2.$
- $\sum_{i=1}^{30} (-1)^i (2i-1)^2 = -1^2 + 3^2 - 5^2 + \dots + 59^2.$

Exercicis: Passeu a notació amb sumatori:

1. $(R) -2 + 0 + 2 + 4 + 6 + \dots + 50.$
2. $3 + 5 + 7 + \dots + 55.$
3. $2 - 4 + 6 - \dots + 50.$
4. $-1^2 + 3^2 - 5^2 + 7^2 - \dots - 49^2.$
5. $(R) \frac{2}{1^3} + \frac{5}{5^3} + \frac{8}{9^3} + \frac{11}{13^3} + \dots + \frac{47}{61^3}.$
6. $-3 + 0 + 3 + 6 + 9 + 12 + \dots + 60.$
7. $1^3 - 4^3 + 7^3 - 10^3 + \dots + 61^3.$
8. $(R) \frac{1}{3} - \frac{1}{7} + \frac{1}{11} - \frac{1}{15} + \dots - \frac{1}{39}.$
9. $-\frac{2}{1} + \frac{4}{4^3} - \frac{6}{7^3} + \frac{8}{10^3} - \dots - \frac{42}{61^3}.$

Propietats dels sumatoris:

$\sum_{i=m}^n (f(i) + g(i)) = \sum_{i=m}^n f(i) + \sum_{i=m}^n g(i)$
$\sum_{i=m}^n c f(i) = c \sum_{i=m}^n f(i)$

Exercicis:

10. Expressen les sumes següents en funció de $S = \sum_{n=1}^{10} a_n$:

a. $\sum_{m=1}^{10} a_m$

b. $\sum_{i=0}^9 a_i$

c. $\sum_{j=1}^{10} a_{j-1}$

11. (R) Calculeu:

a. $\sum_{i=0}^{n+1} a_i - \sum_{i=0}^n a_i$

b. $\sum_{i=1}^{n+2} a_i - \sum_{i=1}^{n-1} a_i$

12. (R) Proveu que si $n \geq 0$ $\sum_{k=0}^{n+3} r^k - \sum_{k=0}^n r^k = r^n(r + r^2 + r^3)$.

13. Sabent que $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ i $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$,

a. (R) Calculeu $\sum_{k=1}^n (k + 3)^2$.

b. Calculeu $\sum_{i=1}^n \sum_{j=1}^n ij$.

14. Si $A = \sum_{i=n}^m a_i$ i $B = \sum_{i=n}^m b_i$, expresseu en funció de A i B :

a. $\sum_{i=n}^m 5a_i$

b. $\sum_{i=n}^m (a_i - b_i)$

c. (R) $\sum_{i=n}^m -3b_i$

d. (R) $\sum_{i=n}^m (2a_i + 4b_i)$

15. (R) Canvieu l'índex dels sumatoris següents perquè comencin en $j = 0$

(quedin de la forma $\sum_{j=0}$):

a. $\sum_{i=8}^n i^2$

b. $\sum_{i=-3}^{n+2} (2i + 3)$

16. Expresseu cada una de les sumes següents amb un sol sumatori:

a. $\sum_{k=1}^n (6k - 3) + \sum_{k=1}^n (4 - 5k)$

b. $\sum_{k=1}^n (4k - 1)^2 + \sum_{k=1}^n (4k + 1)^2$

c. $\sum_{k=1}^{100} (2k - 1)^2 + \sum_{k=0}^{99} (2k - 1)^2$

d. $\sum_{k=0}^{99} (2k + 1)^2 + \sum_{k=1}^{100} (3k - 2)^2$

Progressions aritmètiques

Cada terme a_{i+1} s'obté de l'anterior a_i sumant una quantitat d anomenada diferència:

$$a_{i+1} = a_i + d.$$

$$a_i = a_0 + id$$

Exemple: La successió $a_n = 5n - 3$ és una progressió aritmètica amb diferència $d = 5$

La suma d'una progressió aritmètica s'obté mitjançant la fórmula:

$$\sum_{i=m}^n a_i = \frac{(a_m + a_n)(n-m+1)}{2}$$

Observeu que $n - m + 1$ és el número de termes del sumatori.

Demostració: Ho fem primer pel cas en què el nombre de sumands és parell. Observem que la suma del primer més l'últim és igual que la del segon més el penúltim, que és igual que la del tercer més el antepenúltim Agrupant els sumands de dos en dos obtenim la fórmula, ja que només cal multiplicar $a_m + a_n$ per la meitat del nombre de sumands, que és $\frac{n-m+1}{2}$. Si el nombre de sumands $n - m + 1$ és senar, ens queda un terme desaparellat, que val $\frac{a_m + a_n}{2}$. La resta de sumands dona $\frac{(a_m + a_n)(n-m)}{2}$. Per tant la suma total en aquest cas s'obté amb la mateixa fórmula.

Progressions geomètriques

Cada terme a_{i+1} s'obté de l'anterior a_i multiplicant per una quantitat r anomenada

raó: $a_{i+1} = ra_i$.

$$a_i = a_0 r^i$$

Exemple: La successió $a_n = \frac{3}{4}2^n$ és una progressió geomètrica amb raó $r = 2$

La suma d'una progressió geomètrica amb $r \neq 1$ s'obté mitjançant la fórmula:

$$\sum_{i=m}^n a_i = \frac{a_{n+1} - a_m}{r-1}$$

Demostració:

Si multipliquem el sumatori per $r - 1$ obtenim:

$$\begin{aligned} \left(\sum_{i=m}^n a_i \right) (r - 1) &= (a_m + ra_m + \dots + r^{n-m} a_m) (r - 1) = \\ a_m (1 + r + \dots + r^{n-m}) (r - 1) &= a_m (r^{n-m+1} - 1) = a_{n+1} - a_m. \end{aligned}$$

Productoris

$$\prod_{i=m}^n f(i) = f(m) \cdot f(m+1) \cdots f(n-1) \cdot f(n)$$

Propietats dels productoris:

$\prod_{i=m}^n f(i) \cdot g(i) = \prod_{i=m}^n f(i) \cdot \prod_{i=m}^n g(i)$
$\prod_{i=m}^n f(i)^c = \left(\prod_{i=m}^n f(i) \right)^c$
$\prod_{i=m}^n c f(i) = c^{(n-m+1)} \prod_{i=m}^n f(i)$

Exercicis:

17. (R) Calculeu $\frac{\prod_{i=2}^{n+2} a_i}{\prod_{i=2}^n a_i}$.

18. Si $A = \prod_{i=1}^n a_i$, expresseu en funció de A :

a. (R) $\prod_{i=1}^n a_i^k$

b. (R) $\prod_{i=1}^n k a_i$

c. $\prod_{i=1}^n i a_i$

d. $\prod_{i=1}^n i^r a_i^k$

19. Si $A = \prod_{i=m}^n a_i$ i $B = \prod_{i=m}^n b_i$, expresseu en funció de A, B :

a. (R) $\prod_{i=m}^n a_i b_i$

b. $\prod_{i=m}^n \prod_{j=m}^n a_i b_j$

1. LÒGICA I DEMOSTRACIONS

1.1 LÒGICA

Lògica Proposicional

Enunciat o proposició: frase o expressió correcta del llenguatge natural susceptible de ser certa o falsa. Afirmar alguna cosa que té sentit, sigui certa o falsa.

Exemples:

- I. Són enunciats:
 - A. $2 + 3 = 6$.
 - B. la pissarra és blava.
 - C. són les 7 en punt.
 - D. si $2 + 3 = 6$ llavors la pissarra és blava.
 - E. són les 7 en punt i la pissarra és blava.
- II. No són enunciats:
 - A. $2 + 3$
 - B. 6
 - C. la pissarra
 - D. Quina hora és?
 - E. Esborreu la pissarra!

Per poder estudiar el valor de veritat d'un enunciat és molt important reconèixer la seva forma. Observem en els exemples que hi ha uns enunciats indescomponibles o atòmics ($2+3=6$, *són les 7 en punt*, *la pissarra és blava*) i d'altres que es poden construir a partir d'aquests. Per exemple: $2+3=6$ o *la pissarra no és blava*.

Per entendre millor la *forma* d'un enunciat, representarem els enunciats atòmics mitjançant les lletres p, q, r, \dots i farem servir els símbols $\wedge, \vee, \rightarrow$ per denotar la conjunció, la disjunció i la implicació respectivament. També usarem el símbol \neg per denotar la negació. les expressions obtingudes d'aquesta manera en direm **fórmules**. Veiem com es faria a l'exemple anterior.

Exemple: Si usem les lletres p, q, r per denotar respectivament $2 + 3 = 6$, *la pissarra és blava*, *són les 7h en punt*, les frases de l'exemple anterior quedarien formalitzades així:

- A. p .
- B. q .
- C. r .
- D. $p \rightarrow q$.
- E. $r \wedge q$.

Per a formalitzar F. necessitem lògica primer ordre.

Les **fórmules** de la lògica proposicional es construeixen amb els símbols següents:

- **Lletres proposicionals:** p, q, r, s, \dots (**àtoms** o **fórmules atòmiques**)
- **Connectives lògiques:**
 - binàries: $\wedge, \vee, \rightarrow, \leftrightarrow$
 - unària: \neg
- Parèntesis: $(,)$

A continuació donem una definició més precisa de *fórmula de la lògica proposicional*. Les fórmules són determinades **seqüències finites dels símbols anteriors**. Són totes les seqüències que s'obtenen aplicant un nombre finit de vegades les regles següents.

Definició Recursiva de fórmula:

- Les lletres proposicionals són fórmules
- Si φ és una fórmula, $\neg\varphi$ també és una fórmula
- Si φ, ψ són fórmules i $*$ és una connectiva binària, llavors $(\varphi * \psi)$ també és una fórmula

Exemples de fórmules:

$p, q, r, \neg p, (p \rightarrow q), (p \vee q), (\neg p \wedge q), \neg(\neg p \wedge q), ((p \vee q) \rightarrow r),$
 $(\neg(p \rightarrow \neg r) \leftrightarrow (p \vee \neg q)), \dots$

Notem que:

1. Els parèntesis només es posen a les connectives binàries i **mai a la negació**: no es posa $(\neg p)$. Es fan servir per evitar ambigüitats de lectura. Per exemple, per distingir $(p \vee q) \rightarrow r$ de $p \vee (q \rightarrow r)$.
2. Els parèntesis exteriors se **suprimeixen sempre**: posem $(p \vee q) \rightarrow r$ en lloc de $((p \vee q) \rightarrow r)$.

Nota: És interessant saber que a vegades s'utilitza el conveni següent (encara que a l'assignatura no el farem servir): es prioritzen les connectives binàries seguint aquest ordre: $\wedge, \vee, \rightarrow, \leftrightarrow$. Es posen parèntesis de tal manera que s'executi primer \wedge , segon \vee , ... Per exemple, $p \vee q \rightarrow r$ és la fórmula $(p \vee q) \rightarrow r$, $p \wedge q \vee \neg r$ és la fórmula $(p \wedge q) \vee \neg r$, $p \wedge q \leftrightarrow \neg r \vee p$ és la fórmula $(p \wedge q) \leftrightarrow (\neg r \vee p)$.

Significat de les connectives

Farem servir el 1 per indicar que la proposició és certa i 0 per indicar que és falsa.

φ	$\neg\varphi$
0	1
1	0

φ	ψ	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \rightarrow \psi$	$\varphi \leftrightarrow \psi$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

A la fórmula $\varphi \rightarrow \psi$, φ és l'**antecedent** i ψ és el **conseqüent**.

Les **Taules de veritat** es construeixen aplicant les regles anteriors calculant totes les combinacions de valors possibles dels àtoms. Es comença per les fórmules més senzilles.

Exemple:

p	q	r	$\neg r$	$p \rightarrow \neg r$	$\neg(p \rightarrow \neg r)$	$\neg q$	$p \vee \neg q$	$\neg(p \rightarrow \neg r) \leftrightarrow (p \vee \neg q)$
0	0	0	1	1	0	1	1	0
0	0	1	0	1	0	1	1	0
0	1	0	1	1	0	0	0	1
0	1	1	0	1	0	0	0	1
1	0	0	1	1	0	1	1	0
1	0	1	0	0	1	1	1	1
1	1	0	1	1	0	0	1	0
1	1	1	0	0	1	0	1	1

Tipus de fórmules importants:

Tautologia: fórmula sempre certa (taula de veritat: columna de 1)
Contradicció: fórmula sempre falsa (taula de veritat: columna de 0)
Satisfactible: fórmula que és certa per a alguna assignació (taula de veritat conté algun 1)

insatisfactible = contradicció

Exemples:

- Tautologies: $p \vee \neg p$, $p \rightarrow p$, $(p \wedge q) \rightarrow p$, $p \rightarrow (p \vee q)$, $p \rightarrow (q \rightarrow p)$, $(p \wedge (p \rightarrow q)) \rightarrow q$, $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$, $((p \wedge q) \rightarrow r) \wedge (p \rightarrow q) \rightarrow (p \rightarrow r)$, ...
- Contradiccions: $p \wedge \neg p$, $(p \wedge \neg q) \wedge (p \leftrightarrow q)$, la negació de qualsevol tautologia, ...

Equivalència de fórmules

Quan dues fórmules prenen els mateixos valors de veritat en totes les assignacions es diuen **equivalents**.

Per expressar que les fórmules φ i ψ són equivalents s'escriu:

$$\varphi \equiv \psi$$

Això vol dir que les fórmules φ, ψ tenen la mateixa taula de veritat (ordenant les assignacions de valors de la mateixa manera).

Totes les tautologies són equivalents. Una tautologia la denotarem per 1. De la mateixa manera totes les contradiccions són equivalents. Una contradicció la denotarem per 0.

Equivalències importants:

Quan no hi apareixen $\rightarrow, \leftrightarrow$ tota equivalència té una equivalència dual consistent en intercanviar \wedge per \vee i 0 per 1. La taula següent conté una llista d'equivalències importants juntament amb la seva dual a la columna de la dreta.

El color vermell indica que són propietats bàsiques a partir de les quals es poden deduir formalment totes les altres.

Distributiva	$\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$	$\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta)$
De Morgan	$\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$	$\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$
Absorció	$\varphi \wedge (\varphi \vee \psi) \equiv \varphi$	$\varphi \vee (\varphi \wedge \psi) \equiv \varphi$
Idempotència	$\varphi \wedge \varphi \equiv \varphi$	$\varphi \vee \varphi \equiv \varphi$
Commutativa	$\varphi \wedge \psi \equiv \psi \wedge \varphi$	$\varphi \vee \psi \equiv \psi \vee \varphi$
Associativa	$\varphi \wedge (\psi \wedge \theta) \equiv (\varphi \wedge \psi) \wedge \theta$	$\varphi \vee (\psi \vee \theta) \equiv (\varphi \vee \psi) \vee \theta$
Neutre	$\varphi \wedge 1 \equiv \varphi$	$\varphi \vee 0 \equiv \varphi$
Element absorbent	$\varphi \vee 1 \equiv 1$	$\varphi \wedge 0 \equiv 0$

Complementari	$\varphi \vee \neg\varphi \equiv 1$	$\varphi \wedge \neg\varphi \equiv 0$
Doble negació	$\neg\neg\varphi \equiv \varphi$	
	$\neg 1 \equiv 0$	$\neg 0 \equiv 1$

Nota: La propietat associativa d'una operació permet suprimir parèntesis. Per exemple, $p \wedge (q \wedge r)$ ho escriurem $p \wedge q \wedge r$. També escriurem $p \vee \neg q \vee \neg p \vee r$ enlloc de $(p \vee \neg q) \vee (\neg p \vee r)$.

Equivalències importants per a les demostracions (aquí no hi ha dual):

Traducció de la \rightarrow	$\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$	$\neg(\varphi \rightarrow \psi) \equiv \varphi \wedge \neg\psi$
Traducció de la \leftrightarrow	$\varphi \leftrightarrow \psi \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$ $\equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$	$\neg(\varphi \leftrightarrow \psi) \equiv (\varphi \wedge \neg\psi) \vee (\psi \wedge \neg\varphi)$ $\equiv (\varphi \vee \psi) \wedge (\neg\psi \vee \neg\varphi)$
Contrarecíproc	$\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi$	
Reducció a l'absurd	$\varphi \equiv \neg\varphi \rightarrow 0$	$\varphi \rightarrow \psi \equiv (\varphi \wedge \neg\psi) \rightarrow 0$
\vee al conseqüent	$\psi \vee \theta \equiv \neg\psi \rightarrow \theta$	$\varphi \rightarrow (\psi \vee \theta) \equiv (\varphi \wedge \neg\psi) \rightarrow \theta$
\vee a l'antecedent	$(\psi \vee \theta) \rightarrow \varphi \equiv (\psi \rightarrow \varphi) \wedge (\theta \rightarrow \varphi)$	

Les demostracions de totes les equivalències es poden fer utilitzant les equivalències en **vermell**. Bàsicament el mètode consisteix en: primer reemplaçar les fletxes per la seva equivalència (2a taula) i a continuació utilitzar les equivalències de la primera taula. En algun cas pot no ser tant mecànic, com per exemple l'absorció:

Exemple: Absorció. $p \wedge (p \vee q) \equiv [Neut] (p \wedge (p \vee q)) \wedge 1 \equiv [Compl] (p \wedge (p \vee q)) \wedge (p \vee \neg p) \equiv [Ass] p \wedge ((p \vee q) \wedge (p \vee \neg p)) \equiv [Distr] p \wedge (p \vee (q \wedge \neg p)) \equiv [Distr] (p \wedge p) \vee (p \wedge (q \wedge \neg p)) \equiv [Idem, Comm] p \vee (p \wedge (\neg p \wedge q)) \equiv [Ass] p \vee ((p \wedge \neg p) \wedge q) \equiv [Compl] p \vee (0 \wedge q) \equiv [Elem. Abs.] p \vee 0 \equiv [Neut] p$.

Exercici: Demostreu sintàcticament (utilitzant només les **equivalències en vermell**, sense usar taules de veritat) les equivalències següents:

- $\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi$.
- $\varphi \rightarrow \psi \equiv (\varphi \wedge \neg\psi) \rightarrow 0$.

3. $(\psi \vee \theta) \rightarrow \varphi \equiv (\psi \rightarrow \varphi) \wedge (\theta \rightarrow \varphi)$.
4. $\varphi \rightarrow (\psi \rightarrow \theta) \equiv (\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \theta)$.
5. (R) $\neg(\varphi \leftrightarrow \psi) \equiv (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi) \equiv (\varphi \vee \psi) \wedge (\neg\varphi \vee \neg\psi)$.
6. (R) $\varphi \rightarrow (\psi \vee \theta) \equiv (\varphi \wedge \neg\psi) \rightarrow \theta$.
7. (R) $(\varphi \wedge \psi) \rightarrow \theta \equiv \varphi \rightarrow (\psi \rightarrow \theta)$.
8. $\neg(\varphi \leftrightarrow \psi) \equiv \neg\varphi \leftrightarrow \psi$.
9. $\varphi \leftrightarrow 0 \equiv \neg\varphi$, $\varphi \leftrightarrow 1 \equiv \varphi$.
10. $\varphi \leftrightarrow \varphi \equiv 1$, $\varphi \leftrightarrow \neg\varphi \equiv 0$.
11. Aquí usem $\varphi \oplus \psi$ per a denotar $\neg(\varphi \leftrightarrow \psi)$. La \oplus és coneguda com a XOR.
Demostreu que¹:
 - a. (difícil) $\varphi \oplus (\psi \oplus \theta) \equiv (\varphi \oplus \psi) \oplus \theta$.
 - b. $\varphi \wedge (\psi \oplus \theta) \equiv (\varphi \wedge \psi) \oplus (\varphi \wedge \theta)$.
 - c. $\varphi \oplus 1 \equiv \neg\varphi$, $\varphi \oplus 0 \equiv \varphi$.
 - d. $\varphi \oplus \neg\varphi \equiv 1$.
 - e. $\varphi \oplus \varphi \equiv 0$.
12. (R) $q \vee (p \wedge (\neg p \vee r)) \equiv (q \vee p) \wedge ((q \vee r) \vee (p \wedge \neg p))$.
13. Són equivalents $p \rightarrow (q \rightarrow (p \rightarrow q))$ i $((p \rightarrow q) \rightarrow p) \rightarrow q$?
14. (difícil) $\varphi \leftrightarrow (\psi \leftrightarrow \theta) \equiv (\varphi \leftrightarrow \psi) \leftrightarrow \theta$.
15. $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi) \equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$.
16. $\varphi \rightarrow (\psi \wedge \theta) \equiv (\varphi \rightarrow \psi) \wedge (\varphi \rightarrow \theta)$.
17. $\varphi \vee (\psi \leftrightarrow \theta) \equiv (\varphi \vee \psi) \leftrightarrow (\varphi \vee \theta)$.

Lògica de primer ordre (o lògica de predicats)

Relacions

Per tenir una relació hem de tenir un “domini d’individus” i una propietat d’aquests individus. Una relació d’aritat 1 és una propietat que depèn d’un sol argument. Cada individu del domini té o no té la propietat. Una relació d’aritat 2 té dos arguments; és una propietat que depèn de dos individus. Podem pensar que és una propietat de les parelles d’individus o que relaciona els individus de la parella entre ells. Cada parella d’individus té o no té la propietat (estan relacionats entre ells o no). Una relació d’aritat 3 és una propietat que depèn de tres individus (relaciona aquests tres individus entre ells), etc. En matemàtiques es usual treballar amb relacions binàries. En bases de dades relacionals es treballa de manera natural amb relacions de qualsevol aritat, encara que la terminologia que utilitzen és diferent.

¹ Les fórmules de lògica (mòdul equivalència), amb les operacions XOR i la conjunció formen un anell.

Exemples:

- Domini \mathbb{Z} . Les relacions “ser parell”, “ser un quadrat”, “ser múltiple de 4” son relacions d’arietat 1. Les relacions “ser menor que” ($x < y$), “ser igual que” ($x = y$), “ser congruents mòdul 5” ($x \equiv y \pmod{5}$) són relacions d’arietat 2. La relació “ x està entre y i z ” és una relació d’arietat 3. La relació “ x és congruent amb y mòdul z ” és una relació d’arietat 3.
- Domini: Els alumnes de l’aula. Les relacions “ser alt”, “ser treballador”, “portar ulleres”, ... són relacions d’arietat 1. Les relacions “seure al costat de”, “ser amics”, “calçar el mateix número de sabata”, són relacions d’arietat 2.

Fórmules atòmiques

Es formen a partir dels símbols de relació i variables.

Definició:

Si R és un símbol de relació d’arietat n , i x_1, x_2, \dots, x_n són variables, la següent és una **fórmula atòmica**:

$$R(x_1, x_2, \dots, x_n)$$

Exemple: Si tenim els símbols de relació P d’arietat 1, Q , $<$ d’arietat 2 i R d’arietat 3, les següents són fórmules atòmiques: $P(x)$, $Q(x, y)$, $Q(z, z)$, $x < y$, $R(x, y, z)$, $R(x, z, x)$. També considerem fórmules atòmiques: $x > 0$, $x = y^2$, $1 \leq y^2 + y$ (aquí els símbols de relació són: $>$, $=$, \leq).

Notes:

1. A les relacions binàries (arietat 2) es pot usar notació infixa en lloc de prefixa: es pot escriure xRy en lloc de $R(x, y)$. Per exemple s’escriu: $x < y$, $x = y$, $x \leq y$, $x \in y$, ...
2. A les fórmules atòmiques també hi poden aparèixer expressions més complicades en lloc de simples variables. Com ara noms d’individus particulars, nombres... o bé expressions com ara 0 , 1 , y^2 , $x^2 + 2x \dots^2$.

² és el que s’acostuma a denominar **termes**, però no en donarem la definició formal

Fórmules de la lògica de primer ordre

Les fórmules de la lògica de primer ordre es formen a partir de les atòmiques combinant-les entre elles amb les connectives lògiques ($\wedge, \vee, \rightarrow, \leftrightarrow, \neg$) i els quantificadors:

$$\forall, \exists$$

Definició Recursiva de fórmula:

- Les fórmules atòmiques són fórmules.
- Si φ, ψ són fórmules i $*$ és una connectiva binària llavors $(\varphi * \psi)$ també és una fórmula.
- Si φ és una fórmula $\neg\varphi$ també és una fórmula.
- Si φ és una fórmula i x una variable, $\forall x\varphi$ i $\exists x\varphi$ també són fórmules.

Exemple: Si tenim els símbols de relació P d'arietat 1, $Q, <$ d'arietat 2 i R d'arietat 3: $P(x), Q(x, y), x < y, R(x, y, z), \neg R(x, y, z), (P(x) \rightarrow Q(x, y)), \forall x(P(x) \rightarrow Q(x, y)), \exists y\forall x(P(x) \rightarrow Q(x, y)), \exists y\forall x(P(x) \rightarrow Q(x, y)) \vee \neg R(x, y, z) \forall z(\exists y\forall x(P(x) \rightarrow Q(x, y)) \vee \neg R(x, y, z)), \forall x\exists y(x > 0 \rightarrow x = y^2), \dots$

Nota: Igual que a la lògica proposicional, només es posen parèntesis a les connectives binàries i se suprimeix el parèntesi exterior. No posem parèntesis ni als quantificadors ni a la negació.

Significat de les fórmules de la lògica de primer ordre

Perquè les fórmules de la lògica de primer ordre tinguin sentit, necessitem:

- Un domini (o univers) d'individus. És el domini de variació de les variables i sempre ha de contenir algun individu (un com a mínim).
- El "significat" o "interpretació" dels símbols de relació. Han de ser relacions concretes entre individus del domini.

Llavors:

- $\forall x\varphi$ significa que *tots els individus x del domini compleixen φ* .
- $\exists x\varphi$ significa que *hi ha (almenys) un individu x del domini que compleix φ* .

Exemple: Si el domini és \mathbb{Z} , $P(x)$ s'interpreta: x és un parell, $Q(x)$ s'interpreta: x és un quadrat, $M(x)$ s'interpreta: x és múltiple de 4 i, $x < y$ s'interpreta de manera obvia (x és menor que y):

fórmula	Significat
$\forall x (M(x) \rightarrow P(x))$	Tot enter múltiple de 4 és parell
$\exists x (P(x) \wedge \neg M(x))$	Hi ha nombres parells que no són múltiples de 4
$\forall x ((P(x) \wedge Q(x)) \rightarrow M(x))$	Tot parell quadrat és múltiple de 4
$\exists x (P(x) \wedge \neg M(x) \wedge \neg Q(x))$	Hi ha nombres parells que ni són múltiples de quatre ni són quadrats
$P(2) \wedge \neg Q(2) \wedge \neg M(2)$	2 és parell però no és quadrat ni múltiple de 4
$\exists x (P(x) \wedge x > 2 \wedge \neg Q(x))$	Hi ha nombres parells més grans que 2 que no són quadrats

Notes:

- A vegades, el domini de variació de les variables s'indica a la fórmula. Així, fórmules de l'exemple anterior les podem escriure: $\forall x \in \mathbb{Z}(M(x) \rightarrow P(x))$, $\exists x \in \mathbb{Z}(P(x) \wedge \neg M(x))$, $\exists x \in \mathbb{Z}(P(x) \wedge \neg M(x) \wedge \neg Q(x))$...
- A vegades s'escriuen expressions de l'estil $\forall x \in \mathbb{Z} \exists y \in \mathbb{N}(x < y)$, però això ja no és una fórmula de primer ordre. Perquè fos una fórmula de primer ordre hauríem d'afegir un predicat $N(x)$ (que s'interpretés com x és *natural*) i escriure: $\forall x \exists y (N(y) \rightarrow x < y)$ o bé $\forall x \in \mathbb{Z} \exists y \in \mathbb{Z}(N(y) \rightarrow x < y)$.

Equivalència en lògica de primer ordre

Dues fórmules³ de la lògica de primer ordre són **equivalents** quan prenen el mateix valor de veritat en totes les "interpretacions" possibles (en tot "domini" i en tota tota "interpretació" dels símbols de relació).

³ sense variables lliures

Algunes equivalències importants:

$\neg \forall x \varphi \equiv \exists x \neg \varphi$	$\neg \exists x \varphi \equiv \forall x \neg \varphi$
$\forall x \forall y \varphi \equiv \forall y \forall x \varphi$	$\exists x \exists y \varphi \equiv \exists y \exists x \varphi$
$\forall x (\varphi \wedge \psi) \equiv \forall x \varphi \wedge \forall x \psi$	$\exists x (\varphi \vee \psi) \equiv \exists x \varphi \vee \exists x \psi$

Observació:

1. No és certa l'equivalència: de $\forall x \exists y \varphi$ i $\exists y \forall x \varphi$. Per exemple, si el domini són els nombres naturals $\forall x \exists y (x < y)$ és certa, en canvi $\exists y \forall x (x < y)$ és falsa.
2. Tampoc són certes $\forall x (\varphi \vee \psi) \equiv \forall x \varphi \vee \forall x \psi$ ni $\exists x (\varphi \wedge \psi) \equiv \exists x \varphi \wedge \exists x \psi$. Per exemple, si el domini són els nombres naturals, $P(x)$ és “ x és parell”, $S(x)$ és “ x és senar”, $\forall x (P(x) \vee S(x))$ és certa en canvi $\forall x P(x) \vee \forall x S(x)$ és falsa.

Exercicis. Demostreu les equivalències següents:

18. $\neg \exists x (C(x) \wedge N(x)) \equiv \forall x (C(x) \rightarrow \neg N(x))$.
19. $\neg \forall x (P(x) \rightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x))$.
20. (R) $\exists x (P(x) \rightarrow Q(x)) \equiv \forall x P(x) \rightarrow \exists x Q(x)$.
21. (R) $\neg \forall x (P(x) \leftrightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x)) \vee \exists x (Q(x) \wedge \neg P(x))$.
22. (R) Demostreu que la fórmula $\exists x (P(x) \rightarrow \forall y P(y))$ sempre és certa (sigui qui sigui P).
23. $\neg \exists x \exists y (x \neq y \wedge P(x) \wedge P(y)) \equiv \forall x \forall y ((P(x) \wedge P(y)) \rightarrow x = y)$
24. $\forall x (C(x) \rightarrow \neg N(x)) \equiv \forall x (N(x) \rightarrow \neg C(x)) \equiv \forall x (\neg C(x) \vee \neg N(x))$.

Formalització

Formalitzar consisteix en expressar en un llenguatge “formal” un enunciat. En el nostre cas consistirà en trobar una fórmula de la lògica de primer ordre. Quan formalitzem amb quantificadors es pressuposen:

- Un domini (o univers) d'individus.
- Relacions entre individus que “interpretin” els símbols de relació.

Hi ha dos **patrons** que apareixen de manera habitual:

- A. $\forall x (A(x) \rightarrow B(x))$ Tots els individus de tipus A (que tenen la propietat A) tenen la propietat B .
- B. $\exists x (A(x) \wedge B(x))$ Hi ha individus de tipus A que tenen la propietat B .

Exercicis:

25. Un món de Tarski està format per una graella i diverses formes geomètriques que tenen un color i que poden portar una etiqueta, com a la figura. Considerem els símbols de relació següents:

$T(x)$: x és un triangle

$C(x)$: x és un cercle

$Q(x)$: x és un quadrat

$B(x)$: x és blau

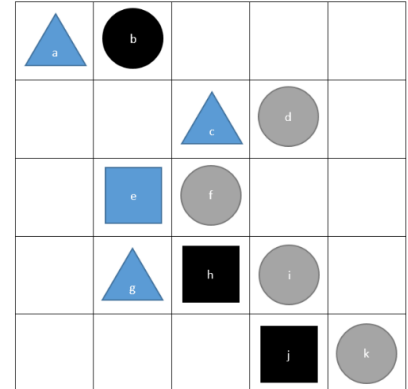
$N(x)$: x és negre

$G(x)$: x és gris

$E(x, y)$: x està a l'esquerra de y

$S(x, y)$: x està a sobre de y

$K(x, y)$: x té el mateix color que y



Usant els símbols indicats, formalitzeu les frases següents:

- Hi ha un quadrat negre.
 - Tots els cercles són blaus;
 - No hi ha cap cercle negre.
 - a està a sobre de e .
 - Hi ha un cercle que té el mateix color que d .
 - (R) d està a l'esquerra de qualsevol cercle.
 - (R) Alguna forma geomètrica és blava.
 - Tots els quadrats són negres.
 - (R) Tots els triangles estan a l'esquerra de d .
 - Hi ha un triangle a l'esquerra de d .
 - (R) Hi ha un triangle que està a sobre de d però no a l'esquerra de a .
 - Algun triangle no és gris.
 - (R) Cap quadrat té el mateix color que b .
 - Algun cercle és blau.
 - Tots els cercles estan a sobre de d .
 - Tot triangle està a l'esquerra de a o a sobre de b .
26. Usant els símbols de relació del problema anterior, expresseu en llenguatge natural les proposicions següents i determineu si a la figura anterior són certes o falses:

- a. $\forall x(B(x) \rightarrow (T(x) \vee Q(x)))$
- b. $\exists y(C(y) \wedge \neg S(y, d))$
- c. (R) $\forall x(N(x) \rightarrow (T(x) \vee Q(x)))$
- d. $\exists y(C(y) \wedge S(y, d))$
- e. (R) $\exists y(C(y) \wedge \neg E(y, d))$
- f. $\forall x(T(x) \rightarrow \exists y(Q(y) \wedge K(x, y)))$

27. En aquest exercici el domini és el conjunt dels enters. A més de les variables, connectives i quantificadors, podeu utilitzar només els símbols següents:

$|$, $<$, \cdot , $=$, $+$, P , Q , 0 , 1 , 2 , 3 , 4 ...

$x | y$ formalitza x divideix y (o y és múltiple de x).

$P(x)$ formalitza x és primer.

$Q(x)$ formalitza x és un quadrat.

Formalitzeu els enunciats següents:

- a. 1 no és primer.
- b. Tot enter múltiple de 6 és també múltiple de 3 i de 2.
- c. Cap nombre primer és un quadrat.
- d. (R) Tot enter múltiple de 3 i de 5 és múltiple de 15.
- e. 2 és primer i és parell.
- f. Tot quadrat parell és múltiple de 4.
- g. (R) La suma de dos senars és parell.
- h. (R) Tot enter positiu és suma de quatre quadrats.
- i. Hi ha nombres senars que són primers i d'altres senars que no són primers.
- j. x és un nombre parell (amb una variable lliure: la x). Les variables lliures d'una fórmula són les que no estan sota l'efecte d'un quantificador.
- k. Tot nombre parell més gran que 2 és suma de dos primers.

28. En aquest exercici suposem que totes les variables prenen valors enters. A més de les variables, connectives lògiques i quantificadors, **només** podeu utilitzar els símbols següents: $<$, \cdot , $=$, $+$, 0 , 1 , 2 , 3 , 4 ... (Ull, ara no podem usar: $|$, P , Q). Formalitzeu:

- a. (R) x divideix y (x, y són variables sense quantificar).
- b. x és un quadrat (x variable sense quantificar).
- c. (R) x és un nombre primer (x variable sense quantificar).
- d. (R) 2 és l'únic nombre primer parell.
- e. (R) Hi ha infinits nombres primers (pista: sempre n'hi un més gran que un donat).
- f. 2 és el nombre primer més petit.
- g. Tots els apartats de l'exercici anterior.

29. Aquí només podeu fer servir el predicat 1-ari P i el predicat binari $=$.
Formalitza:

- a. Hi ha com a molt un element que té la propietat P .
- b. Hi ha com a molt 2 element que tenen la propietat P .
- c. Hi ha com a mínim 2 element que tenen la propietat P .
- d. Hi ha exactament 2 element que tenen la propietat P .
- e. Hi ha un únic element que té la propietat P .
- f. Hi ha com a molt 3 element que tenen la propietat P .
- g. Hi ha com a mínim 3 element que tenen la propietat P .
- h. Hi ha exactament 3 element que tenen la propietat P .

Veracitat i quantificadors

Com es justifica (o demostra) que un enunciat és cert? En general, depèn de la seva “forma”. Normalment, encara que a vegades de manera no explícita, hi ha quantificadors. La justificació dependrà, en primer lloc, de si els quantificadors són existencials o universals.

Demostració d'un existencial $\exists xP(x)$:

El mètode més senzill és donar un element a del domini que tingui la propietat P . Un sol exemple és suficient.

Exemples:

- $\exists x \in \mathbb{R} (x > 0 \wedge x^2 - 1 < 0)$ és cert.
- $\exists x \in \mathbb{Z} (x \text{ parell} \wedge x \equiv 1 \text{ mod } 5)$ és cert.

Això mateix s'aplica a la demostració que un enunciat universal és fals, ja que $\neg \forall xP(x) \equiv \exists x \neg P(x)$. La demostració de la falsedat de $\forall xP(x)$ es fa donant un element a del domini que **no** tingui la propietat P ; a rep el nom de **contraexemple**.

Exemples:

- $\forall x \in \mathbb{R} (x > 0 \rightarrow x \geq 1)$ és fals.
- $\forall x \in \mathbb{Z} (x \equiv 1 \bmod 3 \rightarrow x \text{ senar})$ és fals

Exercicis: Dieu quins enunciats són certs i quins són falsos:

- 30. $(\mathbb{R}) \exists x \in \mathbb{R} (x > 2 \wedge x < 5)$.
- 31. $(\mathbb{R}) \forall x \in \mathbb{Z} (x^2 \text{ múltiple de } 16 \rightarrow x \text{ múltiple de } 8)$.
- 32. $\forall x \in \mathbb{R} (x > 2 \rightarrow x < 5)$.
- 33. $\exists x \in \mathbb{R} (x^2 - x > 1 \wedge x^2 + x < 1)$.

Demostració d'un universal $\forall x P(x)$:

Hem de veure que tots els elements del domini satisfan la propietat P . Si hi ha pocs elements, ho podem verificar un a un. Si n'hi ha molts o infinits no quedarà més remei que donar-ne una "demostració". Una demostració és un raonament que segueix unes certes regles. Tot i que fer una demostració pot arribar a ser molt difícil, la comprovació que aquesta és correcte no hauria de ser-ho. Però això requereix que la demostració estigui ben escrita. A l'apartat següent explicarem com es fa això.

El mateix s'aplica a la demostració que un existencial és fals.

Exemples/exercicis. $A = \{0, 1, 2, 3\}$

34. Justifiqueu que són falses:

- a. $\exists x \in A (|x + 4| = 2)$
- b. $\exists x \in A (x^3 + 2x^2 - x = 4)$

35. Justifiqueu que són certes:

- a. $\forall x \in A x^2 \leq 3x$
- b. $\forall x \in A (|x - 1| < 2 \vee x^2 - 9 = 0)$

Quantificadors barrejats

Demostració de:

- $\exists x \forall y P(x, y)$: donar un element x que tingui la propietat $P(x, y)$ per a cada y . Fem $x = a$ i demostrem que $\forall y P(a, y)$ és cert. La x no pot dependre de y .
Exemple: $\exists x \in \mathbb{N} \forall y \in \mathbb{N} x \leq y$ és cert. Fem $x = 0$ i veiem que $\forall y \in \mathbb{N} 0 \leq y$ és cert.
- $\forall x \exists y P(x, y)$: per a cada x cal donar una y que satisfà $P(x, y)$. La y normalment dependrà de x . Fem $y = E(x)$ i demostrem que $\forall x P(x, E(x))$ és cert.
Exemple: $\forall x \in \mathbb{N} \exists y \in \mathbb{N} x < y$ és cert. Fem $y = x + 1$ i veiem que $\forall x \in \mathbb{N} x < x + 1$ és cert.
- La demostració de la falsedat de $\exists x \forall y P(x, y)$ o de $\forall x \exists y P(x, y)$ es pot fer veient que els seus negats són certs.

Fet: Si $\exists x \forall y P(x, y)$ és cert $\forall y \exists x P(x, y)$ també és cert, però no és val el recíproc en general. En el primer cas necessitem un mateix valor de x que funcione per a qualsevol y , mentre que en el segon cas necessitem una x per a cada y (la x pot anar variant).

Exercicis: En aquest exercici el domini és \mathbb{R} . Justifiqueu la veritat o falsedat de:

- 36. $\exists y \forall x x y = 0$.
- 37. $\forall x \exists y (xy - 1 = 0)$.
- 38. (R) $\forall x \exists y (x \neq 0 \rightarrow xy - 1 = 0)$.
- 39. (R) $\exists y \forall x x y = x$.
- 40. $\exists y \forall x x y = 1$.
- 41. (R) $\forall x \exists y (xy + 2y - 1 = 0)$.
- 42. $\forall x \exists y (3x + 2y - 1 = 0)$.
- 43. $\exists y \forall x (3x + 2y - 1 = 0)$.

A continuació teniu un quadre resum d'aquest apartat:

Volem demostrar	Què cal fer
$\exists x \in A \ P(x)$ Cert	Donar un exemple : Donar $a \in A$ tal que $P(a)$
$\forall x \in A \ P(x)$ Fals	Donar un contraexemple : Donar $a \in A$ tal que $\neg P(a)$
$\exists y \in A \ \forall x \in A \ P(x, y)$ Cert	Donar $a \in A$ tal que $\forall x \in A \ P(x, a)$ ⁴
$\forall x \in A \ \exists y \in A \ P(x, y)$ Cert	Per a cada $x \in A$ donar $y = E(x)$ tal que $\forall x \in A \ P(x, E(x))$ ⁵

⁴ La y no pot dependre de x: és constant

⁵ La y acostuma a dependre de x, encara que en alguna ocasió pot ser constant

1.2 DEMOSTRACIONS

Què és una demostració?

Una demostració és una justificació de la veracitat d'un enunciat feta seguint unes regles força precises.

Una demostració sempre consta d'una sèrie de petits passos que podríem anomenar implicacions bàsiques o propietats bàsiques *combinades* d'acord a una sèrie de regles o mètodes de demostració que explicarem a continuació. En una demostració també es fan servir les definicions dels conceptes que apareixen a l'enunciat. Comencem explicant què o quins són aquests petits passos bàsics (implicacions o propietats bàsiques).

Han de ser o bé propietats que no ofereixen cap mena de dubte sobre la seva veracitat (les podríem anomenar axiomes) o bé petites implicacions que tampoc no ofereixen cap mena de dubte.

Què podem usar en una demostració?

Alguns passos bàsics

Aquí donarem, a moda d'exemple alguns dels passos bàsics més habituals. A l'apèndix hi ha una llista força més exhaustiva. Comencem pels passos bàsics de tipus lògic o petites implicacions lògiques.

Passos lògics: (aquí A, B, C són enunciats)

- | | | | |
|------|---------------------------------|---------------|------------------|
| I. | A, B | \Rightarrow | A |
| II. | A | \Rightarrow | $A \text{ o } B$ |
| III. | $A \text{ o } B, \text{ no } A$ | \Rightarrow | B |
| IV. | $A, A \Rightarrow B$ | \Rightarrow | B |
| V. | $\text{no } B, A \Rightarrow B$ | \Rightarrow | $\text{no } A$ |

- VI. $A \Rightarrow B, B \Rightarrow C \Rightarrow A \Rightarrow C$
 VII. $ABSURD \Rightarrow A$

La manera de veure que cada una d'aquestes implicacions és correcta és comprovar que cada una de les fórmules següents són tautologies:

- I. $(p \wedge q) \rightarrow p$
 II. $p \rightarrow (p \vee q)$
 III. $((p \vee q) \wedge \neg p) \rightarrow q$
 IV. $(p \wedge (p \rightarrow q)) \rightarrow q$
 V. $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
 VI. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
 VII. $0 \rightarrow p$

Ara donem alguns exemples de passos bàsics de tipus no lògic importants. Aquest tipus de propietats es solen anomenar **axiomes** i s'accepten com a certs sense demostració. Al final d'aquest primer tema hi ha un apèndix amb una llista més detallada d'axiomes no lògics.

Passos no lògics: (aquí $a, b, c, d...$ són números reals)

- I. $a = b \Rightarrow E(a) = E(b)$ (aquí $E(x)$ és una expressió on apareix x)
 II. $a = b, b = c \Rightarrow a = c.$
 III. $a = b, a' = b' \Rightarrow a + a' = b + b', aa' = bb'.$
 IV. $a \leq b, b \leq a \Rightarrow a = b.$
 V. $a \leq b \Rightarrow -b \leq -a.$
 VI. $a \leq b \Rightarrow a + c \leq b + c.$
 VII. $a \leq b, c \leq d \Rightarrow a + c \leq b + d.$
 VIII. $a \leq b, c \geq 0 \Rightarrow ac \leq bc.$
 IX. $0 \leq a \leq b, 0 \leq c \leq d \Rightarrow ac \leq bd.$
 X. Les propietats V,VI,VII,VIII i IX també valen amb $<$ enlloc de \leq .

Quin llenguatge fem servir?

Quan fem demostracions fem servir un llenguatge “semi-formal”. Cal saber reconèixer la “forma” (l’hem de saber formalitzar) però no usarem la formalització. Per exemple, el quantificador universal normalment no s’escriu, se sobreentén⁶.

A més, en el llenguatge semi-formal (fora de les fórmules), farem servir i, o, no, \Rightarrow , \Leftrightarrow en lloc de \wedge , \vee , \neg , \rightarrow , \leftrightarrow .

Fórmula	\wedge	\vee	\neg	\rightarrow	\leftrightarrow
Demostració	i ,	o	no	\Rightarrow / implica per tant / si ... llavors ...	\Leftrightarrow si i només si

Els símbols \wedge , \vee , \neg , \rightarrow , \leftrightarrow els reservem per a les fórmules. La coma , es fa servir per representar també la conjunció. Igualment escriurem *A implica B* o *si A llavors B* com a alternativa a $A \Rightarrow B$.

Exemple: Volem demostrar que: *per tot enter n, si n és senar llavors $n^2 + 4n - 1$ és parell*. En primer ordre es pot formalitzar així:

$$\forall x (S(x) \rightarrow P(x^2 + 4x - 1)),$$

on $S(x)$ formalitza “x és senar”, $P(x)$ formalitza “x és parell”, i el domini són els enters. Ara bé, per a fer-ne una demostració ho escriurem així :

$$n \text{ senar} \Rightarrow n^2 + 4n - 1 \text{ parell}$$

⁶A vegades tampoc s’escriuen els quantificadors existencials, que també se sobreenten. Encara que això pot causar confusió al principi, es reconeixen pel context.

Com combinem els passos bàsics?

Mètodes de demostració

Ara que ja sabem què són aquests passos bàsics anem a veure com s'estructuren per a donar lloc a una demostració correcta. Així com fer una demostració pot requerir un grau molt elevat d'enginy (hi ha demostracions que han trigat centenars d'anys a trobar-se posant a prova generacions dels millors matemàtics), verificar-la no hauria de requerir-ne gens. Si més no en teoria, ja que depèn molt del llenguatge en el que estiguin escrites. Si la demostració està escrita en un llenguatge totalment formal (com per exemple la lògica de primer ordre) aquesta pot ser verificada fàcilment per un ordinador. A la pràctica no es fan servir aquest tipus de demostracions (en un llenguatge formal) perquè esdevenen llarguíssimes i il·legibles per a una persona.⁷

Al nivell que treballarem aquí les demostracions han de ser escrites d'una manera clara indicant quin mètode s'utilitza. Redactada de tal manera que qualsevol persona amb uns mínims coneixements matemàtics pugui saber quin mètode de prova s'està utilitzant i pugui reconèixer que és el que es fa a cada pas. Un sol pas incorrecte invalida una demostració.

Prova directa.

Quan estem fent una demostració de $A \Rightarrow B$, A rep el nom de **Hipòtesi** i B de **Tesi**. La prova directa és el mètode més senzill, i consisteix a concatenar una sèrie d'implícacions bàsiques i/o propietats bàsiques. També es poden fer servir resultats coneguts (que ja han sigut demostrats prèviament) així com les definicions del conceptes que apareixen a l'enunciat. El que és important és que en cada moment o bé usem una propietat bàsica, una definició, un resultat conegut o apliquem una

⁷ De totes maneres, amb ajuda de "proof assistants" hi ha importants teoremes matemàtics que han estat formalitzats i verificats per ordinador: El teorema dels nombres primers, el teorema del mapa dels 4 colors, El teorema Feit-Thomson, el teorema d'incompletesa de Gödel o el teorema de la curva tancada de Jordan. Una demostració verificada formalment deixa un marge d'error molt baix en comparació amb una demostració escrita i publicada en llenguatge matemàtic estàndard.

implicació bàsica.

Esquemàticament, ho podem resumir així:

Volem demostrar $A \Rightarrow B$.
$A \Rightarrow A' \Rightarrow A'' \Rightarrow \dots \Rightarrow B$

Exercicis: Demostreu que:

1. La suma de dos enters consecutius és senar.
2. El quadrat d'un nombre enter senar és senar.
3. La suma d'un nombre parell i un nombre senar és senar.
4. El producte de dos quadrats és un quadrat.
5. La suma de tres enters consecutius té la mateixa paritat que el que està al mig.
6. (R) La suma de dos nombres senars és parell.
7. La suma de 4 enters consecutius és parell.
8. El quadrat d'un nombre parell és parell.
9. (R) n és enter. Si n és senar llavors $5n^2 - 1$ és parell.
10. El producte de dos nombres senars és senar.

Prova pel contrarecíproc.

Es basa en: $p \rightarrow q \equiv \neg q \rightarrow \neg p$

Volem demostrar $A \Rightarrow B$.
$\neg B \Rightarrow \dots \Rightarrow \neg A$

Exercicis: Demostreu pel contrarecíproc que:

11. n és enter. Si n^2 és parell llavors n és parell.
12. n és enter. Si $3n^2 + 6n + 5$ és parell llavors $n + 1$ és parell.
13. Aquí a, b, c són nombres reals positius. Si $c = ab$ llavors $a \leq \sqrt{c}$ o $b \leq \sqrt{c}$.
14. a, b, c són enters. Si $a + c$ és senar llavors $a + b$ és senar o $b + c$ és senar.
15. n és enter. Si n^3 és senar llavors n també és senar.

16. (R) n és enter. Si $5n^2 - 1$ és senar llavors n és parell.
17. a, b, c són nombres real. Si $c = a + b$ llavors $2a \leq c$ o $2b \leq c$.
18. a, b, c són enters. Si $a + b + c$ és senar llavors $a - b$ és parell o c és parell.
19. (R) Siguin x, y nombres reals positius. Demostreu que si $xy > 1$ llavors $x > 1$ o $y > 1$.
20. x, y són reals. Si $x + y \leq 2$ llavors $x \leq 1$ o $y \leq 1$.
21. n, m són enters. Si nm és parell llavors n és parell o m és parell.

Reducció a l'absurd

Es basa en: $p \equiv \neg p \rightarrow 0$

Volem demostrar A		
$\neg A$	\Rightarrow	\Rightarrow Contradició

Exercicis: Demostreu per reducció a l'absurd que:

22. $\sqrt{2}$ és irracional.
23. Si triem 15 dies diferents d'un calendari, n'hi ha 3 que cauen el mateix dia de la setmana.
24. a, b, c enters. Demostreu que $a + b$ és parell o $b + c$ és parell o $c + a$ és parell.
25. No hi ha cap nombre racional r tal que $r^3 + r + 1 = 0$ (useu que un zero racional, en forma reduïda, $\frac{a}{b}$ del polinomi $a_n x^n + \dots + a_1 x + a_0$ compleix que a divideix a_0 i b divideix a_n).
26. Donats n nombres reals a_1, \dots, a_n positius, algun d'ells ha de ser més gran o igual que la seva mitjana geomètrica $\sqrt[n]{a_1 \dots a_n}$.
27. $\sqrt{2} + \sqrt{3}$ és irracional (Pista: podeu usar que $\sqrt{6}$ és irracional).
28. (R) a, b, c reals. Demostreu que $a \leq \frac{b+c}{2}$ o $b \leq \frac{a+c}{2}$ o $c \leq \frac{a+b}{2}$.
29. (R) $\log_2 3$ és irracional.
30. $\sqrt{6}$ és irracional.
31. Donats n nombres reals, algun d'ells ha de ser menor o igual que la mitjana

- aritmètica dels restants.
32. Idem per a la mitjana geomètrica. Aquí suposem que els nombres són tots positius.
33. (R) $a + c$ és senar o $b - a$ és senar o $b + c - 1$ és senar.
34. Donats n nombres reals a_1, \dots, a_n , algun d'ells ha de ser més gran o igual que la seva mitjana aritmètica $\frac{a_1 + \dots + a_n}{n}$.
35. $2\sqrt{2}-2$ és irracional. (Pista: useu que $\sqrt{2}$ és irracional.)

Reducció a l'absurd II

Es basa en: $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow 0$

Volem demostrar $A \Rightarrow B$.		
$A, \neg B$	\Rightarrow	\Rightarrow Contradicció

Exercicis: Demostreu per reducció a l'absurd que:

36. La suma d'un nombre racional i un irracional és irracional.
37. Si a, b, c són nombres enters i $a + b + c = 0$, com a mínim un d'ells és parell.
38. a, b, c són reals positius. Si $c = ab$ llavors o $a \leq \sqrt{c}$ o $b \leq \sqrt{c}$.
39. (R) El resultat de multiplicar un racional no nul que és un quadrat per un racional que no és un quadrat és un nombre racional que no és un quadrat (que un nombre racional sigui un quadrat vol dir que és igual al quadrat d'un cert nombre racional).
40. Si a, b, c són nombres enters i $a + 3 = b + c$, com a mínim un d'ells és senar.
41. Si n és un quadrat llavors $n + 2$ no és un quadrat (n enter).
42. Si p és un primer senar llavors $\log_2 p$ és irracional.

Prova d'una disjunció

Es basa en: $(q \vee r) \equiv (\neg q \rightarrow r)$

Volem provar $B \vee C$		
$\neg B \Rightarrow$	$\Rightarrow C$

També val amb més disjuntands : $p_1 \vee \dots \vee p_n \equiv (\neg p_1 \wedge \dots \wedge \neg p_{n-1}) \rightarrow p_n$

Volem provar $B_1 \vee \dots \vee B_n$:		
$\neg B_1, \neg B_2, \dots, \neg B_{n-1} \Rightarrow$	$\Rightarrow B_n$

Exercicis: Demostreu, usant prova de la disjunció que:

43. n és enter. Demostreu que n és senar o n^2 és múltiple de 4.
44. a, b són reals. Demostreu que $a \leq \frac{a+b}{2}$ o $b \leq \frac{a+b}{2}$.
45. a, b, c són reals. Demostreu que $a \leq \frac{a+b+c}{3}$ o $b \leq \frac{a+b+c}{3}$ o $c \leq \frac{a+b+c}{3}$.
46. a, b són reals positius. Demostreu que o $a \leq \sqrt{ab}$ o $b \leq \sqrt{ab}$.
47. n és enter. Demostreu que n o $n^2 + 1$ és senar.
48. a, b, c són reals positius. Demostreu que $a \leq \sqrt[3]{abc}$ o $b \leq \sqrt[3]{abc}$ o $c \leq \sqrt[3]{abc}$.
49. (R) a, b són enters. Demostreu que $a - b$ és parell o $b - c$ és parell o $c - a$ és parell.
50. a, b, c són reals. Demostreu que $a \leq \frac{b+c}{2}$ o $b \leq \frac{a+c}{2}$ o $c \leq \frac{a+b}{2}$.

Disjunció al conseqüent

Es basa en: $p \rightarrow (q \vee r) \equiv (p \wedge \neg q) \rightarrow r$

Volem provar $A \Rightarrow (B \vee C)$
$A, \neg B \Rightarrow \dots \Rightarrow C$

Amb més disjuntands:

$$p \rightarrow (q_1 \vee \dots \vee q_n) \equiv (p \wedge \neg q_1 \wedge \dots \wedge \neg q_{n-1}) \rightarrow q_n$$

Volem provar $A \Rightarrow (B_1 \vee \dots \vee B_n)$
$A, \neg B_1, \neg B_2, \dots, \neg B_{n-1} \Rightarrow \dots \Rightarrow B_n$

Exercicis: Demostreu, usant prova de la disjunció al conseqüent que:

51. La suma d'un nombre racional i un irracional és irracional (amb contrarecíproc).
52. x, y reals. Si $x + y \leq 2$ llavors $x \leq 1$ o $y \leq 1$.
53. a, b, c són enters. Si $a + 5 = c - b$ llavors a és senar o b és senar o c és senar.
54. x, y, z reals. Si $x < \frac{2y+z}{3}$ llavors $y \geq \frac{2z+x}{3}$ o $z \geq \frac{2x+y}{3}$.
55. a, b, c, d són enters. Si $a + b + c + d$ és parell llavors $a + b$ és parell o $a + c$ és parell o $a + d$ és parell. Podem afirmar que els tres són parells? Val el recíproc?
56. a, b, c són nombres reals positius. Si $c = ab$ llavors $a \leq \sqrt{c}$ o $b \leq \sqrt{c}$.
57. (R) a, b, c, d són nombres reals positius. Si $d = abc$ llavors $a \leq \sqrt[3]{d}$ o $b \leq \sqrt[3]{d}$ o $c \leq \sqrt[3]{d}$.
58. a, b, c són nombres real. Si $c = a + b$ llavors $2a \leq c$ o $2b \leq c$.
59. a, b, c són enters. Si $a + c$ és senar llavors $a + b$ és senar o $b + c$ és senar.
60. a, b, c són enters. Si $a + b + c$ és senar llavors $a - b$ és parell o c és parell.
61. a, b, c són enters. Si $12 + a - b - 3c = 0$ llavors a és parell o $a + 3b$ és

- parell o $a - 5c$ és parell.
62. a, b, c, d són enters. Si $a + b + c + d$ és senar llavors $a + b$ és senar o $a + c$ és senar o $a + d$ és senar. Podem afirmar que els tres són senars? Val el recíproc?
63. x, y, z reals. Si $x < \frac{2y+3z}{5}$ llavors $y \geq \frac{2z+3x}{5}$ o $z \geq \frac{2x+3y}{5}$.
64. a, b, c són enters. Si $1 - a - 3b - 5c = 0$ llavors $a + b + c$ és senar o $a - b - c$ és senar o $a + b - c$ és senar. Podem afirmar que els tres són senars? Val el recíproc?

Disjunció a l'antecedent

Es basa en: $(q \vee r) \rightarrow p \equiv (q \rightarrow p) \wedge (r \rightarrow p)$

És equivalent a fer una prova per casos (distingim segons B o C).

Volem demostrar $(B \vee C) \Rightarrow A$		
B	\Rightarrow	$\Rightarrow A$
C	\Rightarrow	$\Rightarrow A$

També val amb més casos:

Volem demostrar $(B_1 \vee \dots \vee B_n) \Rightarrow A$		
B_1	\Rightarrow	$\Rightarrow A$
	
B_n	\Rightarrow	$\Rightarrow A$

Exercicis: Demostreu, usant prova de la disjunció a l'antecedent que:

65. n és enter. Si el residu de n al dividir per 4 és 1 o 3, el residu de n^2 és 1.
66. n és enter. Si n acaba en 3 o en 7 llavors n^2 acaba en 9 (Pista: n acaba en 9 sii $n = 10k + 9$ per algun k enter).
67. (R) m, n són enters. Si mn és senar llavors m i n són senars (amb contrarecíproc).
68. x és enter. Demostrar que si el residu de dividir x per 6 és 0, 3 o 4 llavors x^2 i x tenen el mateix residu al dividir-los per 6 (Pista: el residu de dividir x per 6 és 4 sii $n = 6k + 4$ per algun k enter. Idem els altres residus).

Prova per casos

Es basa en la tautologia:

$$(p_1 \vee \cdots \vee p_n) \rightarrow (p \leftrightarrow ((p_1 \rightarrow p) \wedge \cdots \wedge (p_n \rightarrow p)))$$

Es pot usar en qualsevol moment.

Volem demostrar B, distingim els casos A_1, \dots, A_n		
<u>Cas 1:</u> A_1		
$A_1 \Rightarrow$	$\Rightarrow B$
...		
<u>Cas n:</u> A_n		
$A_n \Rightarrow$	$\Rightarrow B$

Important: Cal que els diferents casos exhaureixin **totes** les possibilitats (es compleix $A_1 \vee \cdots \vee A_n$).

Exercicis: Demostreu, usant prova per casos que:

- 69. n és enter. $n^2 + n$ és parell (2 casos).
- 70. La suma de dos nombres enters de la mateixa paritat és parell (2 casos).
- 71. Si n és enter, llavors $n^2 \geq n$ (2 o 3 casos).
- 72. Si x, y, z són nombres reals llavors:
 - a. $\max(x, y) + \min(x, y) = x + y$ (2 casos).
 - b. $\max(\max(x, y), z) = \max(x, \max(y, z)) = \max(x, y, z)$ (6 casos).
- 73. Si la suma de dos nombres enters és parell llavors tenen la mateixa paritat. (amb contrarecíproc)
- 74. Si x, y són nombres reals llavors $||x| - |y|| \leq |x - y|$ (6 o 8 casos).
- 75. No hi ha cap quadrat de la forma $3n + 2$.
- 76. n és enter. $3n^2 + n + 3$ es senar (2 casos).
- 77. (R) n és enter. $n^3 + 2n$ es múltiple de 3 (3 casos).
- 78. Tot quadrat perfecte que no és múltiple de 3 és de la forma $3k + 1$ (2 casos).
- 79. n és enter. Si n no és múltiple de 3 llavors $n^2 - 1$ és múltiple de 3 (2 casos).
- 80. Si x, y són nombres reals llavors $|xy| = |x| \cdot |y|$ (4 casos).
- 81. Si x, y, z són nombres reals llavors:
 - a. (R) $z \geq x$ i $z \geq y \Leftrightarrow z \geq \max(x, y)$ (2 casos).
 - b. (R) $\min(\min(x, y), z) = \min(x, \min(y, z)) = \min(x, y, z)$ (6 casos).
 - c. $\max(z + x, z + y) = z + \max(x, y)$ (2 casos).
- 82. El quadrat d'un nombre enter mai acaba en 8 (10 casos).
- 83. Tot cub perfecte és de la forma $9k$ o $9k + 1$ o $9k + 8$ per a algun k (pista: 3 casos).
- 84. m, n són enters. Si $m + n$ és senar llavors mn és parell (2 casos).
- 85. n és enter. El residu de la divisió de n^2 per 4 no és mai 3 (2 casos).
- 86. Si x, y, z són nombres reals llavors:
 - a. $z \leq x$ i $z \leq y \Leftrightarrow z \leq \min(x, y)$ (2 casos).
 - b. $\min(z + x, z + y) = z + \min(x, y)$ (2 casos).

Demostració d'una equivalència

Es basa en: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Volem demostrar	$A \Leftrightarrow B$
$A \Rightarrow B$	
$B \Rightarrow A$	

Equivalència de 3 o més. Es basa en:

$$\begin{aligned}(p_1 \leftrightarrow p_2) \wedge (p_2 \leftrightarrow p_3) \wedge \dots \wedge (p_{n-1} \leftrightarrow p_n) &\equiv \\ &\equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)\end{aligned}$$

Volem demostrar que A_1, A_2, \dots, A_n són equivalents (dos a dos)
$A_1 \Rightarrow A_2$
$A_2 \Rightarrow A_3$
...
$A_{n-1} \Rightarrow A_n$
$A_n \Rightarrow A_1$

Nota: Podem canviar l'ordre dels enunciats A_1, A_2, \dots, A_n

Exercicis: Demostreu que:

87. n és enter. n és senar si i només si $n^2 + 3$ és parell.
88. n, m és enters. Són equivalents:

- a. $5n + 3m$ és senar.
 - b. $n - 3m$ és senar.
 - c. n i m tenen diferent paritat.
89. a, b són reals. Són equivalents:
- a. $a > \frac{a+b}{2}$.
 - b. $a > b$.
 - c. $b < \frac{a+b}{2}$.
90. n és enter. mn és parell si i només si n és parell o m és parell.
91. a, b són racionals. $a + b\sqrt{2}$ racional $\Leftrightarrow b = 0$.
92. (R) n és enter. Són equivalents:
- a. $n = 3k + 1$ per a algun k enter.
 - b. $n^2 + n = 9k + 2$ per a algun k enter.
 - c. $n^2 + n$ no és múltiple de 3.
93. n, m són enters. Són equivalents:
- a. n i m tenen la mateixa paritat
 - b. $n + m$ és parell
 - c. $n - m$ és parell
94. n és enter. Són equivalents:
- a. n parell,
 - b. $n + 1$ senar,
 - c. $3n^2 + 1$ senar.
95. x és real. Són equivalents:
- a. x és racional,
 - b. $3x - 1$ és racional,
 - c. $(x + 1)/2$ és racional.
96. (R) a, b són reals. Són equivalents (pista: $(a - b)^2 \geq 0$):
- a. $a^2 + b^2 = 2ab$
 - b. $a^2 + b^2 \leq 2ab$
 - c. $a = b$
97. a, b són reals positius. Són equivalents:
- a. $a > \sqrt{ab}$
 - b. $a > b$
 - c. $b < \sqrt{ab}$
98. n és enter. Són equivalents:
- a. El residu de dividir n per 4 és 3.

- b. $n(n + 2)(n + 3)$ no és múltiple de 4.
- c. $2n^2 + n - 1$ és múltiple de 4.
99. n és enter. Són equivalents:
- a. n és el producte de dos enters consecutius.
- b. $4n + 1$ és un quadrat.
100. x és real. Són equivalents:
- a. x irracional.
- b. $x + 1$ irracional.
- c. $x/3$ és irracional .
101. a, b són enters. Són equivalents:
- a. $a + b, ab$ parells.
- b. a, b parells.
- c. $a + b, a + 2b$ parells .
102. a, b, c són reals. Són equivalents:
- a. $a > \frac{b+c}{2}$
- b. $a > \frac{a+b+c}{3}$
- c. $a - b > \frac{c-b}{2}$

Demostració de la unicitat

Quan diem que “*si hi ha un x que satisfà $P(x)$ aquest és únic*” volem dir que *hi ha com a molt un x satisfent $P(x)$* . O també que *no hi ha dos x diferents que satisfacin $P(x)$* . Ho podem expressar així: $\neg \exists x \exists y (x \neq y \wedge P(x) \wedge P(y))$. Aquesta fórmula és equivalent a:

$$\forall x \forall y (P(x) \wedge P(y) \rightarrow x = y)$$

Volem veure: hi ha com a molt un x tal que $P(x)$.		
$P(x), P(y)$	\Rightarrow	$\Rightarrow x = y$

Nota: No afirmem que l'element x existeixi, potser no n'hi ha cap x satisfent $P(x)$. Quan volem veure que "hi ha un únic x tal que $P(x)$ " haurem de veure dues coses: que l'element x existeix i que és únic. **Exemple:** El quocient i el residu de la divisió euclidiana existeixen i són únics.

Exercicis: Demostreu que:

- 103. En tota operació $(A, *)$ el neutre (u és neutre sii $\forall x \in A (x * u = u * x = x)$), en cas d'existir, és únic.
- 104. (R) La inversa d'una matriu, si existeix, és única.
- 105. En una operació $(A, *)$ associativa amb neutre u , l'invers y d'un element x (aquell element y que verifica $x * y = y * x = u$), si existeix, és únic.

1.3 Apèndix: Passos no lògics

En aquest apèndix intentarem donar una llista força exhaustiva de propietats o passos bàsics no lògics. I els presentarem per grups.

*El color vermell indica que són propietats bàsiques (**axiomes**) a partir de les quals es poden demostrar totes les altres.*

Propietats de la igualtat (aquí a, b, c, \dots són nombres reals):

1. $a = a$ (reflexiva)
2. $a = b \Rightarrow b = a$ (simètrica)
3. $a = b, b = c \Rightarrow a = c$ (transitiva)
4. $a = b \Rightarrow E(a) = E(b)$ (aquí $E(x)$ és una expressió on apareix x)
5. $a = b \Rightarrow a + c = b + c$
6. $a = b \Rightarrow ac = bc$
7. $a = b \Rightarrow a^2 = b^2$
8. $a = b, a' = b' \Rightarrow a + a' = b + b'$
9. $a = b, a' = b' \Rightarrow aa' = bb'$

Exercici: Demostreu que totes les propietats 5,6,7,... surten de les 4 primeres (pista: prendre $E(x)$ adequades).

Propietats de la suma i el producte (aquí a, b, c, \dots són nombres reals):

1. $a + (b + c) = (a + b) + c$ (Associativa de la suma)
2. $a + b = b + a$ (Commutativa de la suma)
3. $a + 0 = a$ (0 és el neutre de la suma)
4. $a + (-a) = 0$ ($-a$ és l'invers de a per la suma)
5. $a(bc) = (ab)c$ (Associativa del producte)
6. $ab = ba$ (Commutativa del producte)
7. $a1 = a$ (1 és el neutre del producte)
8. $a \neq 0 \Rightarrow a \cdot (1/a) = 1$ ($1/a$ és l'invers de a pel producte)

$$9. a(b + c) = ab + ac \quad (\text{distributiva})$$

Propietats de l'ordre (aquí a, b, c, \dots són nombres reals):

1. $a \leq a$ (reflexiva de \leq)
2. $a \leq b, b \leq a \Rightarrow a = b$ (antisimètrica de \leq)
3. $a \leq b, b \leq c \Rightarrow a \leq c$ (transitiva de \leq)
4. $a \leq b$ o $b \leq a$ (total)
5. $a \leq b \Rightarrow a + c \leq b + c$ (compatibilitat amb la suma)
6. $a \leq b, c \geq 0 \Rightarrow ac \leq bc$ (compatibilitat amb el producte)
7. $a \leq b, c \leq d \Rightarrow a + c \leq b + d$
8. $a \leq b \Rightarrow -b \leq -a$
9. $a^2 \geq 0$
10. $0 \leq a \leq b, 0 \leq c \leq d \Rightarrow ac \leq bd$
11. $0 \leq a \leq b \Rightarrow a^2 \leq b^2$
12. És cert $(a \leq b \Rightarrow a^2 \leq b^2)$?
13. $a \leq b \Rightarrow a^3 \leq b^3$
14. (n natural parell) $0 \leq a \leq b \Rightarrow a^n \leq b^n$
15. (n natural senar) $a \leq b \Rightarrow a^n \leq b^n$
16. El recíproc de l'anterior

Exercici: Demostreu que totes aquestes propietats es dedueixen de les **6 primeres**. Demostreu també les següents tenint en compte que $a < b$ és una abreviatura de $a \leq b \wedge a \neq b$.

17. $a < b, b < c \Rightarrow a < c$.
18. $a < b$ o $a > b$ o $a = b$.
19. $a < b \Rightarrow a + c < b + c$.
20. $a < b, c > 0 \Rightarrow ac < bc$.
21. $a < b, c \leq d \Rightarrow a + c < b + d$.
22. $a < b \Rightarrow -b > -a$.
23. $0 < a < b \Rightarrow a^2 < b^2$.
24. És cert $(a < b \Rightarrow a^2 < b^2)$?

25. $a < b \Rightarrow a^3 < b^3$.
26. (n natural parell) $0 < a < b \Rightarrow a^n < b^n$.
27. (n natural senar) $a < b \Rightarrow a^n < b^n$.
28. El recíproc de l'anterior.

Altres:

1. a natural, b natural $\Rightarrow a + b$ natural, ab natural.⁸
2. a enter, b enter $\Rightarrow -a$ enter, $a + b$ enter, ab enter.
3. a racional, b racional $\Rightarrow -a$ racional, $a + b$ racional, ab racional.
4. b racional, $b \neq 0 \Rightarrow 1/b$ racional.
5. a racional, b racional, $b \neq 0 \Rightarrow a/b$ racional.

Exercici: Demostreu que totes surten de la **primera** (pista: un **enter** és un element de la forma $\pm a$ amb a natural. Un **racional** és un nombre de la forma n/m amb n, m enters, $m \neq 0$).

A vegades les implicacions \Rightarrow són reversibles i podem usar el \Leftrightarrow en lloc de la implicació. Per exemple, els axiomes 5 i 8 de l'ordre són reversibles, mentre que el

11 no ho és.

⁸ Podem definir els naturals així: **0 és natural i si a és natural, $a+1$ és natural**. No hi ha més naturals que els que es construeixen aplicant un nombre finit de vegades aquestes regles.

2. INDUCCIÓ



2.1 Inducció simple

El mètode de demostració per inducció simple es basa en el principi següent:

$$\forall n \geq n_0 P(n) \quad \equiv \quad P(n_0) \wedge \forall n > n_0 (P(n-1) \rightarrow P(n))$$

Volem demostrar	$\forall n \geq n_0 P(n)$
$P(n_0)$ $\forall n > n_0 (P(n - 1) \rightarrow P(n))$	

Ho presentem així:

-
- Pas Base. $P(n_0)$
 - Pas inductiu. Sigui $n > n_0$:
 - Hipòtesi d'Inducció: $P(n - 1)$
 - Volem veure(Tesi d'Inducció): $P(n)$

En efecte:

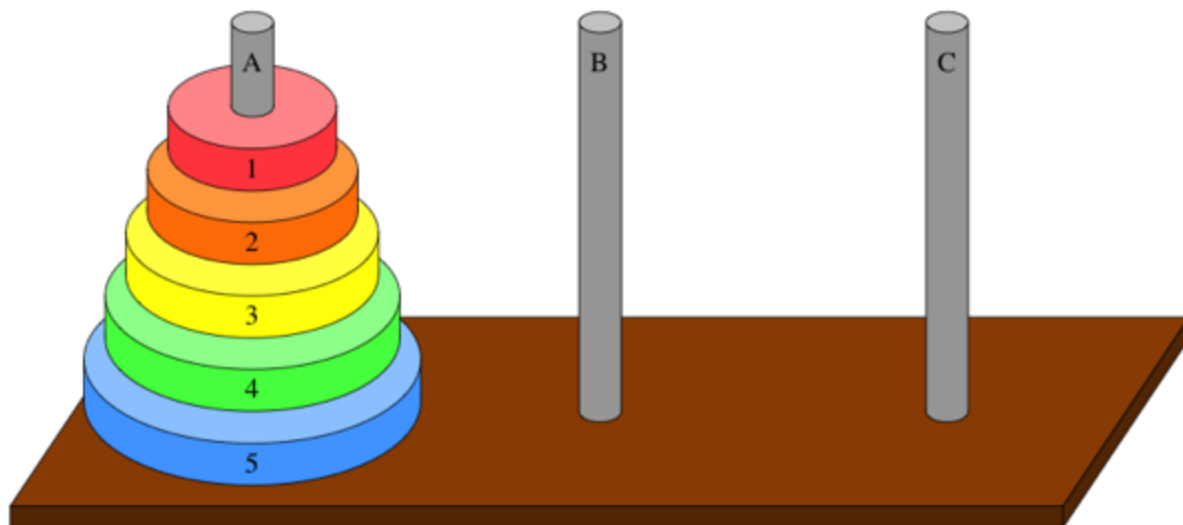
Exercicis:

1. $\sum_{i=0}^n i = \frac{n(n+1)}{2}$ per a $n \geq 0$.
2. $\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$ per a $n \geq 1$.
3. $\sum_{i=1}^n \frac{1}{(4i-3)(4i+1)} = \frac{n}{4n+1}$ per a $n \geq 1$.
4. $\prod_{k=2}^n (1 - \frac{1}{k}) = \frac{1}{n}$ per a $n \geq 2$.
5. $\prod_{i=1}^n (1 + \frac{2}{i}) = \frac{(n+1)(n+2)}{2}$ per a $n \geq 1$.
6. $3^n < (n + 2)!$ per a $n \geq 0$.

7. $\sum_{i=2}^n 1/i^2 < \frac{n-1}{n}$ per a $n \geq 2$.
8. La successió de Fibonacci es defineix així: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ per a tot $n > 1$. El nombre d'or és el nombre $\phi = \frac{1+\sqrt{5}}{2}$, que satisfà $\phi^2 = \phi + 1$. Demostreu que $\phi^n = F_n \phi + F_{n-1}$ per a tot $n \geq 1$.
9. La successió de Fibonacci es defineix així: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ per a tot $n > 1$. Demostreu que $F_0^2 + \dots + F_n^2 = F_n F_{n+1}$ per a tot $n \geq 0$.
10. Demostreu que $6^{2n+1} - 6$ és múltiple de 210 per a $n \geq 0$.
11. Demostreu que $11^{n+1} + 12^{2n-1}$ és múltiple de 133 per a $n \geq 1$.
12. (difícil) Demostreu per inducció sobre n que les tres últimes xifres de 11^n coincideixen amb les de $50n^2 - 40n + 1$.
13. En aquest exercici calcularem el nombre de multiplicacions més divisions (les sumes no les comptem, tenen una complexitat inferior) que cal fer per a triangular un matriu $n \times n$ pel mètode de Gauss. Denotem per a_n el nombre de multiplicacions més divisions que efectuem amb el mètode de Gauss. Demostreu que $a_1 = 0$ i que $a_n = n(n-1) + a_{n-1}$ quan $n > 1$. Demostreu per inducció que $a_n = \frac{n^3-n}{3}$ per a tot $n \geq 1$.
14. Aquest exercici és una generalització de l'anterior: calcularem el nombre de multiplicacions més divisions que cal fer per a triangular una matriu $n \times m$ (amb n files i m columnes) pel mètode de Gauss quan $n \leq m$. Denotem per $f(n, m)$ el nombre de multiplicacions més divisions que efectuem amb el mètode de Gauss al triangular una matriu amb n files i m columnes. Demostreu que $f(1, m) = 0$ i que $f(n, m) = m(n-1) + f(n-1, m-1)$ quan $n > 1$. Demostreu per inducció sobre n que $f(n, m) = \frac{n(n-1)(3m-n+2)}{6}$ per a tot $n \geq 1$.
15. En aquest exercici calcularem el nombre de multiplicacions (les sumes no les comptem, tenen una complexitat inferior) que cal fer per a calcular el determinant d'una matriu desenvolupant per files o columnes. Denotem per

a_n el nombre de multiplicacions que efectuem al desenvolupar una matriu $n \times n$ per files o columnes. Demostreu que $a_1 = 0$ i que $a_n = na_{n-1} + n$ quan $n > 1$. Demostreu per inducció que $n! \leq a_n < n \cdot n!$ per a tot $n \geq 2$.

16. Calculeu el mínim nombre de passos per resoldre el problema de les **torres de Hanoi** amb n discs. (Pista: considereu $f(n)$ el mínim nombre de passos per resoldre el problema amb n discs i trobeu una fórmula recurrent per calcular $f(n)$).



17. Sigui $n \geq 1$. Demostreu per inducció que si suprimim un quadrat 1×1 a un tauler d'escacs de mida $2^n \times 2^n$, la resta es pot cobrir amb peces com les de la figura.



18. Definim la successió geomètrica a_m, a_{m+1}, \dots, a_n mitjançant $a_{i+1} = a_i r$.

Demostreu que
$$\sum_{i=m}^n a_i = \frac{a_{n+1} - a_m}{r - 1}.$$

19. (difícil) Definim recursivament les fórmules φ_n així:

$$\varphi_1 = p_1 \text{ i per a } n > 1 \text{ } \varphi_n = \varphi_{n-1} \leftrightarrow p_n.$$

Aquí $p_1, p_2, \dots, p_n, \dots$ són lletres proposicionals. Observeu que les lletres que apareixen a φ_n són p_1, p_2, \dots, p_n . Si $v: \{p_1, p_2, \dots, p_n, \dots\} \rightarrow \{0, 1\}$ és una assignació de valors de veritat a les lletres $p_1, p_2, \dots, p_n, \dots$, demostreu per

inducció, que per a tot $n \geq 1$ són equivalents:

- v fa certa φ_n
- el nombre de zeros que assigna v a les lletres p_1, p_2, \dots, p_n és parell.

$$20. \sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6} \text{ per a } n \geq 1.$$

$$21. \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1} \text{ per a } n \geq 1.$$

$$22. (R) \sum_{i=1}^n \frac{i}{2^i} = 2 - \frac{n+2}{2^n} \text{ per a } n \geq 1.$$

$$23. \sum_{i=0}^n 2^i i! (2i+1) = 2^{n+1} (n+1)! - 1 \text{ per a } n \geq 0.$$

$$24. (R) \prod_{i=3}^n \left(1 - \frac{2}{i}\right) = \frac{2}{n(n-1)} \text{ per a } n \geq 3.$$

25. (R) Definim una successió recurrent mitjançant $a_0 = -2$ i $a_n = 3a_{n-1} + 6$ per a $n > 0$. Demostreu per inducció que $a_n = 3^n - 3$ per a tot $n \geq 0$.

$$26. 4^n < n! \text{ per a } n \geq 9.$$

$$27. (R) \sum_{i=0}^n \frac{1}{2^{i+1}} \leq n/3 + 1 \text{ si } n \geq 0.$$

28. Demostreu per inducció que per a tot $n \geq 0$, $15 \cdot 2^{3n+2} + 8(-9)^n$ és múltiple de 68.

$$29. (1+x)^n \geq 1 + nx \text{ (} n \geq 0, x \geq 0 \text{)}.$$

30. La successió de Fibonacci es defineix així: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ per a tot $n > 1$. Demostreu que $F_0 + F_1 + \dots + F_n = F_{n+2} - 1$ per a tot $n \geq 0$.

31. Definim la successió aritmètica a_m, a_{m+1}, \dots, a_n mitjançant $a_{i+1} = a_i + d$.

Demostreu que per a tot $n \geq m$:

$$\sum_{i=m}^n a_i = \frac{(a_m + a_n)(n-m+1)}{2}.$$

32. (difícil). Demostreu que $\left(\frac{n}{e}\right)^n < n!$ per a $n \geq 1$ (Pista: useu que

$$\left(1 + \frac{1}{n}\right)^n < e).$$

33. (R) Demostreu que $2^{3n+1} + 3 \cdot 5^{2n+1}$ és múltiple de 17 per a $n \geq 0$.

34. Demostreu que $5^{2n+1} - 120n - 5$ és múltiple de 576 per tot $n \geq 0$

35. Demostreu que $\sum_{i=1}^n i!$ és de la forma de $90k + 63$ per a $n \geq 5$.

36. Calculeu unes quantes potències de la matriu

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Conjectureu una fórmula per a calcular A^n i demostreu-la per inducció. (per si no la “trobeu” [aquí](#) teniu la fórmula) .

37. $\sum_{i=2}^n \frac{i-1}{i!} = 1 - \frac{1}{n!}$ per a $n \geq 2$.

38. $\sum_{i=1}^n 1/i \leq n/2 + 1$ si $n \geq 1$.

39. Demostreu que $2 \cdot 3^n + 5^{2n-1}$ és múltiple de 11 per a $n \geq 1$.

40. Definim una successió recurrent mitjançant $a_0 = 1$, $a_n = na_{n-1} + 1$ per a

$n > 0$. Demostreu per inducció que $\sum_{i=0}^n \frac{1}{i!} = \frac{a_n}{n!}$ per a tot $n \geq 0$ (càlcul del nombre e).

41. Demostreu que la suma dels angles interiors d'un polígon de n costats és $180(n - 2)$ per a $n \geq 3$.

42. (difícil). $\sum_{i=1}^n 1/i \leq \log_2 n$, si $n \geq 5$ (Pista: useu el binomi Newton).

Variant: A vegades és necessari fer més d'un cas inicial:

Ho presentem així:

-
- Pas Base. $P(n_0), \dots, P(n_1)$
 - Pas inductiu. Sigui $n > n_1$:
 - Hipòtesi d'Inducció: $P(n - 1)$
 - Volem veure: $P(n)$

En efecte:

Exemple: $5^n \leq 27n!$ per a $n \geq 0$.

2.2 Inducció completa

El mètode de demostració per inducció completa es basa en el principi següent:

$$\forall n \geq n_0 P(n) \quad \equiv \quad P(n_0) \wedge \forall n > n_0 \left(P(n_0) \wedge \dots \wedge P(n - 1) \rightarrow P(n) \right)$$

Volem demostrar	$\forall n \geq n_0 P(n)$
$P(n_0)$ $\forall n > n_0 \left(P(n_0) \wedge \dots \wedge P(n - 1) \rightarrow P(n) \right)$	

Ho fem així:

- Pas Base: $P(n_0)$
- Pas inductiu: per a $n > n_0$:

- H.I. $P(n_0), \dots, P(n-2), P(n-1)$
- Volem veure: $P(n)$

En efecte:

Exercicis:

43. En un determinat país, per a cada dues ciutats hi ha una carretera d'un sol sentit que les uneix sense passar per cap altre ciutat. Demostreu que es pot fer un recorregut passant per totes les ciutats un sol cop. Pista: trieu una ciutat C i considereu d'una banda totes les ciutats a les que es pot anar desde C i de l'altra totes desde les quals es pot anar a C .
 44. Demostreu que si tenim una rajola de xocolata de de $n \times m$ preses, es faci com es faci s'han de fer $nm - 1$ talls (trencar una de les peces en dues) per deixar-la en trossos d'una presa.
 45. Demostreu que tot nombre enter $n \geq 2$ es primer o es descompon en producte de primers. És a dir, $n = p_1 \cdots p_k$ per a algun $k \geq 1$ i primers p_1, \dots, p_k . (Pista: Useu que si un enter positiu n no és primer llavors $n = rs$ per a uns certs r, s enters, amb $2 \leq r, s < n$).
 46. Definim una funció recursivament així: $f(1) = 0$ $f(n) = 2f(E(n/2)) + n$, si $n > 1$. Demostreu que $f(n) \leq n \log_2 n$ per a $n \geq 1$. (Pista: useu que $2E(n/2) \leq n$. Aquí demostrem que el nombre de comparacions que es fa amb Mergesort és $\leq n \log_2 n$).
- Nota: $E(x)$ és la part entera inferior del nombre real x .
47. Definim una funció recursivament així: $f(1) = 0$ i per a $n > 1$ $f(n) = f(n/p) + 1$, on p és el primer més petit que divideix n . Qui és $f(n)$? Demostreu-ho per inducció.
 48. La longitud de una fórmula proposicional és el nombre total de símbols (comptant parèntesis i repeticions) que té. Aquí no suprimim els parèntesis exteriors. Demostreu que: $l(\varphi) = n(\varphi) + 4cb(\varphi) + 1$ ($l(\varphi)$ és la longitud de φ , $n(\varphi)$ és el nombre de negacions de φ i $cb(\varphi)$ és el nombre de connectives binàries de φ). Doneu una definició recursiva de la longitud de la fórmula.

49. Definim una successió recursivament així: $x_1 = 1$ i per a tot $n > 1$

$$x_n = x_{n-1} + 2x_{n-2} + 2^2x_{n-3} + \dots + 2^{n-2}x_1 + 2^{n-1}. \quad \text{Demostreu que}$$

$$x_n = 3^{n-1} \text{ per a } n \geq 1.$$

50. Els joc dels mistos. Hi ha dues piles amb el mateix nombre de mistos i dos jugadors. Cada jugador tria una pila i treu com a mínim un misto d'aquesta pila. Juguen alternativament. El joc acaba quan no queden mistos i guanya l'últim que treu mistos. Demostreu que si el segon jugador treu cada cop els mateixos mistos que el primer però de l'altre pila, guanya.

51. (difícil) Definim $x_1 = 1$, $x_{2r} = 2x_r$, $x_{2r+1} = 2x_{r+1}$ per $r > 0$. Demostreu

$$\text{que } x_n = 2^{ES(\log_2 n)} \text{ per a } n \geq 1.$$

Nota: $ES(x)$ és la part entera superior del nombre real x .

Aquesta és la versió **amb més casos inicials** (Se suposa que $n_0 \leq n_1$):

-
- Pas Base: $P(n_0), P(n_0 + 1), \dots, P(n_1)$
 - Pas inductiu: per a $n > n_1$:
 - H.I. $P(n_0), P(n_0 + 1), \dots, P(n - 1)$
 - Volem veure: $P(n)$
-

Exercicis:

52. La successió de Fibonacci es defineix així: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

per a tot $n > 1$. La raó d'or és el nombre $\phi = \frac{1+\sqrt{5}}{2}$, que satisfà $\phi^2 = \phi + 1$

. Demostreu que $F_n \geq \phi^{n-2}$ per a tot $n \geq 1$.

53. Definim una successió a_n recursivament fent $a_0 = 0, a_1 = 2,$

$$a_n = 4a_{n-1} - 4a_{n-2} \text{ per a } n \geq 2. \text{ Demostreu que } a_n = n2^n \text{ per a } n \geq 0.$$

54. Demostreu que tot $n \geq 12$ es pot posar de la forma $n = 5a + 4b$ amb a, b naturals. (Pista: considereu 4 casos inicials).
55. Definim una successió a_n recursivament fent $a_0 = 1, a_1 = 1, a_2 = 0$,
 $a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3} + 2$ per a $n > 2$. Demostreu que
 $a_n = 2^n - n^2$ per a $n \geq 0$.
56. (R) Definim una successió a_n recursivament fent $a_1 = 3, a_2 = 5$,
 $a_n = 3a_{n-1} - 2a_{n-2}$ per a $n > 2$. Demostreu que $a_n = 2^n + 1$ per a $n \geq 1$.
57. Definim una successió a_n recursivament fent $a_0 = 1, a_1 = 2, a_2 = 6$,
 $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ per a $n > 2$. Demostreu que
 $a_n = 1 - 2^n + 3^n$ per a $n \geq 0$.
58. El problema de les piles. Tenim una pila de n caixes i la volem convertir en n piles d'una caixa. Això ho farem subdividint cada pila de k caixes en dues piles de r i s caixes, on $r + s = k, r, s > 0$. Li demanem a un operari que efectui aquesta feina i cada vegada que divideix una pila de $r + s$ caixes en dues piles de r i s caixes li paguem rs euros. Demostreu que al final, independentment de l'estratègia que l'operari hagi seguit, si al principi hi ha n caixes, li pagarem $n(n - 1)/2$ euros.
59. Només tenim monedes de 3 i de 4 cèntims. Demostreu que per a tot $n \geq 9$ es pot pagar una factura de n cèntims amb monedes de 3 i 4 cèntims (Pista: feu 3 casos inicials).
60. Definim una funció així: $f(1) = 2$, si $n \geq 2, f(n) = (f(n/p))^2$, on p és el primer més petit que divideix n . Demostreu per inducció que per a tot $n \geq 2$, si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ és la descomposició en factors primers de n llavors

$$f(n) = 2^{2^{\alpha_1 + \dots + \alpha_k}}.$$
61. Considerem la funció definida recursivament per $f(n) = n$ si $n \leq 2$,
 $f(n) = f(E(n/3)) + f(ES(2n/3))$, altrament. Aquí $E(x)$ i $ES(x)$ denoten la part entera i la part entera superior del nombre real x respectivament. Demostreu que per a tot $n \geq 1$ tenim que $f(n) \leq 2n - 1$ (Pista: useu que

- $E(n/3) + ES(2n/3) = n$.
62. Definim recursivament una funció així: $f(1) = 1$, $f(n) = f(E(n/2)) + 1$, si $n > 1$. Demostreu que $f(n) \leq \log_2 n + 1$ per a $n \geq 1$.
63. Definim una funció recursivament així: $f(0) = 0$, $f(n) = 4f(E(n/4)) + n$, si $n > 0$. Demostreu que $f(n) \leq n \log_4 n + 1$ per a tot $n \geq 1$.
64. Demostreu que tot nombre enter $n \geq 0$ es pot escriure en base 2, és a dir, és una suma de potències de 2. (Pista: feu la divisió euclidiana per 2).
65. Tenim una successió de nombres reals que sabem que compleix $a_1 = 0$, $a_p = 1$ si p és primer i $a_{nm} \leq 2a_n + a_m$. Demostreu que per a tot $n \geq 2$ si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ és la descomposició en factors primers de n , llavors $a_n \leq 2\alpha_1 + \cdots + 2\alpha_k - 1$.
66. Definim $a_0 = 1$, $a_n = a_0 - a_1 + \cdots + (-1)^{n-1} a_{n-1}$ si $n > 0$. Demostreu que $a_n = 0$ per a $n \geq 2$.
67. (Dues induccions)
- Demostreu per inducció simple que per a tot $n \geq 2$ $1 + 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + (n-1) \cdot (n-1)! = n!$.
 - Definim $a_1 = 1$, $a_n = a_1 + 2a_2 + \cdots + (n-1)a_{n-1}$ per $n \geq 2$. Demostreu per inducció completa que $a_n = n! / 2$ per $n \geq 2$. (Pista: useu l'apartat a.)
68. Definim $x_1 = 1$, $x_{2r} = 2x_r$, $x_{2r+1} = 2x_{r+1}$ per $r > 0$. Demostreu que $x_n \leq n^2$ per a $n \geq 1$.
69. Definim recursivament l'altura de una fórmula proposicional φ així: $h(p) = 0$, $h(\neg\varphi) = 1 + h(\varphi)$, $h(\varphi * \psi) = \max\{h(\varphi), h(\psi)\} + 1$.
- Demostreu que el nombre de lletres proposicionals de φ és $\leq 2^{h(\varphi)}$.
 - Demostreu que per a cada $n \geq 0$ hi ha una fórmula d'altura n que compleix la igualtat.
 - (difícil) Demostreu que per a cada $n \geq 0$ i cada m amb $1 \leq m \leq 2^n$ existeix una fórmula d'altura n amb exactament m lletres

proposicionals (comptant repeticions). (Pista: feu inducció completa sobre n . Useu que tot nombre $\leq 2^n$ és de la forma $2^r + s$ amb $r < n$ i $s \leq 2^r$).

3. CONJUNTS I RELACIONS

3.1 CONJUNTS

Els conjunts són un nou tipus d'objecte. **Idea:** Mena de “contenedor” que conté certs objectes a l'interior, de manera desordenada. Només importa quins objectes hi són i quins no. També podem pensar en una espècie de llista on no importa l'ordre i no hi poden haver repeticions. No podem “cridar” el primer element, només podem preguntar si un determinat objecte hi és o no (això és un Booleà, que els matemàtics anomenen “funció característica”).

Quan un objecte x és al conjunt A direm que x **és un element de** A o que x **pertany** a A . Ho denotem per $x \in A$.

Quan un objecte x no és al conjunt A direm que x **no és un element de** A o que x **no pertany** a A . Ho denotem per $x \notin A$.

Notem que: quan posem $x \in A$, A ha de ser conjunt, mentre que x pot ser qualsevol tipus d'objecte.

Descripció d'un conjunt

Per descriure un conjunt hem de dir quins elements té (i quins no té). Hi ha dues maneres de fer-ho:

Per **extensió:** Donem la “llista” dels seus elements entre claus(cal recordar que no hi ha repeticions i no importa l'ordre: els podem ordenar de qualsevol manera):

$$A = \{1, 3, 5, 7, 9\}.$$

Per **comprensió:** Donem una propietat $P(x)$ que caracteritza els seus elements (una propietat $P(x)$ que tenen tots els seus elements i ningú més):

$$A = \{x \mid P(x)\}.$$

Exemple:

- $A = \{x \mid x \text{ és enter senar, } 0 \leq x \leq 10\}.$
- $B = \{x \mid x \in \mathbb{Z}, x \text{ és parell}\}.$

Notem que: Si $A = \{x \mid P(x)\}$ llavors,

$$\begin{array}{l} \text{per a tot } x: \\ x \in A \Leftrightarrow P(x) \end{array}$$

Notació alternativa

Si volem definir el conjunt de tots els elements de B que satisfan la propietat P es pot fer alternativament així:

$$\{x \in B \mid P(x)\} = \{x \mid x \in B, P(x)\}$$

Exemple: $\{x \in \mathbb{Z} \mid x \text{ és parell}\} = \{x \mid x \in \mathbb{Z}, x \text{ és parell}\}.$

Notem que: Si $A = \{x \in B \mid P(x)\}$ llavors

$$\begin{array}{l} \text{per a tot } x \in B: \\ x \in A \Leftrightarrow P(x) \end{array}$$

Però **no** es compleix per a tot x (hi poden haver $x \notin B$ que compleixin $P(x)$)

Igualtat entre conjunts (principi d'extensionalitat)

El que caracteritza un conjunt són els elements que té (i els que no té). Expressat més clarament, dos conjunts A, B són iguals si i només si tenen els mateixos elements:

$$A = B \Leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$$

Exemple: els conjunts $\{1, 3, 5, 7, 9\}$ i $\{x \mid x \text{ és enter senar}, 0 \leq x \leq 10\}$ són iguals. Són el mateix conjunt!

Conjunt buit

És el conjunt que no té elements i es denota per \emptyset :

$$\emptyset = \{\} = \{x \mid x \neq x\}$$

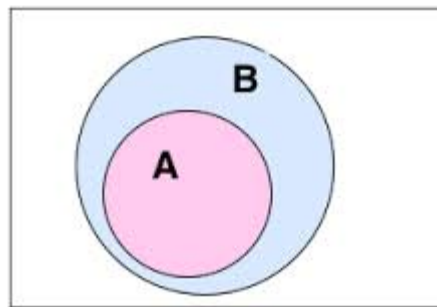
Inclusió entre conjunts (\subseteq)

Idea: A és una “part” de B : A conté “alguns” (potser tots!) dels elements de B . Aquesta idea s’expressa més clarament dient que tots els elements de A també són elements de B :

Definició:

$$A \subseteq B \quad \Leftrightarrow \quad \forall x (x \in A \rightarrow x \in B)$$

Es llegeix dient que A és **subconjunt de** B (o que A està **inclòs** a B)



Exemple: Si $A = \{1, 3, 5\}$, $B = \{1, 3, 5, 7, 9\}$ llavors $A \subseteq B$.

Notem que: el principi de extensionalitat es pot expressar així:

$$A = B \quad \Leftrightarrow \quad A \subseteq B, B \subseteq A$$

Per tant, quan volem demostrar una igualtat entre conjunts, tenim una segona manera de fer-ho: demostrar les dues inclusions.

Propietats:

-
- I. $\emptyset \subseteq A$.
 - II. $A \subseteq A$.
 - III. $A \subseteq B$ i $B \subseteq C$ implica $A \subseteq C$.
-

Exercicis:

1. Siguin $X = \{1, 2, 3, 4\}$, $Y = \{\{1, 2\}, \{3, 4\}\}$, $Z = \{\{1\}, \{2, 3\}, \{4\}\}$. Dieu quines afirmacions són certes i quines són falses:
 - $1 \in X, 1 \in Y, 1 \in Z$.
 - $\{1\} \in X, \{1\} \in Y, \{1\} \in Z, \{1\} \subseteq X, \{1\} \subseteq Y, \{1\} \subseteq Z$.
 - $\{\{1\}\} \in X, \{\{1, 2\}\} \in Y, \{\{1\}\} \in Z, \{\{1\}\} \subseteq X, \{\{1, 2\}\} \subseteq Y, \{\{1\}\} \subseteq Z$.
 - $\{3, 4\} \in X, \{3, 4\} \in Y, \{3, 4\} \in Z, \{3, 4\} \subseteq X, \{3, 4\} \subseteq Y, \{3, 4\} \subseteq Z$.
2. Demostreu que les dues fórmules següents són equivalents:
 - a. $\forall x (x \in A \leftrightarrow x \in B)$.
 - b. $\forall x (x \in A \rightarrow x \in B) \wedge \forall x (x \in B \rightarrow x \in A)$.
3. Demostreu les propietats I., II. i III. anteriors.

Operacions amb conjunts

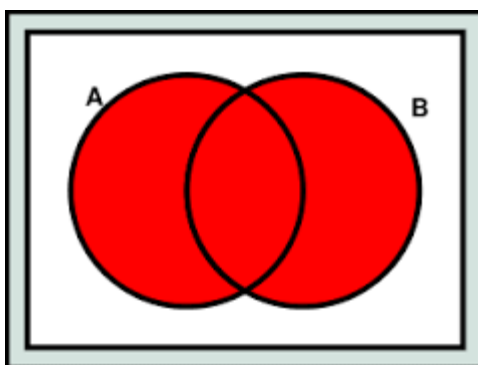
Unió

Donats dos conjunts A i B definim el **conjunt unió** de A i B així:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Això es pot expressar de manera equivalent així:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$



Exemples:

- Si $A = \{1, 3, 5, 7, 9\}$ i $B = \{5, 6, 7, 8, 9, 10\}$
 $A \cup B = \{1, 3, 5, 6, 7, 8, 9, 10\}$.
- Si $A = \{x \in \mathbb{Z} \mid x \text{ és parell}\}$ i $B = \{x \in \mathbb{Z} \mid x \text{ és senar}\}$
 $A \cup B = \mathbb{Z}$.

Propietats:

-
- I. $A \cup A = A$.
 - II. $A \cup \emptyset = A$.
 - III. $A \cup B = B \cup A$.
 - IV. $A \cup (B \cup C) = (A \cup B) \cup C$.
 - V. $A \subseteq A \cup B$, $B \subseteq A \cup B$.
 - VI. $A \subseteq B \Leftrightarrow A \cup B = B$.
 - VII. $A \cup B \subseteq C \Leftrightarrow A \subseteq C, B \subseteq C$.
-

Exercicis:

4. Demostreu les propietats I., III., V. anteriors.
5. Demostreu les propietats II.(R), VI. anteriors.
6. Demostreu les propietats IV. i VII. anteriors.

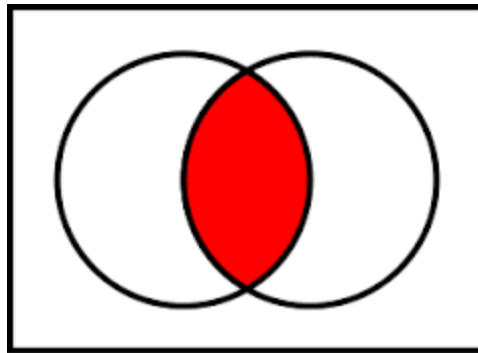
Intersecció

Donats dos conjunts A i B definim el **conjunt intersecció** de A i B així:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Això es pot expressar de manera equivalent així:

$$x \in A \cap B \Leftrightarrow x \in A \text{ i } x \in B$$



Exemple:

- Si $A = \{1, 3, 5, 7, 9\}$ i $B = \{5, 6, 7, 8, 9, 10\}$
 $A \cap B = \{5, 7, 9\}$.
- Si $A = \{x \in \mathbb{Z} \mid x \text{ és parell}\}$ i $B = \{x \in \mathbb{Z} \mid x \text{ és senar}\}$
 $A \cap B = \emptyset$.

Propietats:

- I. $A \cap A = A$.
 - II. $A \cap \emptyset = \emptyset$.
 - III. $A \cap B = B \cap A$.
 - IV. $A \cap (B \cap C) = (A \cap B) \cap C$.
 - V. $A \cap B \subseteq A, A \cap B \subseteq B$.
 - VI. $A \subseteq B \Leftrightarrow A \cap B = A$.
 - VII. $C \subseteq A \cap B \Leftrightarrow C \subseteq A \text{ i } C \subseteq B$.
-

Exercicis:

- 7. Demostreu les propietats IV. i V. anteriors.
- 8. Demostreu les propietats I., III. i VII.(R) anteriors.
- 9. Demostreu les propietats II. i VI. anteriors.

Quan dos conjunts A, B no tenen elements comuns es diu que són **disjunts**:

$$A \text{ i } B \text{ són disjunts} \Leftrightarrow A \cap B = \emptyset$$

Exercicis. Expresses mitjançant quantificadors i \in el fets següents:

- 10. $A = \emptyset$.
- 11. $\neg (A \subseteq B)$.
- 12. $A \subset B$. ($A \subset B$ vol dir $A \subseteq B$ i que són diferents)
- 13. $A \neq \emptyset$.
- 14. $\neg (A \subset B)$.
- 15. (R) A i B no són disjunts.
- 16. A i B son disjunts.
- 17. $A \neq B$.

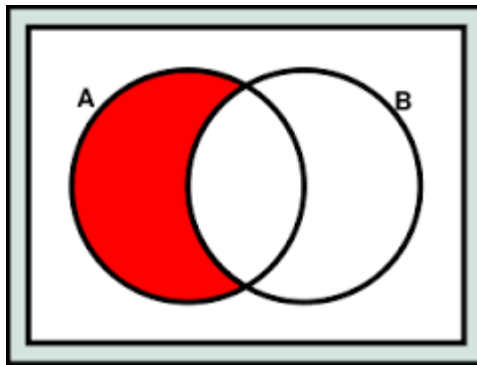
Diferència

Donats dos conjunts A i B definim el **conjunt diferència** de A i B així:

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Això es pot expressar de manera equivalent així:

$$x \in A - B \Leftrightarrow x \in A \text{ i } x \notin B$$



Exemples:

- Si $A = \{1, 3, 5, 7, 9\}$ i $B = \{5, 6, 7, 8, 9, 10\}$:
$$A - B = \{1, 3\}$$
- Si $A = \{x \in \mathbb{Z} \mid x \text{ és parell}\}$ i $B = \{x \in \mathbb{Z} \mid x \text{ és senar}\}$:
$$A - B = A$$

Propietats:

-
- $A - A = \emptyset$
 - $A - \emptyset = A$
 - $\emptyset - A = \emptyset$
 - $A - B \subseteq A$

- V. $(A - B) \cap B = \emptyset$
 VI. $A \subseteq B \Leftrightarrow A - B = \emptyset$
 VII. $C \subseteq A - B \Leftrightarrow C \subseteq A, C \cap B = \emptyset$
-

Exercicis:

18. Demostreu les propietats I., III., i VII. anteriors.
 19. Demostreu les propietats II. i IV.(R) anteriors.
 20. Demostreu les propietats V. i VI. anteriors.

Altres propietats:

I. (distributiva)

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
--

- II. $A \cap (A \cup B) = A, A \cup (A \cap B) = A$
 III. $A - (B \cup C) = (A - B) \cap (A - C)$
 IV. $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ i la unió és disjunta (els conjunts $(A - B), (B - A), (A \cap B)$ són disjunts 2 a 2)
-

Exercicis:

21. Demostreu les propietats I. i III. anteriors.
 22. Demostreu que $(A - B) \cap (A - C) \subseteq A - (B \cap C)$. Val la igualtat?
 23. Demostreu que si $A \cup C = B \cup C$ llavors $A - C = B - C$. Val el recíproc?
 24. Demostreu que $(A - B) \cup (B - A) = A$ sii $B = \emptyset$.
 25. Demostreu les propietats II. i IV. anteriors.
 26. Raoneu si és cert o fals i demostreu-ho:
 a. (R) $A - (A - B) = A \cap B$.
 b. $(A - B) \cup B = A \cup B$.

- c. $(A - (A \cap B)) \cap B = \emptyset$
 - d. (R) $A - (B \cup C) = (A - B) \cup (A - C)$.
 - e. Si $A \cap B = A \cap C$ llavors $B = C$.
 - f. Si $A \subseteq B \cup C$ i $A \cap B = \emptyset$ llavors $A \subseteq C$.
27. Demostreu que $A - B \subseteq C$ si i només si $A - C \subseteq B$ (Pista: contrarecíprocs).
28. Demostreu que si $B \cap C = \emptyset$ llavors:
- $$(A - B) \cup C \subseteq (A \cup B \cup C) - (A \cap B).$$
29. (R) Demostreu que si $B \subseteq C$ llavors $A - C \subseteq A - B$.
30. (R) Demostreu que $(A - B) \cup (B - A) = A \cup B$ si i només si $A \cap B = \emptyset$.
31. Demostreu que si $A \cap C \subseteq B \cap C$ i $A \cup C \subseteq B \cup C$ llavors $A \subseteq B$.
(Pista: distingir segons $x \in C$ o no). Deduiu que si $A \cap C = B \cap C$ i $A \cup C = B \cup C$ llavors $A = B$.
32. Demostreu que si $A \cap B \neq \emptyset$ i $B \cap C^c = \emptyset$ llavors $A \cap C \neq \emptyset$.
33. Definim la diferència simètrica $\Delta(A, B)$ de A, B així:
- $$\Delta(A, B) = (A - B) \cup (B - A).$$
- Demostreu que:
- g. $\Delta(A, B) = \emptyset \Leftrightarrow A = B$
 - h. $\Delta(A, C) \subseteq \Delta(A, B) \cup \Delta(B, C)$
 - i. $\Delta(A, \Delta(B, C)) = \Delta(\Delta(A, B), C)$
 - j. $\Delta(A \cup B, C) \subseteq \Delta(A, C) \cup \Delta(B, C)$
 - k. $\Delta(A, C) \cap \Delta(B, C) \subseteq \Delta(A \cap B, C)$
34. Demostreu que $A \cup B = A \cap B$ sii $A = B$.
35. Raoneu si és cert o fals i demostreu-ho:
- a. $(A \cup B) - B = A$.
 - b. $(A \cup B) - (A \cap B) = (A - B) \cup (B - A)$.
 - c. Si $A \cup B = \emptyset$ llavors $A = B = \emptyset$.
36. Demostreu que $(A - B) - C \subseteq A - (B \cup C)$. Val la igualtat?
37. Demostreu que si $A \cap B = \emptyset$ llavors $A - B = A$. Val el recíproc?

Complementari

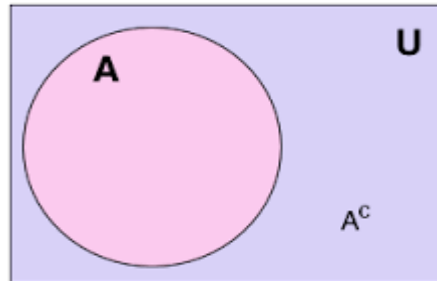
Ara suposem que hi ha un conjunt *gran* o *univers* Ω al qual pertanyen tots els elements amb els que treballarem. En particular tots els altres conjunts són subconjunts d'aquest.

Donat un conjunt A subconjunt de Ω , definim el **conjunt complementari** de A així:

$$A^c = \Omega - A = \{x \in \Omega \mid x \notin A\}$$

Això es pot expressar de manera equivalent així:

$$x \in A^c \Leftrightarrow x \in \Omega \wedge x \notin A$$



Par a tot $x \in \Omega$:

$$x \in A^c \Leftrightarrow x \notin A$$

Nota: Encara que la notació A^c no ho indiqui, aquest conjunt depèn de Ω . Per exemple, el complementari de $A = \{0, 1, 2\}$ relatiu a $\{0, 1, 2, 3, 4, 5, 6\}$ és $\{3, 4, 5, 6\}$ mentre que el complementari de A relatiu a $\{x \in \mathbb{Z} \mid x \geq 0\}$ és $\{3, 4, 5, 6, 7, 8, 9, \dots\}$.

Propietats:

Suposem que $A, B, C \subseteq \Omega$

I. $(A^C)^C = A.$

II. $\emptyset^C = \Omega, \Omega^C = \emptyset.$

III. $A \cap A^C = \emptyset, A \cup A^C = \Omega.$

IV.

(De Morgan) $(A \cup B)^C = A^C \cap B^C, (A \cap B)^C = A^C \cup B^C.$

V.

$$A - B = A \cap B^C$$

VI. $A \subseteq B \Leftrightarrow B^C \subseteq A^C \Leftrightarrow A \cap B^C = \emptyset \Leftrightarrow A^C \cup B = \Omega.$

VII. $B = A^C \Leftrightarrow A \cap B = \emptyset, A \cup B = \Omega.$

Exercicis:

38. Demostreu les propietats II., IV. i VI. anteriors.

39. Demostreu les propietats I., III. i V. anteriors.

40. (R alguna) Demostreu que:

$$A^C \subseteq B \Leftrightarrow B^C \subseteq A \Leftrightarrow A^C \cap B^C = \emptyset \Leftrightarrow A \cup B = \Omega.$$

41. Demostreu que:

$$A \subseteq B^C \Leftrightarrow B \subseteq A^C \Leftrightarrow A \cap B = \emptyset \Leftrightarrow A^C \cup B^C = \Omega.$$

42. Demostreu la propietat VII. anterior.

Parts d'un conjunt

Donat un conjunt A definim el **conjunt de les parts** (o conjunt potència) de A així:

$$P(A) = \{ x \mid x \subseteq A \}$$

Això es pot expressar de manera equivalent així:

$$x \in P(A) \Leftrightarrow x \subseteq A$$

Exemples:

- $P(\emptyset) = \{\emptyset\}$
- $P(\{1\}) = \{\emptyset, \{1\}\}$
- $P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
- $P(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
- $P(\{1, 2, 3, 4\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$

Nota: El nombre d'elements d'un conjunt A rep el nom de **cardinal de A** i es denota per $|A|$. Tenim: $|P(A)| = 2^{|A|}$.

Propietats:

-
- I. $\emptyset \in P(A)$.
 - II. $A \in P(A)$.
-

Exercicis: Demostreu:

43. Les 2 propietats anteriors.
44. $\{a\} \in P(A) \Leftrightarrow a \in A$.
45. $P(A \cap B) = P(A) \cap P(B)$.

46. $A \subseteq P(A), B \subseteq P(B) \Rightarrow A \cap B \subseteq P(A \cap B)$.
47. $|P(A)| = 2^{|A|}$ per inducció simple sobre $|A|$.
48. $\{a, b\} \in P(A) \Leftrightarrow a \in A, b \in A$.
49. (R) $P(A) \cup P(B) = P(A \cup B) \Leftrightarrow A \subseteq B \text{ o } B \subseteq A$.
50. $P(A - B) \subseteq (P(A) - P(B)) \cup \{\emptyset\}$.
51. $\{A, B\} \in P(P(C)) \Rightarrow \{A \cup B\} \in P(P(C))$. Val el recíproc?
52. Són equivalents:
- a. Per a tot $x, y: y \in x \in A \Rightarrow y \in A$.
 - b. Per a tot $x: x \in A \Rightarrow x \subseteq A$.
 - c. $A \subseteq P(A)$.
 - d. $A \in P(P(A))$.
53. (R) $A \subseteq P(A), B \subseteq P(B) \Rightarrow A \cup B \subseteq P(A \cup B)$.
54. $A \subseteq P(A)$ implica $P(A) \subseteq P(P(A))$. Val el recíproc?
55. $P(A) \cup P(B) \subseteq P(A \cup B)$. Val la igualtat?
56. Si $A \subseteq B$ llavors $P(A) \subseteq P(B)$. Val el recíproc?
57. Si $A \cap B = \emptyset$ llavors $P(A) \cap P(B) = \{\emptyset\}$. Val el recíproc?

Parella ordenada

La parella ordenada d'objectes no la definirem formalment. Idea: la **parella ordenada** és com una llista (o vector) de longitud 2 posada entre parèntesis: (a, b) . La propietat fonamental (que podem prendre com a "definició") de les parelles ordenades és la següent:

$$(a, b) = (c, d) \Leftrightarrow a = c, b = d$$

Producte cartesià

Donats dos conjunts A, B definim el **conjunt producte cartesià** de A per B així:

$$A \times B = \{x \mid x = (a, b) \text{ per a uns certs } a \in A \text{ i } b \in B\}$$

Aquest conjunt també l'escriurem, de manera més informal, així:

$$A \times B = \{ (a, b) \mid a \in A, b \in B \}$$

Exemple:

$$\{1, 2, 3, 4\} \times \{a, b\} = \{ (1, a), (2, a), (3, a), (4, a), (1, b), (2, b), (3, b), (4, b) \}$$

Això es pot expressar de manera equivalent així:

$$x \in A \times B \Leftrightarrow x = (a, b) \text{ per a uns certs } a \in A \text{ i } b \in B$$

Sabent que els elements de $A \times B$ són tots parells ordenats, també es pot expressar així:

$$(a, b) \in A \times B \Leftrightarrow a \in A \wedge b \in B$$

Notem que: $|A \times B| = |A| \cdot |B|$

Exercici: Demostreu aquesta fórmula per inducció.

Propietats:

-
- I. $A \times \emptyset = \emptyset, \emptyset \times A = \emptyset.$
 - II. $A \times (B \cap C) = (A \times B) \cap (A \times C).$
 - III. $A \times (B \cup C) = (A \times B) \cup (A \times C).$
 - IV. $A \times (B - C) = (A \times B) - (A \times C).$
-

Exercicis: Demostreu:

58. Les propietats I. i II. anteriors.

59. $A \times B = B \times A \Leftrightarrow A = B \text{ o } A = \emptyset \text{ o } B = \emptyset.$

60. (difícil) Son equivalents:

- a. $A \times B = C \times D$.
- b. $(A \times B = \emptyset \text{ i } C \times D = \emptyset) \text{ o } (A = C \text{ i } B = D)$.
- c. $((A = \emptyset \text{ o } B = \emptyset) \text{ i } (C = \emptyset \text{ o } D = \emptyset)) \text{ o } (A = C \text{ i } B = D)$.
- d. $(A = \emptyset \text{ i } C = \emptyset) \text{ o } (A = \emptyset \text{ i } D = \emptyset) \text{ o } (B = \emptyset \text{ i } C = \emptyset) \text{ o } (B = \emptyset \text{ i } D = \emptyset) \text{ o } (A = C \text{ i } B = D)$.

61. La propietats III. (R) anterior.

62. $A \times B = \emptyset \Leftrightarrow (A = \emptyset \text{ o } B = \emptyset)$

63. (R) $A \times B = C \times D, B \neq \emptyset, D \neq \emptyset \Rightarrow A = C$.

64. $(A \times A) - (B \times B) = A \times (A - B) \cup (A - B) \times (B \cap A)$.

65. (difícil) $(A \times A) - (B \times B) = (A - B) \times (A - B) \Leftrightarrow A \cap B = \emptyset \text{ o } A \subseteq B$.

66. La propietat IV. anterior.

67. $(A \times A) - (B \times B) = A \times (A - B) \cup (A - B) \times A$.

68. $A \times B = (C \times D) \cup (E \times F), B \neq \emptyset, D \neq \emptyset, F \neq \emptyset \Rightarrow A = C \cup E$.

RECEPTES: Demostracions amb conjunts



Demostració de la igualtat entre conjunts (1a. manera)

Volem veure: $A = B$
Sigui x qualsevol:

$$x \in A \Leftrightarrow \dots \Leftrightarrow \dots \Leftrightarrow x \in B$$

Demostració d'una inclusió entre conjunts

Volem veure: $A \subseteq B$

Sigui x qualsevol:

$$x \in A \Rightarrow \dots \Rightarrow \dots \Rightarrow x \in B$$

Demostració de la igualtat entre conjunts (2a. manera)

Volem veure: $A = B$

Demostrem dues coses: $A \subseteq B, \quad B \subseteq A$

Demostració que un conjunt és buit

Una bona estratègia per provar que un conjunt és buit és fer-ho per reducció a l'absurd (encara que no és pas l'únic mètode).

Volem veure: $A = \emptyset$

Per reducció a l'absurd:

$$\exists x \in A \Rightarrow \dots \Rightarrow \dots \Rightarrow \textit{Absurd}$$

Més generalment:

Demostració on intervé que un conjunt és buit

En aquest tipus de demostracions una bona estratègia és usar contrarecíproc o reducció a l'absurd per tal que la condició "ser buit" hi aparegui negada.

Notem que:

- $A \neq \emptyset \Leftrightarrow \exists x \, x \in A$
- $A \not\subseteq B \Leftrightarrow \exists x (x \in A \wedge x \notin B)$

- $A \neq B \Leftrightarrow \exists x (x \in A \wedge x \notin B) \vee \exists x (x \in B \wedge x \notin A)$

Exercici: Useu aquesta estratègia per a demostrar que:

69. $A \cap \emptyset = \emptyset$

70. $A - A = \emptyset$

71. $\emptyset - A = \emptyset$

72. $(A - B) \cap B = \emptyset$

73. $A \cap A^C = \emptyset$

74. $\Omega^C = \emptyset$

75. $A \times \emptyset = \emptyset, \emptyset \times A = \emptyset$

76. $A \subseteq B$ si i només si $A - B = \emptyset$

77. $C \subseteq (A - B)$ si i només si $C \subseteq A$ i $C \cap B = \emptyset$

3.2 RELACIONS D'EQUIVALÈNCIA

Relacions binàries

Idea intuïtiva: una relació binària en un conjunt A “relaciona” parelles d'elements de A . Cada parella d'elements de A poden estar o no estar relacionats. Determinar la relació consisteix en indicar quines parelles estan relacionades i quines no.

Siguin $x, y \in A$. Si estan relacionats per la relació R ho escriurem així:

$$xRy$$

Quan no estan relacionats ho denotarem per:

$$x \not R y$$

Exemples:

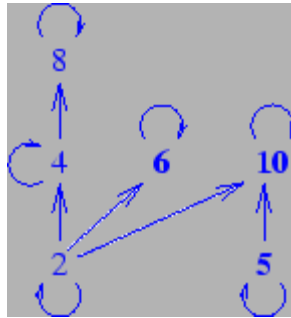
- Al conjunt \mathbb{Z} , les relacions següents:
 - “tenir el mateix residu mòdul 4”
 - “ser més petit o igual que”
 - “ser més gran que”
- Al conjunt A dels alumnes d'aquesta classe, les relacions següents:
 - “seure al costat de”
 - “calçar el mateix número que”
 - “residir a menys d'un km de”
- A un conjunt A qualsevol, les relacions següents:
 - “ser igual que”
 - la relació “buida” (ningú està relacionat amb ningú)
 - la relació “total” (tothom està relacionat amb tothom)

Una relació R en A està determinada pel conjunt dels parells que “estan relacionats” per la relació.

Exemple: $A = \{2, 4, 5, 6, 8, 10\}$

$R = \{ (2, 2), (2, 4), (2, 6), (2, 10), (4, 4), (4, 8), (5, 5), (5, 10), (6, 6), (8, 8), (10, 10) \}$

Això vol dir, per exemple, que $2R4$ (2 està relacionat amb 4, ja que la parella $(2, 4) \in R$) en canvi 2 no està relacionat amb 3 perquè la parella $(2, 3) \notin R$. També es poden representar les relacions mitjançant diagrames de Venn amb fletxes: cada fletxa representa una parella relacionada. L'exemple anterior seria:



En tot conjunt A sempre hi ha les relacions següents:

- La identitat en A (o igualtat), definida per: $x I_A y \Leftrightarrow x = y$:

$$I_A = \{ (x, y) \in A \times A \mid x = y \} = \{ (x, x) \mid x \in A \}$$
- La relació buida (ningú està relacionat amb ningú): $R = \emptyset$
- La relació total (tothom està relacionat amb tothom) $R = A \times A$

Propietats importants que *poden tenir* les relacions:

Reflexiva	$\forall x \in A \ xRx$
Simètrica	$\forall x, y \in A \ (xRy \rightarrow yRx)$
Transitiva	$\forall x, y, z \in A \ ((xRy \wedge yRz) \rightarrow xRz)$
Antisimètrica	$\forall x, y \in A \ ((xRy \wedge yRx) \rightarrow x = y)$

Una **relació d'equivalència** és una relació binària que és reflexiva, simètrica i transitiva.

Exercicis: Sigui R una relació binària a A . Demostreu que:

78. R és reflexiva $\Leftrightarrow I_A \subseteq R$.

79. Suposem que R és irreflexiva (satisfà $\forall x \in A \neg xRx$. Ull, no és el mateix que “no reflexiva”) i transitiva. Definim S així: $xSy \Leftrightarrow xRy \vee x = y$. Demostreu que S és reflexiva, antisimètrica i transitiva.

80. Suposem que R és simètrica i transitiva a A . Considerem

$$B = \{x \in A \mid xRy \text{ per a algun } y \in A\}$$

Demostreu que:

a. $B = \{x \in A \mid xRx\}$.

b. R és una relació d'equivalència a B .

81. La intersecció de relacions d'equivalència és relació d'equivalència. Més precisament: si R, S són relacions d'equivalència en A llavors la relació T definida per

$$xTy \Leftrightarrow xRy \wedge xSy$$

és d'equivalència.

82. Si R és simètrica i antisimètrica llavors $R \subseteq I_A$.

83. (R) Una relació R a A es diu *circular* si verifica $\forall x, y, z \in A (xRy \wedge yRz \rightarrow zRx)$. Demostreu que una relació binària és d'equivalència \Leftrightarrow és reflexiva i circular.

84. (difícil i llarg) Sigui S una relació binària qualsevol en A . Definim la relació R així: $xRy \Leftrightarrow$ existeixen x_1, \dots, x_n amb $n \geq 1$ tals que $x = x_1, y = x_n$ i per a tot $1 \leq i < n$ es compleix: $(x_i S x_{i+1} \vee x_{i+1} S x_i)$. Demostreu que R és la més petita relació d'equivalència que conté (estén) S . Per fer això, heu de veure tres coses: 1. Que R és una relació d'equivalència. 2. Que R conté S . 3. Que si T és una relació d'equivalència que conté S llavors $R \subseteq T$ (aquí heu d'usar inducció).

85. (difícil i llarg) Sigui S una relació binària qualsevol en A . Demostreu que existeix una relació binària R en A que és la més petita relació que estén S i que es reflexiva i transitiva. Pista: modifiqueu convenientment la definició de l'exercici anterior i verifiqueu que es compleixen totes les propietats.

86. Si R és simètrica, transitiva i compleix $\forall x \in A \exists y \in A (xRy)$ llavors R és reflexiva.

87. Si R és transitiva, llavors la relació S definida per

$$xSy \Leftrightarrow x = y \vee (xRy \wedge yRx)$$

és d'equivalència.

88. Si R és reflexiva, simètrica i antisimètrica llavors $R = I_A$. Val el recíproc?

89. Suposem que R és reflexiva, antisimètrica i transitiva. Definim S així:
 $xSy \Leftrightarrow xRy \wedge x \neq y$. Demostreu que S és irreflexiva ($\forall x \neg xSx$) i transitiva.

Classes d'equivalència i conjunt quocient

Si R és una relació d'equivalència en A i $a \in A$ la **classe de** a es defineix així:

$$\bar{a} = \{ x \in A \mid xRa \}$$

Per tant, donats $x, a \in A$ tenim:

$$x \in \bar{a} \Leftrightarrow xRa$$

El **conjunt quocient**, que denotem per A/R , és el conjunt de totes les classes:

$$A/R = \{ x \mid x = \bar{a} \text{ per a un cert } a \in A \} = \{ \bar{a} \mid a \in A \}$$

Notem que:

1. Cada classe d'equivalència és un subconjunt del domini A .
2. El conjunt quocient A/R és un subconjunt de $P(A)$ (exercici: demostrar-ho).

Propietats que satisfà tota relació d'equivalència:

- I. $x \in \bar{x}$.
 - II. Si $x \in \bar{y}$ llavors $\bar{x} = \bar{y}$.
 - III. Si $x \notin \bar{y}$ llavors $\bar{x} \cap \bar{y} = \emptyset$.
 - IV. Les classes formen una "partició" de A . És a dir:
 - a. Cada classe és no buida (ja que $x \in \bar{x}$).
 - b. Dues classes diferents són disjunts: $\forall x, y \in A (\bar{x} \neq \bar{y} \rightarrow \bar{x} \cap \bar{y} = \emptyset)$.
 - c. La reunió de totes les classes és A (ja que $x \in \bar{x}$).
-

Exercicis:

90. Demostreu les 4 propietats anteriors.
91. Demostreu que "tenir el mateix residu mòdul 4" a \mathbb{Z} és relació d'equivalència i que el seu conjunt quocient és $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.
92. Sigui $A \subseteq \mathbb{Z}$, i a un enter fixat. La relació:
- $$xRy \Leftrightarrow mcm(x, a) = mcm(y, a)$$
- és una relació d'equivalència a A . Calculeu el conjunt quocient quan $A = \{1, 2, \dots, 11, 12\}$ i $a = 8$.
93. A \mathbb{Z} definim la relació següent:
- Donats $x, y \in \mathbb{Z}$,
$$xRy \Leftrightarrow x^2 - y^2 = x - y.$$
- Demostreu que és d'equivalència, calculeu les classes de 0, 1, 2. Calculeu la classe \bar{n} d'un element qualsevol n i el conjunt quocient \mathbb{Z}/R .
94. Si B, C són conjunts i $B \subseteq C$, al conjunt $A = P(C)$ definim la relació següent:
- Donats $x, y \in P(C)$:
- $$xRy \Leftrightarrow x - B = y - B.$$
- Demostreu que és una relació d'equivalència. Calculeu totes les classes de R i el conjunt quocient A/R quan $C = \{1, 2, 3, 4\}$ i $B = \{1, 2\}$.
95. Si R és una relació d'equivalència a A i $x, y, z \in A$, demostreu (usant només les definicions de relació d'equivalència i classe) que si $\bar{z} \subseteq \bar{x} \cap \bar{y}$ llavors

$$\overline{x} \cup \overline{y} \subseteq \overline{z}.$$

96. Si R és una relació d'equivalència a A i $x, y \in A$, demostreu (usant només les definicions de relació d'equivalència i classe) que són equivalents:

- $\overline{x} = \overline{y}$.
- Existeix $z \in A$ tal que $\overline{z} \subseteq \overline{x} \cap \overline{y}$.
- Existeix $z \in A$ tal que $\overline{x} \cup \overline{y} \subseteq \overline{z}$.
- Per a tot $z \in A$, si $\overline{x} \cap \overline{z} \neq \emptyset$ llavors $\overline{y} \cap \overline{z} \neq \emptyset$.

97. (R) Sigui $A \subseteq \mathbb{N}$, i s l'aplicació $s: \mathbb{N} \rightarrow \mathbb{N}$ definida per $s(n)$ = la suma dels díigits de n expressat en base 10. Demostreu que la relació

$$xRy \Leftrightarrow s(x) = s(y)$$

és una relació d'equivalència a A . Calculeu el conjunt quocient quan $A = \{4, 44, 42, 22, 36, 8, 11, 35, 13, 15, 17, 18, 51, 33, 6\}$.

98. (R) Si B, C són conjunts i $B \subseteq C$, al conjunt $A = P(C)$ definim la relació següent: Donats $x, y \in P(C)$:

$$xRy \Leftrightarrow x \cup B = y \cup B.$$

Demostreu que és una relació d'equivalència. Calculeu totes les classes de R i el conjunt quocient A/R quan $C = \{1, 2, 3, 4\}$ i $B = \{1, 2\}$.

99. (R) A \mathbb{Z} definim la relació següent:

$$\text{Donats } x, y \in \mathbb{Z}, \quad xRy \Leftrightarrow x^2 + 3y = y^2 + 3x.$$

Demostreu que és d'equivalència, calculeu les classes de 0, 1, 2. Calculeu la classe \overline{n} d'un enter n qualsevol i el conjunt quocient \mathbb{Z}/R .

100. (R) Considerem la relació "tenir la mateixa part entera" a \mathbb{R} . Demostreu que és d'equivalència, calculeu les classes de 1.2, π , -1.2 . Descriviu el conjunt quocient.

101. (R) Si $A = \mathbb{Z} \times \mathbb{Z}$, considerem la relació:

$$(x, y) R (x', y') \Leftrightarrow xy = x'y'.$$

Demostreu que és d'equivalència, calculeu les classes de (1, 0), (1, 1), (2, 1), (2, 3), $(-2, 4)$. Descriviu el conjunt quocient.

102. (R alguna) Sigui R una relació a A que és simètrica i transitiva. Donats $x, y \in A$, demostreu que són equivalents (usant només les definicions de relació d'equivalència i classe):

- a. $\bar{x} \cap \bar{y} \neq \emptyset$.
 - b. $\bar{y} \subseteq \bar{x}$.
 - c. $\bar{x} \subseteq \bar{y}$.
 - d. $\bar{x} \cap \bar{y} = \bar{x}$.
 - e. Existeix $z \in A$ tal que $\bar{x} \subseteq \bar{z} \subseteq \bar{y}$.
 - f. Per a tot $z \in A$, si $\bar{z} \subseteq \bar{x}$ llavors $\bar{y} \subseteq \bar{z}$.
103. Demostreu que (usant només les definicions de relació d'equivalència i classe) en una relació d'equivalència no hi ha dues classes diferents, una continguda a l'altre.
104. (R) Demostreu (usant només les definicions de relació d'equivalència i classe) que en una relació d'equivalència es verifica: si $\bar{x} \cap \bar{y} \neq \emptyset$ i $\bar{x} \cap \bar{z} \neq \emptyset$ llavors $\bar{y} \cap \bar{z} \neq \emptyset$.
105. (difícil i llarg) Sigui S una relació a A que és reflexiva i transitiva. Demostrea que la relació R definida per $xRy \Leftrightarrow xSy \wedge ySx$ és d'equivalència. En el conjunt quocient A/R definim la relació binària següent: $\bar{x}T\bar{y} \Leftrightarrow xSy$. Demostreu que està ben definida (no depèn del representant: $xSy, xRx', yRy' \Rightarrow x'Sy'$) i satisfà les propietats reflexiva, antisimètrica i transitiva (és una relació d'ordre parcial).
106. Si R és una relació d'equivalència a A i $x, y, z \in A$, demostreu (usant només les definicions de relació d'equivalència i classe) que:
- $$x \in \bar{z}, y \in \bar{z} \Rightarrow \bar{x} = \bar{y}.$$
107. Si R és una relació d'equivalència a A i $x, y \in A$, demostreu (usant només les definicions de relació d'equivalència i classe) que són equivalents:
- a. xRy .
 - b. $x \in \bar{y}$.
 - c. $\bar{x} \cup \bar{y} = \bar{y}$.
108. Si $A \subseteq \mathbb{Z}$, la relació "tenir els mateixos divisors primers" és d'equivalència a A . Calculeu el conjunt quocient quan $A = \{1, 2, \dots, 11, 12\}$.
109. Si B, C són conjunts i $B \subseteq C$, al conjunt $A = P(C)$ definim la relació següent: Donats $x, y \in P(C)$:
- $$xRy \Leftrightarrow x \cap B = y \cap B.$$

Demostreu que és una relació d'equivalència. Calculeu totes les classes de R i el conjunt quocient A/R quan $C = \{1, 2, 3, 4\}$ i $B = \{1, 2\}$.

110. Sigui $A \subseteq \mathbb{Z}$, i a un enter fixat. Demostreu que la relació en el conjunt A :

$$xRy \Leftrightarrow \text{mcd}(x, a) = \text{mcd}(y, a)$$

és una relació d'equivalència a A . Calculeu el conjunt quocient quan $A = \{1, 2, \dots, 11, 12\}$ i $a = 8$.

111. A \mathbb{Z} definim la relació següent:

$$\text{Donats } x, y \in \mathbb{Z}, \quad xRy \Leftrightarrow x^2 - 2y = y^2 - 2x.$$

Demostreu que és d'equivalència, calculeu les classes de 0, 1, 2. Calculeu la classe \bar{n} d'un element qualsevol n i el conjunt quocient \mathbb{Z}/R .

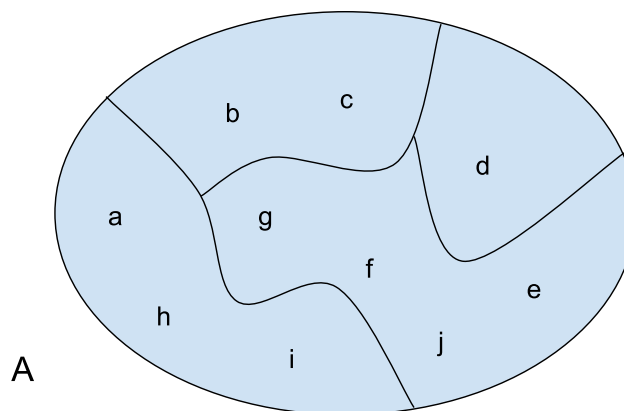
112. A \mathbb{R} definim la relació següent:

$$\text{Donats } x, y \in \mathbb{R}: \quad xRy \Leftrightarrow xy > 0 \vee x = y = 0.$$

Demostreu que és d'equivalència, calculeu totes les classes i el conjunt quocient \mathbb{R}/R .

PARTICIONS

La idea de partició és molt senzilla: tenim un conjunt A i el trenquem (o repartim) en trossos.



En el dibuix hem trencat el conjunt $A = \{a, b, c, d, e, f, g, h, i, j\}$ en 4 trossos: $\{b, c\}$, $\{d\}$, $\{e, f, g, j\}$, $\{a, h, i\}$.

El conjunt format per aquestes 4 parts és una partició de A :

$$\{\{b, c\}, \{d\}, \{e, f, g, j\}, \{a, h, i\}\}$$

Definició:

Una **partició** P de A és un conjunt de subconjunts no buits de A , disjunts dos a dos i tal que la seva reunió és A .

Més precisament: P és una partició de A si :

- $\forall B \in P \ B \subseteq A$ (de manera equivalent: $P \subseteq P(A)$).
- $\forall B \in P \ B \neq \emptyset$.
- $\forall B \in P \forall C \in P (B \neq C \rightarrow B \cap C = \emptyset)$.
- Si $P = \{A_1, A_2, \dots, A_n\}$ llavors $A = A_1 \cup A_2 \cup \dots \cup A_n$
($\forall x \in A \exists B \in P \ x \in B$ si la partició és infinita).

Exemples:

- A. $\{\{1\}, \{2, 3\}, \{4\}, \{5, 6, 7\}\}$ és una partició de $\{1, 2, 3, 4, 5, 6, 7\}$.
- B. $\{\{1, 3, 5\}, \{2, 3\}, \{4\}, \{5, 6, 7\}\}$ **no** és una partició de $\{1, 2, 3, 4, 5, 6, 7\}$.
- C. $\{\{1\}, \{2, 3\}, \{4\}, \{6, 7\}\}$ **no** és una partició de $\{1, 2, 3, 4, 5, 6, 7\}$.

Exemple/Exercici: Trobeu totes les particions del conjunt $\{1, 2, 3, 4\}$.

Hem vist que si R és una relació d'equivalència a A , llavors A/R és una partició de A . De fet, totes les particions són el quocient d'una relació d'equivalència. Si P és una partició de A podem definir una relació R així:

$$xRy \Leftrightarrow x \text{ i } y \text{ pertanyen a un mateix } B \in P$$

En els exercicis veurem que és una relació d'equivalència i que el conjunt quocient és $A/R = P$.

Exercicis:

113. Considerem a $\mathbb{R} \times \mathbb{R}$ la relació següent:

$$(x, y) R (z, t) \Leftrightarrow |x| + |y| = |z| + |t|.$$

- a. Proveu que R és una relació d'equivalència.
- b. Dibuixeu en el pla la classe del punt $(1, 0)$.
- c. Dibuixeu en el pla la classe del punt (a, b) .
- d. Doneu el conjunt quocient.
- e. Quina partició determina? Dibuixeu les classes.

114. (R) Definim la funció $f: \mathbb{R} \times \mathbb{R} \rightarrow \{-1, 0, 1\}$ així:

$$f(x, y) = 1 \text{ si } xy > 0.$$

$$f(x, y) = 0 \text{ si } xy = 0.$$

$$f(x, y) = -1 \text{ si } xy < 0.$$

A $\mathbb{R} \times \mathbb{R}$ definim la relació: $(x, y)R(u, v)$ si $f(x, y) = f(u, v)$. Demostreu que és una relació d'equivalència i descriu les classes i el conjunt quocient.

115. Sigui P una partició de A . Definim una relació R a A així:

$$xRy \Leftrightarrow \exists B \in P (x \in B \wedge y \in B)$$

Demostreu que:

- a. per a cada $x \in A$ hi ha un únic $B \in P$ tal que $x \in B$.
- b. R és una relació d'equivalència a A (pista: useu a.).
- c. Si $x \in B$ i $B \in P$ llavors $\bar{x} = B$.
- d. $A/R = P$.

116. A $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ considerem la relació "estar a la mateixa distància de l'origen".

- a. Proveu que R és una relació d'equivalència.
- b. Dibuixeu en el pla la classe del punt $(1, 0)$.
- c. Dibuixeu en el pla la classe del punt (a, b) .
- d. Doneu el conjunt quocient.
- e. Quina partició determina? Dibuixeu les classes.

117. A $\mathbb{Z} - \{0\}$ es defineix la relació: dos enters estan relacionats si i només si tenen mateix signe i mateixa paritat o diferent signe i diferent paritat. Demostreu que és una relació d'equivalència i descriu les classes i el conjunt quocient.