CIÈNCIES APLICADES
41

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

UPCGRAU

Fonaments matemàtics

Com apendre a resoldre problemes. Raonament i demostració

Joan Trias Pairó

41

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

iniciativa
digital politècnica
Publicacions Acadèmiques UPC

UPCGRAU

Fonaments matemàtics

Com apendre a resoldre problemes. Raonament i demostració

Joan Trias Pairó

Primera edició: juliol de 2016

Disseny i dibuix de la coberta: Jordi Soldevila
Disseny maqueta interior: Jordi Soldevila
Maquetació: Mercè Aicart

Oficina de Publicacions Acadèmiques Digitals de la UPC
Jordi Girona 31,
Edifici Torre Girona, Planta 1, 08034 Barcelona
Tel.: 934 015 885
www.upc.edu/idp
E-mail: info.idp@upc.edu

Dipòsit legal: B.15591-2016
ISBN: 978-84-9880-598-7

Índex

Pròleg

Entendre, formalitzar, demostrar i redactar

Per què aquest llibre? Suport a la transició de la secundària a la universitat. Sorgeix de l'observació de les dificultats d'una bona quantitat d'alumnes amb relació al raonament, la demostració i la resolució de problemes. Són manifestes les dificultats creixents del pas de la secundària a la universitat, i molts de problemes són comuns a àmplies capes d'alumnes. L'entrada a la universitat suposa per a l'alumne una pujada en el nivell d'abstracció i moltes vegades no sap com abordar la resolució de problemes. Una de les accions que es poden fer en relació amb aquest problema és crear un material, com aquest llibre, amb el qual pugui aprendre a resoldre problemes. Aquest material és ben necessari o, com a mínim, convenient per a ajudar l'alumne a obtenir millors resultats.

És un llibre de suport per a assignatures de **fonamentació matemàtica** a un nivell de primer curs. S'hi han tingut en compte els interessos específics de l'alumne que cursa estudis d'informàtica. S'hi presenten:

a) **resums teòrics**,
b) **exemples** i
c) **problemes resolts**,

amb l'objectiu d'ensenyar a resoldre problemes, i tot el que hi està relacionat: la formalització de l'enunciat, la comprensió de l'enunciat, l'anàlisi de la metodologia de resolució, la resolució pròpiament dita i la redacció correcta de la resolució, la discussió d'alternatives en el mètode de resolució i, fins i tot, d'alternatives en l'exposició de la resolució.

Ensenyar a raonar, resoldre problemes i redactar-ne la resolució. Estem interessats a resoldre problemes de manera molt completa, i a analitzar de manera molt detallada tot el que està relacionat amb un problema. Volem fer èmfasi en els diversos mètodes, les idees guia de resolució, l'estructura demostrativa. L'objectiu és ensenyar a resoldre'n, a raonar, a demostrar, a plantejar estratègies de resolució. Això significa que moltes vegades s'hi intercalen molts de comentaris explicatius o de suggeriment, que esperem que no hi facin gaire nosa. L'orientació i la intencionalitat és marcadament didàctica.

Els objectius concrets de l'obra són:

a) presentar resums teòrics (que emmarquin els problemes i els exemples) i una quantitat notable d'exemples,
b) presentar amb detall la resolució dels problemes més estàndards (resolts),
c) presentar models de resolució d'exercicis segons les diverses tipologies possibles,
d) il·lustrar totes les metodologies de demostració possibles (es procura presentar el màxim de mètodes possibles),
e) oferir consells i estratègies de resolució,
f) insistir molt en la correcció formal i la bona formalització, segons diferents graus possibles,
g) insistir molt en les explicacions exhaustives, les bones argumentacions, amb diversos nivells d'explicacions,
h) presentar diverses alternatives de redacció correctes,
i) presentar anàlisis de demostracions i de l'estructura demostrativa.

Quines qüestions s'hi tracten. Aspectes importants són: la formalització, el llenguatge de proposicions i de predicats, el raonament en general, la demostració (amb el mètode d'inducció), els conjunts i les relacions, les funcions (aplicacions) i l'aritmètica "elemental". Aquesta obra intenta cobrir aquests aspectes. S'estructura en dos volums:

Volum 1: Formalització, lògica, raonament, demostració i conjunts.

Volum 2: Funcions, relacions, aritmètica elemental.

Resolució per diversos mètodes. Un mateix problema potser es resol per més d'un mètode, en un mateix lloc o bé en diverses localitzacions, per tal d'il·llustrar les diferents metodologies (per això, alguns enunciats es repeteixen). O, en cas que no es faci això en totes la situacions en què sigui possible, se n'indicaran les possibilitats i se'n donarà la idea.

És possible que en algun problema el lector es pregunti si no seria millor resoldre'l per un altre mètode. Possiblement ja estigui fet així en algun altre lloc del llibre. Cal tenir en compte que potser es vol exposar, amb aquest problema, una determinada metodologia de resolució, encara que n'hi hagi d'altres d'aplicables. En aquesta circumstància, estem interessats tant a resoldre el problema com a presentar un mètode de resolució possible.

Un aspecte que cal remarcar és que la majoria de problemes corresponen a temes de poca dificultat tècnica, cosa que ens permet concentrar-nos en els aspectes de metodologia demostrativa i expositiva, que es poden així comprendre millor.

Barreja d'estils expositius. També en diverses parts de la publicació es troben diversos estils expositius, que van des de l'exposició altament formalitzada, amb un ús sistemàtic de la formulació en termes del llenguatge de predicats, fins a una exposició més planera en llenguatge natural, amb resolucions més verbalitzades o conversacionals, aproximacions totes igualment vàlides. El lector també trobarà un cert nivell de repetició, convenient en un procés d'aprenentatge. Es fa un èmfasi especial en la formalització. Les resolucions es donen amb un alt grau de detall.

Resolució guiada. Es fa èmfasi en les idees que guien o dirigeixen la resolució. Les preguntes que es van fent poden servir de guia per a avançar.

Redacció de les resolucions. Hi ha eines diverses que poden ajudar a la tasca important de redactar les resolucions. Vegeu, en particular, [ESQTRI] i [ESQTRI2], on s'analitzen els errors més freqüents en la redacció d'exàmens i es donen consells per tal d'evitar-los i millorar-ne el redactat.

Origen dels enunciats. Molts dels enunciats dels problemes que es resolen són propis. D'altres són molt generals o molt bàsics, absolutament estàndards, gairebé de domini general i, de fet, no es pot considerar que siguin de cap autor en particular (per exemple, "demostreu per inducció la fórmula de la suma dels n primers nombres naturals" o "demostreu que la suma de dos nombres senars és parell"). Són enunciats amb els quals l'autor ha treballat al llarg de molts anys de docència. Altres, molt pocs, provenen d'algunes obres de la bibliografia (però no la resolució ni l'exposició, que són pròpies de l'autor); pel que fa als enunciats, considerin-se els autors citats per aquesta referència genèrica, si és el cas.

Ordenació. Atès que aquest no és un llibre de teoria, els problemes i els temes no estan ordenats necessàriament ni per ordre cronològic d'aparició a les explicacions teòriques usuals ni per ordre de dificultat. És possible que fins i tot un mateix enunciat es repeteixi en diversos llocs, a cada un d'ells il·lustrant diferents metodologies o idees.

Atès que és un llibre de problemes, no cal seguir l'ordre que s'hauria de mantenir en una exposició teòrica, ja que tampoc no està pensat per a fer-ne una lectura lineal de principi a fi. De manera que, en qualsevol lloc, podem trobar una demostració per inducció (encara que hi hagi un capítol específic per a descriure el mètode i per a ensenyar a fer demostracions per inducció); el mateix podem dir, per exemple, de les demostracions per casos o per reducció a l'absurd, que es poden presentar en qualsevol lloc, a banda del capítol dedicat a exposar els mètodes de demostració. Ho facilita també el fet que alguns problemes es puguin resoldre per més d'un mètode. El lector anirà llegint aquí i allà, segons li interessi.

Un "bon consell" final. El lector ha d'entendre bé l'enunciat, eventualment revisar la teoria corresponent si no entén de què parla, i intentar reexpressar, reescriure l'enunciat i, eventualment, formalitzar-lo o expressar-lo de manera més formal (i hi poden haver diverses modalitats).

Es recomana que no miri la resolució fins després d'haver intentat resoldre l'apartat o la qüestió; només ho ha de fer com a últim recurs o, finalment, com a comprovació de la seva resposta. En cas que la llegeixi, és un bon exercici mirar d'arribar-hi posteriorment pel seu propi compte i, en qualsevol cas, redactar-la completament a partir de “full en blanc”.

Observació final. El final d’exemple o de demostració s’indica amb el símbol ■ .

Barcelona, 30 de juny de 2015

Joan Trias Pairó
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya

→ 1

Preliminars i fórmules útils

En aquest capítol s'estableixen notacions bàsiques i es veuen diverses propietats simples, necessàries per a poder presentar exemples concrets de raonament i demostració. Alguns temes es tractaran amb detall més endavant (el de conjunts, per exemple).

1.1. Conjunts

Informalment, un conjunt A és una col·lecció d'objectes, els seus *elements*, sense repetició i en què l'ordre no importa. Per exemple, el conjunt de les lletres vocals és $V = \{a, e, i, o, u\}$. Els elements de V són a, e, i, o, u; es diu de *pertanyen* a V, cosa que denotem: $a \in V, \dots, u \in V$. Escrivim $a \in A$ si a és un element de A. S'expressa que un objecte b no és element del conjunt A mitjançant $b \notin A$. Podem descriure un conjunt mitjançant propietats que en caracteritzin els seus elements, com per exemple $\{2, -2\} = \{x | x \text{ és un nombre enter tal que } |x| = 2\}$.

Es diu que el conjunt A és subconjunt del conjunt B si tot element de A és de B. Notació: $A \subseteq B$.

1.2. Conjunts de nombres: nombres naturals, enters, racionals i reals

Conjunts importants són els conjunts de nombres, per als quals se suposa ja un coneixement bàsic i intuïtiu; els presentem sense gaire formalismes.
Indiquem la notació habitual per als diversos **conjunts de nombres**.

Nombres **naturals**.

$$\mathbb{N} = \{0, 1, 2, 3, 5, 6, \dots\}.$$

Observeu que considerem que $0 \in \mathbb{N}$.

Nombres **enters**.

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{0, 1, -1, 2, -2, 3, -3, \ldots\},$$

simetritzat del conjunts dels nombres naturals.

Denotem

$$\begin{aligned} \mathbb{Z}^+ &= \{x \in \mathbb{Z} \mid x \geq 0\} \text{ (nombres enters no negatius)} \\ \mathbb{Z}^+ - \{0\} &= \{x \in \mathbb{Z} \mid x > 0\} \text{ (nombres enters positius)} \end{aligned}$$

Tenim que $\mathbb{Z}^+ = \{m \in \mathbb{Z} | m \geq 0\} = \mathbb{N}$.

És $\mathbb{N} \subseteq \mathbb{Z}$.

Notació: $[n] = \{1, 2, 3, \cdots, n\} = \{k \in \mathbb{N} | 1 \leq k \leq n\}$.

Nombres **racionals**.

$$\mathbb{Q} = \{\tfrac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}.$$

Podem considerar que tot nombre enter m és també racional, ja que es pot reescriure com $m = \frac{m}{1}$ (identifiquem 3 amb $\frac{3}{1}$, -3 amb$\frac{-3}{1}$, és a dir, $3 = \frac{3}{1}$, $-3 = \frac{-3}{1}$) , i així $\mathbb{Z} \subseteq \mathbb{Q}$, d'on $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$.

Si $\frac{a}{b} > 0$ (a, b tenen el mateix signe), sempre es pot reescriure de manera que a, b siguin no negatius; en efecte, si a, b són positius, ja està; si $a < 0, b < 0$, escrivim $\frac{a}{b} = \frac{-a}{-b}$.

Exemples de nombres racionals:

$$2; -3; \tfrac{2}{3}; 0,3 = \tfrac{3}{10}; 0,33\ldots (= \tfrac{1}{3}) \text{ (període 3)}.$$

Igualtat de dos nombres racionals. És $\dfrac{a}{b} = \dfrac{c}{d}$ si, i només si, $ad = cb$.

Fraccions irreductibles. Algunes fraccions poden simplificar-se. Per exemple,

$$\frac{2 \cdot 2 \cdot 3 \cdot 7}{2 \cdot 3 \cdot 5} = \frac{2 \cdot 3 \cdot 7}{3 \cdot 5} = \frac{2 \cdot 7}{5}.$$
$$\frac{15}{12} = \frac{3 \cdot 5}{3 \cdot 4} = \frac{5}{4}.$$

És $\frac{ad}{bd} = \frac{a}{b}$. Una fracció racional $\frac{a}{b}$ és irreductible si ja no es pot simplificar, és a dir, si a, b ja no tenen més divisors comuns diferents de ± 1; això equival a dir que a, b són primers entre si, és a dir, $\text{mcd}(a, b) = 1$ (màxim comú divisor). Sempre es pot aconseguir una reducció a irreductible: dividint per $\text{mcd}(a, b)$. Si $d = \text{mcd}(a, b)$, és $\frac{a}{b} = \frac{a'd}{b'd} = \frac{a'}{b'}$, on $\text{mcd}(a', b') = 1$, de manera que, si convé, sempre podem considerar, d'entrada, que $\frac{a}{b}$ és irreductible, ja que, si no ho és, es pot realitzar el procés anterior.

Posteriorment en veurem una aplicació a la demostració que $\sqrt{2}$ no és racional, on, *sense pèrdua de generalitat*, podrem suposar que un nombre racional s'expressa com a fracció irreductible i fer l'argumentació a partir d'aquest fet.

Són racionals els nombres naturals, els enters, les fraccions abans indicades i els nombres decimals finits (amb desenvolupament finit) o els nombres amb desenvolupament decimal infinit periòdic.

Exemple 1.1 $0{,}25 = \frac{1}{4}$; $\frac{15}{12}$. ■

Denotem

$$\begin{aligned} \mathbb{Q}^+ &= \{x \in \mathbb{Q} \mid x \geq 0\} \text{ (nombres racionals no negatius)} \\ \mathbb{Q}^+ - \{0\} &= \{x \in \mathbb{Q} \mid x > 0\} \text{ (nombres racionals positius)} \end{aligned}$$

(vegeu la definició i la notació de diferència de conjunts $A - B$ al capítol posterior sobre conjunts).

Nombres **reals**.

La notació que utilitzem és $\mathbb{R}$.

Conté els racionals i els irracionals (entre els quals $\pi, e, \sqrt{2}, \log_2 3$ i infinits més).

Els nombres irracionals corresponen als desenvolupaments decimals infinits no periòdics.

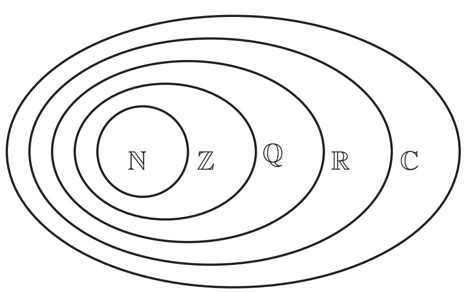
Denotem

$$\begin{aligned} \mathbb{R}^+ &= \{x \in \mathbb{R} \mid x \geq 0\} \text{ (nombres reals no negatius)} \\ \mathbb{R}^+ - \{0\} &= \{x \in \mathbb{R} \mid x > 0\} \text{ (nombres reals positius)} \end{aligned}$$

Finalment, $\mathbb{C}$ denota el conjunt dels nombres **complexos**.

Els nombres complexos són de la forma $a + bi$, amb a, b nombres reals.

És $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.



La recta real. Un model gràfic de representació dels nombres reals, que resulta còmode, és el de la recta real, recta "contínua", on es representen, *com a punts*, nombres naturals, enters, racionals i irracionals. També s'hi poden representar conjunts importants, els intervals.

Conjunts importants de la recta real: els intervals.

Sigui $a, b \in \mathbb{R}$. Definim els diversos conjunts següents:

$$
\begin{aligned}
(a,b) &= \{x \in \mathbb{R} | a < x < b\} && \text{(interval obert d'extrems } a,b\text{).}\\
[a,b] &= \{x \in \mathbb{R} | a \leq x \leq b\} && \text{(interval tancat d'extrems } a,b\text{).}\\
(a,b] &= \{x \in \mathbb{R} | a < x \leq b\} && \text{(interval semiobert-semitancat d'extrems } a,b\text{).}\\
[a,b) &= \{x \in \mathbb{R} | a \leq x < b\} && \text{(interval semitancat-semiobert d'extrems } a,b\text{).}\\
[a,+\infty) &= \{x \in \mathbb{R} | a \leq x\} && \text{(semirecta tancada).}\\
(a,+\infty) &= \{x \in \mathbb{R} | a < x\} && \text{(semirecta oberta).}\\
(-\infty,b] &= \{x \in \mathbb{R} | x \leq b\} && \text{(semirecta tancada).}\\
(-\infty,b) &= \{x \in \mathbb{R} | x < b\} && \text{(semirecta oberta).}\\
(-\infty,+\infty) &= \mathbb{R}
\end{aligned}
$$

Els nombres irracionals no es poden representar a l'ordinador de forma exacta mitjançant un desenvolupament decimal, sinó només amb aproximacions racionals, i encara amb limitacions, dintre d'un rang prefixat (sí en forma simbòlica per a alguns: per exemple, "$\sqrt{2}$", tot i que depenent del programa). El mateix pot passar amb els racionals; per exemple, $\frac{1}{3}$ es podria representar de forma simbòlica, però no de forma decimal exacta 0,33333... (periòdica), ja que això suposaria infinites xifres decimals. Fins i tot en el cas de desenvolupament decimal finit, es poden presentar problemes si se sobrepassa la capacitat prevista d'emmagatzemament. Pel que fa als enters, apareixen problemes amb nombres molt grans; si la situació ho requereix, aleshores s'ha de tractar de manera específica. Algunes aplicacions requereixen treballar amb nombres naturals molt grans, com la criptografia.

1.3. Idees sobre implicació, raonament, demostració

Donem aquí una idea ràpida i informal d'aquestes qüestions. Posteriorment, es detallaran, completaran i rigoritzaran molts aspectes lligats al raonament i a la demostració. Això és només per a presentar una idea intuïtiva i connectar amb coneixements ja sabuts.

Recordem els **símbols lògics** (connectives lògiques i quantificadors):

$\neg$ (negació, "no")
$\wedge$ (conjunció, "i")
$\vee$ (disjunció, "o")
$\rightarrow$ (condicional, "si ..., aleshores ...")
$\leftrightarrow$ (bicondicional, "si ..., i només si, ...")
$\forall$ ("per a tot")
$\exists$ ("existeix")

Siguin A, B dues afirmacions.

$A \Rightarrow B$ (Es diu que "*A implica B*"). Què vol dir $A \Rightarrow B$?

Exemples 1.2 Exemples d'afirmacions d'aquest tipus:

Exemple 1. Si n és un nombre enter parell, aleshores n^2 és un nombre parell.
Aquí és $A =$ "n és un nombre enter parell", $B =$ "n^2 és un nombre parell".
Reformulació: n és un nombre enter parell $\Rightarrow n^2$ és un nombre parell. ■

Exemple 2. Si n és un nombre enter senar, aleshores n^2 és un nombre senar.
Aquí és $A =$ "n és un nombre enter senar", $B =$ "n^2 és un nombre senar".
Reformulació: n és un nombre enter senar $\Rightarrow n^2$ és un nombre senar. ■

Exemple 3. Si a, b són nombres enters i a és parell, aleshores ab és parell.
Aquí és $A =$ "a, b són nombres enters i a és parell", $B =$ "ab és parell".
Reformulació: (a, b són nombres enters i a és parell) $\Rightarrow ab$ és parell. ■

Aquí A és la hipòtesi (premissa, antecedent) i B és la tesi (conseqüent, conseqüència). Poden ser fórmules complicades amb "i, o, no, si ..., aleshores ..., ... si, i només si, ...", és a dir, compostes. En aquest últim exemple, A és A_1 i A_2, conjunció de $A_1 =$ "a, b són nombres enters" i $A_2 =$ "a és parell".

Per a establir $A \Rightarrow B$ (que A implica B), s'ha de *provar* o *demostrar* la veracitat del condicional

"Si A, aleshores B"

En concret, i al efectes pràctics, cal veure que "si A és cert, aleshores B és cert". És a dir, que no pot ser que A sigui cert i, en canvi, B sigui fals. O sigui, que de la veracitat de A se segueix la veracitat de B. Hi ha més casos possibles de veritat-falsedat, però ara no ens interessen.

Observeu que no s'afirma que A és cert (tot sol). Tampoc no s'afirma que B sigui cert (tot sol). Només s'afirma la veracitat d'un condicional.

Exemples 1.3

Exemple 1. Vegem un exemple del que s'ha dit anteriorment, on, a més, A i B no tenen cap relació: $1 \overset{Hip}{=} 0 \Rightarrow 2 = 3$.
En efecte, a part que podem donar un argument formal: $0(fals) \to 0(fals)$ "és cert", també podem donar una demostració: $3 = 2+1 \overset{Hip}{=} 2+0 = 2$. ■

Exemple 2. Més d'aquest tipus: $1 \overset{Hip}{=} 0 \Rightarrow 6 = 2$. En efecte, $6 = 5+1 \overset{Hip}{=} 5+0 = 5 = 4+1 \overset{Hip}{=} 4+0 = 4 = 3+1 \overset{Hip}{=} 3+0 = 3 = 2+1 \overset{Hip}{=} 2+0 = 2$. ■

Normalment, en els casos realment interessants, les afirmacions A i B estan relacionades. Establir la veracitat de B a partir de la veracitat de A sol no ser obvi o immediat, sinó que calen una sèrie d'etapes en què es justifiqui l'enunciat mitjançant argumentacions. Aquest procés és una *demostració* i exigeix uns *raonaments* apropiats.

Els resultats demostrats es poden enunciar com a *teoremes*.

Vegem ***un exemple de demostració*** del resultat següent:

Teorema 1.1 *"Si n és un nombre enter parell, aleshores n^2 és un nombre parell"*.

Estructura de l'enunciat:

Hipòtesi (A): n és un nombre enter parell.

Tesi (B): n^2 és un nombre parell.

Idea bàsica de la demostració. El problema principal és expressar de forma operativa la propietat de ser parell (vegeu el capítol següent). Un nombre enter és parell si, i només si, és múltiple de 2, és a dir, es pot escriure de la forma $2k$ per a un nombre enter k adequat. Cal veure que n^2 també es pot escriure d'aquesta forma.

Demostració. Vegem uns quants estils expositius per demostrar-ho.

Comentari: és un esquema demostratiu **directe**.

Exposició 1. Escrivim una col·lecció d'afirmacions encadenades, que són els passos de la demostració; s'entén que cada pas implica el següent (és a dir, se'n deriva el següent):

$\mathbf{P_1}$: n és un nombre enter parell (observació: és A).

$\mathbf{P_2}$: existeix un nombre enter k tal que $n = 2k$ (definició de nombre parell) [aquí s'aplica la hipòtesi].

$\mathbf{P_3}$: existeix un nombre enter k tal que $n^2 = (2k)^2$ (elevar al quadrat, "aproximant-nos així a B").

$\mathbf{P_4}$: existeix un nombre enter k tal que $n^2 = 4k^2 = 2(2k^2)$ (reescriptura, fent aparèixer un factor 2, derivant cap al que ens interessa, que és escriure el nombre com a parell).

$\mathbf{P_5}$: existeix un nombre enter k' tal que $n^2 = 2k'$ (observació: escollint $k' = 2k^2$, nombre enter; és una reescriptura com a nombre parell).

$\mathbf{P_6}$: n^2 és un nombre enter parell (observació: és B).

L'esquema demostratiu és: $P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow P_4 \Rightarrow P_5 \Rightarrow P_6$, és a dir, $A \Rightarrow P_2 \Rightarrow P_3 \Rightarrow P_4 \Rightarrow P_5 \Rightarrow B$. En resum, $P1 \Rightarrow P6$, és a dir, $A \Rightarrow B$.

Exposició 2. O bé pot consistir a anar escrivint implicacions:

n és un nombre enter parell (observació: és A)

$\Downarrow$

existeix un nombre enter k tal que $n = 2k$ (expressió d'un nombre parell)

$\Downarrow$

existeix un nombre enter k tal que $n^2 = (2k)^2$ (substitució)

$\Downarrow$

existeix un nombre enter k tal que $n^2 = 4k^2 = 2(2k^2)$ (càlculs)

$\Downarrow$

existeix un nombre enter k' tal que $n^2 = 2k'$ (observació: escollint $k' = 2k^2$, nombre enter)

$\Downarrow$

n^2 és un nombre enter parell (observació: és B)

Exposició 3. O bé enllaçant verbalment les línies anteriors:

n és un nombre enter parell (observació: és A). ***Per tant,***
existeix un nombre enter k tal que $n = 2k$, ***d'on***
existeix un nombre enter k tal que $n^2 = (2k)^2$, ***d'on***
existeix un nombre enter k tal que $n^2 = 4k^2 = 2(2k^2)$ ***i, per tant,***
existeix un nombre enter k' tal que $n^2 = 2k'$ (observació: escollint $k' = 2k^2$, nombre enter).
Finalment,
n^2 és un nombre enter parell (observació: és B).

Potser, a la pràctica, en faríem una redacció més informal. Podem fer redactats més verbalitzats, menys formalitzats. Vegem un parell de versions en aquesta línia, d'entre moltes variants possibles:

Variant 1 (exposició 4): Sigui n un nombre enter parell. Aleshores, existeix un nombre enter k tal que $n = 2k$. Atès que hem de veure que n^2 és parell, calculem n^2 utilitzant l'expressió anterior, és a dir, $n^2 = (2k)^2 = 4k^2$. Hem de veure que n^2 és de la forma $2k'$, amb un nombre enter k' convenient. Expressant $n^2 = 2(2k^2)$ i prenent $k' = 2k^2$, nombre enter, resulta $n^2 = 2k'$, que és parell.

Variant 2 (exposició 5): Si n és un nombre enter parell, aleshores $n = 2k$ per a algun nombre enter k adequat. Per tant, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Considerant el nombre enter $k' = 2k^2$, tenim que $n^2 = 2k'$, amb k' enter convenient. En conseqüència, n^2 és parell, com s'havia de veure.

Enunciats incomplets

Els resultats no sempre s'enuncien explícitament en la forma $A \Rightarrow B$.

Exemples 1.4

Exemple 1. Per exemple, "$\sqrt{2}$ no és racional" no està enunciat d'aquesta forma, bàsicament perquè l'enunciat és incomplet, ja que no ens diu què és $\sqrt{2}$. Moltes vegades es pot reformular perquè sigui complet. Per exemple, en aquest, cas podria ser:
"si x és un nombre real positiu i $x^2 = 2$, aleshores x no és racional". ■

Exemple 2. Un altre exemple el tenim quan s'afirma, per a nombres reals qualssevol, $(x+y)^2 = x^2 + 2xy + y^2$. El problema és que moltes vegades els enunciats són fragmentaris o incomplets i hi ha moltes coses implícites, que se suposen; en aquest cas, podria reenunciar-se com: "si x i y són nombres reals, aleshores $(x+y)^2 = x^2 + 2xy + y^2$" i ja el tenim en forma de condicional. De fet, molts de resultats pressuposen una teoria general (algebraica, geomètrica) que no s'explicita, però que es pot fer servir en el curs de la demostració. ■

Exemple 3. Un tercer exemple el trobem en resultats de geometria, que solen comportar moltes definicions i teoria general implícites, que resultaria molt feixuc d'explicitar de manera completa a l'enunciat. Si considerem el teorema de Pitàgores, possiblement no calgui incloure al propi enunciat la definició de triangle rectangle, de catet, d'hipotenusa, de longitud, que estan involucrades a l'enunciat:

"si T és un triangle rectangle i a, b són les longituds dels catets de T i c és la longitud de la hipotenusa de T, aleshores $c^2 = a^2 + b^2$. ■

Sempre s'ha de procurar explicitar el màxim possible i evitar enunciats confusos o incomplets; si convé, reformulant i formalitzant al màxim l'enunciat. Al capítol de llenguatge de predicats veurem molts exemples i idees per a la formalització.

1.4. Operacions aritmètiques i ordre en $\mathbb{R}$

1.4.1. Operacions en $\mathbb{R}$

Enunciem com a teorema, per a fer-ne referència posteriorment, i per a sistematitzar, el resum de les propietats de la suma i el producte en el conjunt dels nombres reals.

Teorema 1.2 *Sigui $\mathbb{R}$ el conjunt dels nombres reals, amb les operacions usuals de suma $(+)$ i producte $(\cdot)$ ordinaris. Es compleixen les propietats següents, per a tot x, y, z nombres reals:*

– *Respecte de la suma,*

[S1]: $(x+y)+z = x+(y+z)$ *(propietat associativa)*

[S2]: $x+0 = 0+x = x$ *(existència d'element neutre (el zero))*

[S3]: $x+(-x) = (-x)+x = 0$ *(existència d'invers additiu (oposat) per a cada element)*

[S4]: $x+y = y+x$ *(propietat commutativa)*

– *Respecte del producte,*

[P1]: $(xy)z = x(yz)$ *(propietat associativa)*

[P2]: $1 \cdot x = x \cdot 1 = x$ *(existència d'element neutre)*

[P3]: $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$, $x \neq 0$ *(existència d'invers multiplicatiu per a tot x no nul, el recíproc $\frac{1}{x}$ específicament)*

[P4]: $xy = yx$ *(propietat commutativa-cos commutatiu)*

– *Relació entre les dues operacions: distributivitat del producte respecte de la suma, és a dir,*

[D1]: $x(y+z) = xy + yz$.

Respecte d'aquestes operacions, $(\mathbb{R}, +, \cdot)$ és un *cos commutatiu*. Respecte de l'operació suma, $(\mathbb{R}, +)$ és un *grup commutatiu*.

Observeu que "treure factor comú" en una suma no és més que una aplicació de la propietat distributiva [D1]. Es generalitza a més de dos sumands:

$$xa + xb + xc + xd = x(a+b+c+d),$$

aplicant la propietat associativa i la distributivitat per a dos sumands. O a n sumands:

$$xa_1 + xa_2 + \cdots + xa_i + \cdots + xa_{n-1} + xa_n = x(a_1 + a_2 + \cdots + a_i + \cdots + a_{n-1} + a_n)$$

(observeu la notació de punts suspensius).

Veiem que les propietats anteriors també les té $\mathbb{Q}$; no, en canvi, $\mathbb{Z}$. En el conjunt dels nombres naturals, es compleixen les propietats S1, S2, S4, P1, P2, P4, D1 i no la resta; en el conjunt dels nombres enters, es compleixen les propietats S1, S2, S3, S4, P1, P2, P4, D1, i no P3.

Notem que $x-y = x+(-y)$, $-x = (-1)x$ i $\frac{x}{y} = \frac{1}{x}y$ són formes de reescriptura convenients en algunes ocasions. Per exemple, pot convenir escriure

$$(-2)^3 = ((-1)\cdot 2)^3 = (-1)^3 2^3 \quad \text{o bé} \quad (-1)^k a^{n-k} b^k = a^{n-k}(-b)^k.$$

També en resulta que la diferència i la divisió no són pròpiament operacions, sinó casos particulars de les operacions de suma i producte.

Operacions i igualtat: Sumar i multiplicar membre a membre dues igualtats

Les propietats que s'indiquen a continuació són òbvies, ben conegudes, però les ressaltem perquè en el tema de les congruències ens plantejarem si també són certes les anàlogues, enunciades substituint igualtat per congruència. També s'expliciten per a ús i referència.

Teorema 1.3 *Per a nombres reals x, y, z, t, a qualssevol,*

a) $x = y \Rightarrow x + a = y + a$

b) $x = y \Rightarrow x - a = y - a$

c) $x = y, z = t \Rightarrow x + z = y + t, x - z = y - t$

d) $x = y \Rightarrow ax = ay$

e) $x = y, z = t \Rightarrow xz = yt$

(de fet, la primera i la segona són casos particulars de la tercera i la quarta, un cas particular de la cinquena).

És a dir, *podem sumar i multiplicar membre a membre dues igualtats i n'obtenim una nova igualtat*.

Demostració. Es poden justificar pas a pas amb tot detall algunes de les propietats bàsiques, amb la idea que el lector vegi l'ús de les propietats i com s'utilitzen per deduir nous resultats. Per exemple, vegem com provar $x = y \Rightarrow ax = ay$. Hem de veure, equivalentment, que $ax - ay = 0$; noteu que $x = y$ equival a $x - y = 0$. Aleshores, $ax - ay = a(x - y) = a0 = 0$. Més detallat:

$$ax - ay = ax + (-ay) = ax + a(-y) = a(x + (-y)) = a(x - y) = a0 = 0.$$

Vegem com demostrar

$$\left.\begin{array}{l} x=y \\ z=t \end{array}\right\} \Rightarrow xz=yt \qquad \text{o bé, equivalentment,} \qquad \left.\begin{array}{l} x-y=0 \\ z-t=0 \end{array}\right\} \Rightarrow xz-yt=0$$

En efecte, $xz-yt=xz-xt+xt-yt=x(z-t)+t(x-y)=x0+t0=0$.

Algunes argumentacions poden adaptar-se posteriorment a congruències o al càlcul matricial.

La demostració de la resta d'afirmacions es deixa per al lector.

Observació sobre l'enunciat. Vegem-ne algunes precisions notacionals.

Escrit d'una altra manera,

$$\left.\begin{array}{l} x=y \\ z=t \end{array}\right\} \Rightarrow x+z=y+t \qquad \left.\begin{array}{l} x=y \\ z=t \end{array}\right\} \Rightarrow xz=yt$$

Es pot generalitzar a un nombre qualsevol d'igualtats, és a dir,

$$\left.\begin{array}{l} x_1=y_1 \\ \dots \\ x_i=y_i \\ \dots \\ x_n=y_n \end{array}\right\} \Rightarrow x_1+\cdots+x_n=y_1+\cdots+y_n \qquad \left.\begin{array}{l} x_1=y_1 \\ \dots \\ x_i=y_i \\ \dots \\ x_n=y_n \end{array}\right\} \Rightarrow x_1\cdots x_n=y_1\cdots y_n$$

Observació. Cal interpretar la "coma" en enunciats com el següent:

$$x=y, z=t \Rightarrow xz=yt,$$

com a "i", de manera que es podria reescriure:

$$x=y \text{ i } z=t \Rightarrow xz=yt$$

i, per a evitar ambigüitats,

$$(x=y, z=t) \Rightarrow xz=yt$$

$$(x=y \text{ i } z=t) \Rightarrow xz=yt$$

o bé

"Si $x=y$ i $z=t$, aleshores $xz=yt$"

També cal interpretar com a conjunció l'enunciat anterior quan es presenta amb desplegament bidimensional. Així:

$$\left.\begin{array}{l} x=y \\ z=t \end{array}\right\} \Rightarrow xz=yt \qquad \text{és} \qquad \left.\begin{array}{l} x=y \\ \text{i} \\ z=t \end{array}\right\} \Rightarrow xz=yt$$

Propietat de simplificació (multiplicativa). Destaquem aquesta propietat pel seu interès comparatiu amb el cas de les congruències.

Teorema 1.4 *Si x, y, a són nombres reals,*

$$ax = ay, a \neq 0 \Rightarrow x = y.$$

Demostració. Multipliquem els dos membres de la igualtat per $\frac{1}{a}$, que existeix perquè $a \neq 0$. En efecte:

$$ax = ay \Rightarrow \tfrac{1}{a}(ax) = \tfrac{1}{a}(ay) \Rightarrow (\tfrac{1}{a}a)x = (\tfrac{1}{a}a)y \Rightarrow 1 \cdot x = 1 \cdot y \Rightarrow x = y$$

Es tendeix a pensar que sempre es pot simplificar, però això no és sempre així: per exemple, en congruències o en el cas del producte matricial (vegeu la secció posterior corresponent). Si escrivim $ax = ay$, això equival a $ax - ay = 0$, és a dir, per la distributivitat del producte respecte de la suma, $a(x-y) = 0$. Si tenim la propietat $bc = 0, b \neq 0 \Rightarrow c = 0$, podrem simplificar i deduir $x - y = 0$, és a dir, $x = y$. Observem com utilitzen amb cura i explicitació les propietats de les operacions, sobretot amb la idea de com procedir en altres contextos, per exemple, en el de les operacions matricials.

En el conjunt dels nombres reals, tenim una estructura algebraica derivada de les dues operacions de suma i producte, respecte de les quals tenim propietats que no sempre són certes en altres estructures algebraiques; n'esmentem algunes perquè el costum en l'ús rutinari és tan gran que pot fer que la importància passi desapercebuda pel lector.

$$ab = 0 \Rightarrow (a = 0 \text{ o } b = 0)$$

Quantificada:

$$\forall a \forall b (ab = 0 \to (a = 0 \vee b = 0)) \text{ (si queda sobreentès que } a, b \in \mathbb{R}\text{).}$$

De vegades, s'utilitza en aquestes formulacions:

$$(ab = 0, a \neq 0) \Rightarrow b = 0$$
$$(ab = 0, b \neq 0) \Rightarrow a = 0$$
$$(b \neq 0, a \neq 0) \Rightarrow ab \neq 0$$

L'observació que volem fer aquí és que aquesta propietat no és certa per a altres tipus d'objectes diferents dels nombres reals, com ara les matrius amb el producte matricial usual. Pot passar que el producte de dues matrius sigui zero (és a dir, la matriu zero), amb totes dues no nul·les. Vegeu la secció d'aquest capítol dedicada a una revisió de les operacions matricials.

També estem acostumats a la propietat commutativa en els reals (i, per tant, en els racionals, enters i naturals). Però no sempre es compleix en altres conjunts, com per exemple el de les matrius amb el producte matricial o amb l'operació de composició de funcions; això no impedeix que algunes matrius puguin commutar o que, per a dues funcions concretes, la composició sigui commutativa.

Per exemple, si considerem les funcions reals de variable real $f(x) = x+1$, $g(x) = x^2$, resulta que

$$\begin{aligned}(g\circ f)(x) &= g(f(x)) = g(x+1) = (x+1)^2 = x^2+2x+1,\\ (f\circ g)(x) &= f(g(x)) = f(x^2) = x^2+1.\end{aligned}$$

Existeixen valors x per als quals $(f\circ g)(x) \neq (g\circ f)(x)$. Per tant, és $g\circ f \neq f\circ g$.

1.4.2. Ordre en $\mathbb{R}$

En el conjunt dels nombres reals tenim definida la relació d'ordre habitual, que és un ordre *total*, en el sentit que dos elements sempre són comparables. Recordem les propietats bàsiques i les que el relacionen amb les operacions aritmètiques; això últim és especialment important en manipulació algebraica, de fórmules (la pregunta és: com es comporta l'ordre respecte de la suma i respecte del producte?):

Propietats: per a tot $x,y,z,a,b \in \mathbb{R}$, es satisfan les propietats reflexiva, transitiva i antisimètrica:

a) $x \leq x$ (reflexivitat)

b) Si $x \leq y$ i $y \leq z$, aleshores $x \leq z$ (transitivitat)

c) Si $x \leq y$ i $y \leq x$, aleshores $x = y$ (antisimetria)

Observació important: de $x \leq y$ i $x \leq z$ no se'n deriva cap relació entre z i y. En determinats problemes de demostració per inducció de propietats que són desigualtats ens trobem molt sovint en la situació següent: tenim o demostrem $a \leq b$, però ens cal arribar a $a \leq c$; moltes vegades els esforços es dediquem a provar que per a un d convenient és $b \leq d$ i $d \leq c$, si tenim sort! D'aquesta manera aconseguim el que volem: de $a \leq b \leq d \leq c$ resulta $a \leq c$, com volíem. Naturalment el problema radica en aquest pas intermedi. En veurem exemples al capítol d'inducció.

Noteu que $x < y$ significa $x \leq y$ i $x \neq y$; la negació de $x < y$ és $x \geq y$;

Tenim també: si $x < y$ i $y < z$, aleshores $x < z$.

En relació amb les operacions aritmètiques, vegem si es conserven les desigualtats:

Teorema 1.5 *Siguin x,y,b nombres reals qualssevol. Aleshores*

a) $x \leq y \Rightarrow x+a \leq y+a$ *(es manté l'orientació de la desigualtat)*

b) $x \leq y \Rightarrow x-a \leq y-a$ *(es manté l'orientació de la desigualtat)*

c) $x \leq y, b \geq 0 \Rightarrow bx \leq by$ *(es manté l'orientació de la desigualtat)*

d) $x \leq y, b < 0 \Rightarrow bx \geq by$ *(s'inverteix l'orientació de la desigualtat)*

Vegem les variants amb desigualtats estrictes:

Teorema 1.6 *Siguin x,y,b nombres reals. Aleshores*

a) $x < y \Rightarrow x+a < y+a$ *(es manté l'orientació de la desigualtat)*

b) $x < y \Rightarrow x-a < y-a$ *(es manté l'orientació de la desigualtat)* *c)* $x < y, b > 0 \Rightarrow bx < by$ *(es manté l'orientació de la desigualtat)*

d) $x < y, b < 0 \Rightarrow bx > by$ *(s'inverteix l'orientació de la desigualtat)*

Hi ha, per tant, un bon comportament de les operacions aritmètiques respecte de les desigualtats: es mantenen, tot i que poden canviat d'orientació. Aplicant aquestes propietats curosament i sistemàtica es poden fer manipulacions segures amb desigualtats.

Exemple 1.5 Per a nombres naturals a, b, proveu $0 < a < b \Rightarrow a^2 < b^2$.

Multipliquem per $a > 0$ els dos membres de $a < b$. Resulta $aa < ab$, és a dir, $a^2 < ab$. Multipliquem per $b > 0$ els dos membres de $a < b$. Resulta $ab < bb$, és a dir, $ab < b^2$.

Per transitivitat, $a^2 < b^2$. ■

Una propietat més, en $\mathbb{R}$:

Teorema 1.7 *Si a, b són nombres reals, aleshores*

$$a > 0, b > 0 \textit{ implica } ab > 0$$

$$a < 0, b < 0 \textit{ implica } ab > 0$$

$$a < 0, b > 0 \textit{ implica } ab < 0$$

Demostració. Vegem com podem demostrar, per exemple la primera, com a exercici d'aplicació de les propietats bàsiques anteriorment llistades:

Fem servir la propietat (3) del teorema anterior:

$$a > 0, b > 0 \text{ implica } ab > b \cdot 0 \text{ implica } ab > 0.$$

També tenim:

Teorema 1.8

$$ab > 0 \Longrightarrow \textit{a, b són del mateix signe (ambdós positius o ambdós negatius).}$$

$$ab < 0 \Longrightarrow \textit{a, b són de signes diferents.}$$

Més formalitzadament, però sense quantificar,

$$ab > 0 \Longrightarrow ((a > 0 \textit{ i } b > 0) \textit{ o } (a < 0 \textit{ i } b < 0))$$

$$ab < 0 \Longrightarrow ((a > 0 \textit{ i } b < 0) \textit{ o } (a < 0 \textit{ i } b > 0))$$

1.4.3. Valor absolut d'un nombre real

Definició 1.1 *Si $x \in \mathbb{R}$, es defineix el* valor absolut *de x com*

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \geq 0 \end{cases}$$

Observació. La definició anterior és per casos. Equivalentment, es pot definir mitjançant una fórmula compacta:

$$|x| = \text{màx}\,(x, -x)$$

Exemple 1.6

$$|3| = 3 \qquad |-3| = 3 \qquad |0| = 0$$
$$|-3| = -(-3) = 3, \text{ ja que } -3 < 0$$
$$|-3| = \text{màx}(-3, -(-3))) = \text{màx}(-3, 3) = 3 \;\blacksquare$$

Teorema 1.9 (Propietats bàsiques del valor absolut). *Per a tot* $x, y \in \mathbb{R}$,

a) $|x| \geq 0$ *(el valor absolut és sempre no negatiu)*
b) $|x| = 0$ *si, i només si,* $x = 0$
c) $|x + y| \leq |x| + |y|$
d) $|xy| = |x||y|$

També tenim:

$$|x| \leq a \Leftrightarrow -a \leq x \leq a.$$
$$|x - L| < \epsilon \Leftrightarrow -\epsilon < x - L < \epsilon \Leftrightarrow L - \epsilon < x < L + \epsilon.$$

1.4.4. Potenciació

Siguin $a, b \in \mathbb{R}, \quad n, m \in \mathbb{N}$.

$$a^0 = 1 \quad (a \neq 0).$$

Vegem que $a^{n+m} = a^n a^m$

En efecte: $a^{n+m} = a \overset{(n+m)}{\overbrace{\cdots}} a = a \overset{n}{\overbrace{\cdots}} a \cdot a \overset{m}{\overbrace{\cdots}} a = a^n a^m$

Exemple 1.7 $3^{k+5} = 3^k \cdot 3^5$ $\blacksquare$

Vegem que $a^{nm} = (a^n)^m = (a^m)^n$

En efecte: $(a^n)^m = a^n \overset{m}{\overbrace{\cdots}} a^n = a \overset{\overset{m}{\overbrace{n+\cdots+n}}}{\cdots} a = a \overset{nm}{\overbrace{\cdots}} a = a^{nm}$

Exemple 1.8 $3^{2k} = (3^2)^k = (3^k)^2$ $\blacksquare$

Observació: en general, $(a^n)^m$ i $a^{(n^m)}$ no coincideixen.

Exemple 1.9 $(a^2)^3 = a^6 \neq a^{(2^3)} = a^8 \quad (a \neq 1)$ $\blacksquare$

Vegem que $\boxed{(ab)^n = a^n b^n}$

En efecte: $(ab)^n = (ab) \overset{n}{\smile}{\cdots} (ab) = (a \overset{n}{\cdots} a)(b \overset{n}{\cdots} b) = a^n b^n$ per la propietat commutativa del producte en $\mathbb{R}$.

Exemple 1.10 $(-1)^k 5^k = ((-1)\cdot 5)^k = (-5)^k$ ■

Com obtenir alternança de signes:

$$(-1)^k = \begin{cases} 1 & \text{si } k \text{ és parell} \\ -1 & \text{si } k \text{ és senar} \end{cases}$$

Així, per obtenir:

$$1,-1,1,-1,1,-1,\ldots \quad \text{escrivim } (-1)^k \quad (k \geq 0).$$
$$-1,1,-1,1,-1,1,\ldots \quad \text{escrivim } (-1)^{k+1} \quad (k \geq 0).$$

Exemples 1.11

Exemple 1. Si $k \geq 1$, obtindrem

$1,-1,1,-1,1,-1,\ldots$ amb $(-1)^{k-1}$ o $(-1)^{k+1}$.

Exemple 2. Obtindrem $-2,2,-2,2,\ldots$ amb $(-2)^k, k \geq 1$, o bé $(-1)^k 2, k \geq 1$.

Exemple 3. Com obtenir

$$1-2+3-4+5-6+\cdots+(-1)^{n-1}n?$$

Amb $\displaystyle\sum_{k=1}^{n}(-1)^{k-1}k = \sum_{k=1}^{n}(-1)^{k+1}k$. ■

1.5. Algunes fórmules importants

Algunes fórmules útils

Vegem algunes fórmules útils, que el lector ja coneix, com a recordatori. Farem la demostració detallada d'alguna d'elles només per fer evident quines propietats es fan servir; en particular, depenen de la commutativitat del producte. I també es veuran com a pràctica addicional de demostracions.

Teorema 1.10 (Igualtats importants). *Si x,y són nombres reals qualssevol, aleshores es compleix:*

a) $(x+y)^2 = x^2 + 2xy + y^2$
b) $(x-y)^2 = x^2 - 2xy + y^2$

c) $(x+y)(x-y)=x^2-y^2$
d) $(x+y)^3=x^3+3x^2y+3xy^2+y^3$

Demostració (només de la primera)

Observi el lector l'estructura expositiva. Apliquem les propietats de les operacions suma i producte en $\mathbb{R}$.

$$\begin{aligned}
(x+y)^2 = & \ (x+y)(x+y), & \\
= & \ x(x+y)+y(x+y), & \text{per distributivitat del producte respecte} \\
& & \text{de la suma en } \mathbb{R} \\
= & \ x^2+xy+yx+y^2), & \text{per distributivitat del producte respecte de la suma} \\
= & \ x^2+(xy+yx)+y^2, & \text{per associativitat de la suma} \\
= & \ x^2+2xy+y^2, & \text{per la propietat commutativa del producte}
\end{aligned}$$

Anàlogament, es demostren les propietats *b)* i *c)*. La propietat *b* també es pot obtenir a partir de la *a*, ja que

$$(x-y)^2=(x+(-y))^2=x^2+2x(-y)+(-y)^2=x^2-2xy+y^2.$$

La fórmula $(x+y)^3=x^3+3x^2y+3xy^2+y^3$ es pot deduir, si no es recorda, calculant $(x+y)^3=(x+y)^2(x+y)$. Per exemple, $(n+1)^3=n^3+3n^2+3n+1$.

Per a fórmules de grau superior, en teoria podríem aplicar el mateix mètode, per exemple:

$$\begin{aligned}
(x+y)^5 &= (x+y)(x+y)(x+y)(x+y)(x+y) \\
(x+y)^4 &= (x+y)^3(x+y)=(x^3+3x^2y+3xy^2+y^3)(x+y)
\end{aligned}$$

però això està molt exposat a errors, a part que resulta feixuc. A més, no és aplicable amb exponents genèrics, com per exemple $(a+b)^{3n+2}$.

Quan el grau és alt, és preferible utilitzar la fórmula del binomi de Newton (vegeu la secció corresponent en aquest capítol i el capítol posterior específic) per a obtenir aquests desenvolupaments. Vegeu la **notació sumatòria** en un capítol posterior dedicat a sumatoris i tècniques de sumació.

Si x,y són nombres reals i n és un nombre natural,

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}=\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \text{ (intercanviant } x,y\text{)},$$

on el nombre combinatori $\binom{n}{k}$ es defineix com segueix a continuació.

El nombre combinatori $\binom{n}{k}$ es defineix, de manera general, per a $n \geq 0$ com

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } n \geq 0; 0 \leq k \leq n \\ 0 & \text{si } n \geq 0; (k < 0 \text{ o } k > n) \end{cases}$$

amb $j! = \begin{cases} 1 \cdot 2 \cdots j, & \text{si } j \geq 1 \\ 1, & \text{si } j = 0 \end{cases}$ (factorial de j, j nombre natural).

El nombre combinatori $\binom{n}{k}$ s'anomena també *coeficient binomial* o *nombre binomial* (apareix com a coeficient a la fórmula del binomi de Newton).

Vegem el teorema aplicat a algun dels exemples anteriors. Necessitarem alguns resultats:

Exemple 1.12

$$\binom{2}{0} = \frac{2!}{0!(2-0)!} = 1 \quad \binom{2}{1} = \frac{2!}{1!(2-1)!} = 2 \quad \binom{2}{2} = \frac{2!}{2!(2-2)!} = 1$$

$$\binom{3}{0} = 1 \quad \binom{3}{1} = 3 \quad \binom{3}{2} = 3 \quad \binom{3}{3} = 1$$

$$\binom{4}{0} = 1 \quad \binom{4}{1} = 4 \quad \binom{4}{2} = \frac{4!}{2!(4-2)!} = 6 \quad \binom{4}{3} = 4 \quad \binom{4}{4} = 1. \ \blacksquare$$

Només cal substituir els valors a les igualtats següents.

Exemple 1.13

Exemple 1. $(x+y)^2 = \sum_{k=0}^{2} \binom{n}{k} x^k y^{2-k} = \binom{2}{0} y^2 + \binom{2}{1} xy + \binom{2}{2} x^2. \ \blacksquare$

Exemple 2. $(x-y)^2 = (x+(-y))^2 = \sum_{k=0}^{2} \binom{n}{k} x^k (-y)^{2-k} =$

$\binom{2}{0}(-y)^2 + \binom{2}{1} x(-y) + \binom{2}{2} x^2 = \binom{2}{0} y^2 - \binom{2}{1} xy + \binom{2}{2} x^2. \ \blacksquare$

Exemple 3. $(x+y)^3 = \sum_{k=0}^{3} \binom{n}{k} x^k y^{3-k} =$

$\binom{3}{0} y^3 + \binom{3}{1} xy^2 + \binom{3}{2} x^2 y + \binom{3}{3} x^3. \ \blacksquare$

Exemple 4. $(x+y)^4 = \sum_{k=0}^{4} \binom{n}{k} x^k y^{4-k} =$

$\binom{4}{0} y^4 + \binom{4}{1} xy^3 + \binom{4}{2} x^2 y^2 + \binom{4}{3} x^3 y + \binom{4}{4} x^4. \ \blacksquare$

Una propietat molt útil és la següent:

Teorema 1.11 (Igualtats importants). *Si x, y són nombres reals qualssevol, i n és un nombre natural qualsevol, aleshores es compleix:*

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

Vegeu el capítol dedicat a aquesta fórmula.

1.6. Factorial, nombres combinatoris i fórmula del binomi de Newton

Factorial. Es defineix, per a tot $n \geq 0, n \in \mathbb{N}$:

- factorial de n, n factorial
- notació $n!$

com

$$n! = \begin{cases} 1 \cdot 2 \cdots n, & \text{si } n \geq 1 \\ 1, & \text{si } n = 0 \end{cases}$$

Així, $0! = 1$.

Exemples 1.14

Exemple 1. $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$. ■

Exemple 2. $3! = 1 \cdot 2 \cdot 3 = 6$. ■

Es pot expressar en termes de **"productoris"**:

$$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdots n = n! \qquad (n \geq 1).$$

Relació recurrent per al factorial. Per a $n \geq 1$,

$$n! = 1 \cdots (n-1)n = (1 \cdots (n-1))n = (n-1)!n.$$
$$(n+1)! = 1 \cdots (n-1)n(n+1) = (1 \cdots n)(n+1) = n!(n+1).$$

Exemple 1.15 $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 5!6$. ■

Podem definir la funció recursiva:

$$f(n) = nf(n-1)$$
$$f(0) = 1$$

S'obté efectivament el factorial:

$$\begin{aligned} f(0) &= 1 = 0! \\ f(1) &= 1 \cdot f(0) = 1 = 1! \\ f(2) &= 2 \cdot f(1) = 2 \cdot 1 = 2! \\ f(3) &= 3 \cdot f(2) = 3 \cdot 2 \cdot 1 = 3! \\ f(4) &= 4 \cdot f(3) = 4 \cdot 3 \cdot 2 \cdot 1 = 4! \end{aligned}$$

i així successivament.

Nombres combinatoris. Recordem la definició:

El nombre combinatori $\binom{n}{k}$ es defineix, de manera general, per a $n \geq 0$ com

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } n \geq 0; 0 \leq k \leq n \\ 0 & \text{si } n \geq 0; (k < 0 \text{ o } k > n) \end{cases}$$

Es pot reescriure de la forma següent:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = (\frac{n}{1})(\frac{n-1}{2})(\frac{n-2}{3})\cdots(\frac{n-j+1}{j})\cdots(\frac{n-k+1}{k}),$$

El nombre combinatori $\binom{n}{k}$ s'anomena també coeficient binomial o nombre binomial (apareix com a coeficient a la fórmula del binomi de Newton).

Suposem que $n, k \in \mathbb{N}, n \geq k \geq 0$. Aleshores, resulta:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Exemples 1.16

Exemple 1. $\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{n!} = 1.$ ■

Exemple 2. $\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n!}{n-1!} = \frac{(n-1)!n}{(n-1)!} = n.$ ■

Exemple 3. $\binom{n}{2} = \frac{n!}{2!(n-2)!}.$ ■

Exemple 4. $\binom{n}{n-1} = \frac{n!}{(n-1)!(n-(n-1))!} = \frac{n!}{(n-1)!} = \frac{(n-1)!n}{(n-1)!} = n.$ ■

Exemple 5. $\binom{n}{n} = \frac{n!}{n!(n-n)!} = 1.$ ■

Exemple 6. $\binom{9}{3} = \dfrac{9!}{3!(9-3)!} = \dfrac{9!}{3!6!} = \dfrac{6!7\cdot 8\cdot 9}{3!6!} = \dfrac{7\cdot 8\cdot 9}{2\cdot 3} = 7\cdot 4\cdot 3.$ ■

Segueixen ara algunes fórmules relacionades amb els nombres combinatoris o coeficients binomials.

Recordem que $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$, per a n,k naturals, amb $n \geq k \geq 0$, amb $0! = 1$.

Hi ha unes propietats trivials: $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = n$, de comprovació immediata.

Indiquem només uns resultats que poden ser útils (d'entre els molts possibles).

Teorema 1.12 (Simetria). *Es compleix:* $\binom{n}{k} = \binom{n}{n-k}$.

Així, $\binom{3}{2} = \binom{3}{3-2} = \binom{3}{1} = 3$, $\binom{4}{3} = \binom{4}{4-3} = \binom{4}{1} = 4$.

Teorema 1.13 (Fórmula recursiva). *Es compleix:* $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Fórmula del binomi de Newton

Teorema 1.14 (Binomi de Newton). *Per a $x,y \in \mathbb{R}$, $n \in \mathbb{N}$, es compleix:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Exemple 1.17

$$(x+y)^5 = \sum_{k=0}^{5} \binom{n}{k} x^k y^{5-k} =$$

$$\binom{5}{0} y^5 + \binom{5}{1} xy^4 + \binom{5}{2} x^2y^3 + \binom{5}{3} x^3y^2 + \binom{5}{4} x^4y + \binom{5}{5} x^5. \ ■$$

1.7. Part entera

Mereix una secció específica una funció molt important per a la informàtica, i específicament per a l'algorísmica, la funció part entera.

L'expressió *part entera* dóna nom a dues funcions molt importants per a l'algorísmica, concretament per a la formulació d'algorismes i per a programació; també té el seu interès en aritmètica i per a l'anàlisi d'algorismes en general.

Definicions:

Part entera inferior o, simplement, *part entera*.

Definició 1.2 *Si $x \in \mathbb{R}$, la* part entera inferior *de x, que denotem per $\lfloor x \rfloor$, és l'enter més gran que no supera x, és a dir*

$$\lfloor x \rfloor = \text{màx}\{m \in \mathbb{Z} | m \leq x\}$$

Exemple 1.18 $\lfloor 2{,}5 \rfloor = 2$, $\lfloor -2{,}5 \rfloor = -3$. ■

$\lfloor x \rfloor$ és l'enter per al qual es compleix $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Altres maneres equivalents d'expressar la part entera (inferior):

- Si x és un nombre real, aleshores existeix un únic enter n tal que $n \leq x \leq n+1$. És $\lfloor x \rfloor = n$.
- $x = \lfloor x \rfloor + h$ per a algun nombre real h tal que $0 \leq h < 1$.

  Exemple: $3{,}4 = \lfloor 3{,}4 \rfloor + 0{,}4$ ($\lfloor 3{,}4 \rfloor = 3$, $h = 0{,}4$)

  Exemple: $-3{,}4 = \lfloor -3{,}4 \rfloor + 0{,}6$ ($\lfloor -3{,}4 \rfloor = -4$, $h = 0{,}6$)

La propietat anterior és útil per a fer demostracions sobre la funció part entera.

La *part entera superior* d'un nombre real x es denota $\lceil x \rceil$ i es defineix:

Definició 1.3 *Si $x \in \mathbb{R}$, la* part entera superior *de x, que denotem per $\lceil x \rceil$, és l'enter més petit que supera o iguala x, és a dir:*

$$\lceil x \rceil = \text{mín}\{m \in \mathbb{Z} | m \geq x\}$$

Propietats:

Teorema 1.15 (Propietats de la part entera). *Siguin $x \in \mathbb{R}$ i $n \in \mathbb{Z}$.*

a) $x - 1 < \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$

b) $\lfloor x \rfloor = x$ *si, i només si, x és enter.*

c) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

d) $x \leq y \Rightarrow \lfloor x \rfloor \leq \lfloor y \rfloor$

e) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$

f) *Si $x \geq 0$ i $y \leq 0$, aleshores* $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor$

g) $\lfloor \frac{\lfloor x \rfloor}{m} \rfloor = \lfloor \frac{x}{m} \rfloor$ *(x nombre real, m nombre natural no nul)*

Teorema 1.16 *Tot nombre real positiu està comprès entre dues potències consecutives de 2. Concretament: Sigui x un nombre real positiu. Aleshores existeix n natural tal que* $2^n \leq x \leq 2^{n+1}$.

Demostració. Provarem que és cert i obtindrem una expressió de l'exponent n en funció de x.

La idea és imposar $2^n \leq x \leq 2^{n+1}$ per veure quin pot ser el nombre n apropiat. Prenem logaritmes en base 2:

$$n \log_2 2 \leq \log_2 x \leq (n+1) \log_2 2$$
$$n \leq \log_2 x \leq n+1$$

Prenem $n = \lfloor \log_2 x \rfloor$. Es compleix:

$$\lfloor \log_2 x \rfloor \leq \log_2 x \leq \lfloor \log_2 x \rfloor + 1$$

I, per tant, essent la funció exponencial creixent:

$$2^{\lfloor \log_2 x \rfloor} \leq 2^{\log_2 x} \leq 2^{\lfloor \log_2 x \rfloor + 1},$$

és a dir,

$$2^{\lfloor \log_2 x \rfloor} \leq x \leq 2^{\lfloor \log_2 x \rfloor + 1},$$

Així, doncs, $n = \lfloor \log_2 x \rfloor$.

Exercici: Estudieu què es pot afirmar per a $x < 0$. Estudieu si es pot fer una afirmació similar per a potències de 3.

Propietats de la part entera superior.

Teorema 1.17 *Siguin x, y nombres reals i n un nombre enter.*

a) $\lfloor x \rfloor \leq \lceil x \rceil$
b) $\lceil x \rceil = -\lfloor -x \rfloor$
c) $\lceil x+n \rceil = \lceil x \rceil + n$
d) $\lceil x \rceil - \lfloor x \rfloor \leq 1$
e) $\lfloor x+y \rfloor - 1 \leq \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$

Vegem un parell d'exemples addicionals d'ús de la funció part entera:

Exemple 1.19 *Una aplicació de la funció part entera per al càlcul del nombre de xifres d'un nombre natural* $n \geq 1$. Si n és un nombre natural expressat en base 10, el nombre de xifres és $\lfloor \log_{10} n \rfloor + 1$. Vegem-ne la justificació. Suposem que $n = a_k a_{k-1} \cdots a_1 a_0$ és l'expressió decimal de n, amb $a_k \neq 0$ i en què les xifres satisfan $0 \leq a_i \leq 9$, de manera que $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$. El nombre de xifres és $k+1$. Vegem que

$k = \lfloor \log_{10} n \rfloor$. Reescrivim $n = 10^k(a_k + a_{k-1}10^{-1} + a_{k-2}10^{-2} + \cdots + a_1 10^{-(k-1)} + a_0 10^{-k}) = 10^k(a_k + 0.a_{k-1} + 0.0a_{k-2} + \cdots + 0.0\cdots 0a_0) = a_k.a_{k-1}\cdots a_1 a_0$ Prenent logaritmes de base 10, resulta:

$$\log_{10} n = k + \log_{10} a_k.a_{k-1}\cdots a_1 a_0.$$

Si denotem $r = a_k.a_{k-1}\cdots a_1 a_0$, és $1 \leq r < 10$ $(1 \leq a_k)$ i, per tant, $0 \geq \log_{10} r < 1$. Prenent part entera, resulta:

$$\lfloor \log_{10} n \rfloor = \lfloor k + \log_{10} a_k.a_{k-1}\cdots a_1 a_0 \rfloor = \lfloor k \rfloor = k.$$

És vàlida una fórmula anàloga per a d'altres bases de numeració. ■

Exemple 1.20 *Ús de la funció part entera per a expressar formalment una bipartició d'una llista*. En la descripció d'algorismes recursius, es presenta sovint la necessitat de descompondre una llista de n elements, $L = [a_1, \cdots, a_n]$ en dues subllistes del mateix nombre d'elements (quan n és parell) o bé en el mateix nombre d'elements excepte, com a màxim, un elements (cas en què n és senar). Com es pot expressar això formalment, de manera que es cobreixin ambdós casos? Una possibilitat és utilitzar la funció part entera:

$$L_1 = [a_1, \cdots, a_{\lfloor \frac{n}{2} \rfloor}] \text{ i } L_2 = [a_{\lfloor \frac{n}{2} \rfloor + 1}, \cdots, n]. \ ■$$

1.8. Càlcul matricial

1.8.1. El conjunt de les matrius $n \times m$

Considerem el conjunt de les matrius $M_{n,m}$, de n files i m columnes:

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2m} \\ \cdots & & & & & \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{im} \\ \cdots & & & & & \\ a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nm} \end{pmatrix},$$

on $a_{ij} \in \mathbb{R}$. L'element a_{ij} és el que ocupa la fila i i la columna j, on $1 \leq i \leq n$ i $1 \leq j \leq m$; també es descriu la variació dels índexs com $i = 1, \cdots, n$, $j = 1, \cdots, m$. En casos concrets, potser convindrà escriure $a_{i,j}$ (per exemple, $a_{12,23}$. I encara: $(a_{ij})_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}}$ o altres variants, com $(a_{ij})_{\substack{1\leq i\leq n \\ 1\leq j\leq m}}$ .També s'anomenen *coeficients de la matriu*.

Exemple: Quin seria el terme de la fila 3, columna 5? a_{35}

Si es vol fer èmfasi en el fet que els escalars són reals, s'indica $M_{n,m}(\mathbb{R})$. En el cas particular que $m = n$, tenim les matrius quadrades d'ordre n, el conjunt de les quals s'indica per M_n o $M_n(\mathbb{R})$.

Les matrius poden servir per emmagatzemar dades (en distribució matricial, bidimensional).

1.8.2. Suma i producte per escalars

Definim les operacions de suma de matrius i de producte per escalars en el conjunt de matrius anterior $M_{n,m}$. Es defineixen element a element. Per exemple, per a la suma, si $A=(a_{ij})$, $B=(b_{ij})$, es defineix la matriu suma $C=A+B$ com una nova matriu del mateix tipus matriu $C=(c_{ij})$ dient quin és el valor del terme genèric c_{ij} en termes dels coeficients de les altres dues.

Definició 1.4 Suma matricial. *$C=A+B$: si $A=(a_{ij})$, $B=(b_{ij})$, es defineix la matriu suma $C=A+B$ com la matriu $C=(c_{ij})$ tal que és $c_{ij}=a_{ij}+b_{ij}$, $i=1,\cdots,n;\ j=1,\cdots,m$.*

Producte per escalars. *$D=\lambda A$: si $A=(a_{ij})$, $D=(d_{ij})$, és $d_{ij}=\lambda a_{ij}$, $i=1,\cdots,n;\ j=1,\cdots,m$.*

Teorema 1.18 *Amb les operacions de suma i producte per escalars abans definides, $M_{m,n}$ és un espai vectorial sobre $\mathbb{R}$.*

Demostració. És de rutina comprovar que, amb les operacions anteriors, de suma de matrius i de producte per escalars, es compleixen les propietats que defineixen un espai vectorial. En particular, la suma matricial és associativa i commutativa, és a dir, $A+(B+C)=(A+B)+C$ i $A+B=B+A$; el zero additiu és la matriu que té totes les entrades o posicions nul·les; si $A=(a_{ij})$, l'oposat sempre existeix i és $-A=(-a_{ij})$. ■

De vegades, també expressem els vectors $\vec{x}=(x_1,\ldots,x_n)$ en forma matricial, com a *matriu o vector columna* $n\times 1$:

$$X=\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

1.8.3. Producte matricial

A més de les operacions d'espai vectorial, definim una altra operació entre matrius, que poden ser de diferents espais vectorials de matrius.

Producte de matrius. Siguin $A=(a_{ij})\in M_{m,r}$, $B=(b_{ij})\in M_{r,n}$ (observeu que el nombre de columnes de la primera (A) coincideix amb el nombre de files de la segona (B)). Definim el producte (en l'ordre indicat) AB com la matriu $AB=(c_{ij})$ tal que $c_{ij}=\sum_{k=1}^{r} a_{ik}b_{kj}$ (fila i de A, columna j de B). Quan el producte és possible, aleshores és associatiu, és a dir, $A(BC)=(AB)C$ i és distributiu respecte de la suma (per la dreta i per l'esquerra), és a dir, $A(B+C)=AB+AC$ i $(B+C)A=BA+CA$.

Commutativitat? No es pot afirmar la commutativitat. Si $n=m$, podem multiplicar A,B en els dos ordres, AB, BA; en general, no coincideixen, és a dir, el producte no és commutatiu, llevat de casos especials. Vegeu un exemple de nocommutativitat:

Exemple 1.21

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ -2 & 2 \end{pmatrix} \blacksquare$$

És clar que no és cert $\forall A \forall B(AB = BA)$, és a dir, que és cert: $\exists A \exists B(AB \neq BA)$.

Matriu identitat. Respecte del producte en M_n (matrius quadrades d'ordre n), existeix la identitat, anomenada matriu identitat, denotada per I_n (o I, si n se sobrentén), és a dir, la matriu $n \times n$ tal que $AI = IA = A$. És la matriu formada per 1 a la diagonal principal i 0 a la resta de posicions.

$$I = I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \cdots & & & & & \\ 0 & 0 & \cdots & 1 & \cdots & 0 \\ \cdots & & & & & \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

Matriu inversa. Una matriu $A \in M_n$ (quadrada) es diu que és *invertible* si existeix $A' \in M_n$ tal que $AA' = A'A = I$. Si existeix, és única i es denota per $A' = A^{-1}$, de manera que $AA^{-1} = A^{-1}A = I$.

Exemple 1.22 Les matrius

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

són invertibles. La inversa de la matriu anterior és la matriu

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

Això es pot comprovar efectuant el producte matricial en els dos ordres i comprovant que és la matriu identitat. Utilitzant la identitat $\sin^2 t + \cos^2 t = 1$, resulta:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \blacksquare$$

Exemple 1.23 Les matrius de canvi d'escala, amb factors d'escala no nuls, són invertibles (a, b, c no nuls):

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}\begin{pmatrix} \frac{1}{a} & 0 & 0 \\ 0 & \frac{1}{b} & 0 \\ 0 & 0 & \frac{1}{c} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 & 0 \\ 0 & \frac{1}{b} & 0 \\ 0 & 0 & \frac{1}{c} \end{pmatrix}\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \blacksquare$$

Pot passar que el producte de dues matrius no nul·les sigui la matriu zero (un fenomen nou, que no es dóna en el conjunt dels nombres reals!), com a l'exemple següent:

Exemple 1.24

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \blacksquare$$

Exemple 1.25 Les matrius anteriors ens donen exemples de matrius no invertibles. En efecte, si tenim $XY = 0$, amb $X \neq 0$, $Y \neq 0$, aleshores les matrius X, Y no poden tenir inversa. Per exemple, si existís X^{-1}, multiplicant per l'esquerra resultaria $X^{-1}(XY) = X^{-1}0 = 0$, d'on $0 = X^{-1}(XY) = (X^{-1}X)Y = IY = Y$, cosa que és una contradicció. Si existís Y^{-1}, aleshores multiplicaríem per la dreta. $\blacksquare$

És fàcil veure que, si A, B són invertibles, també ho és AB i és $(AB)^{-1} = B^{-1}A^{-1}$. En efecte, es comprova immediatament que $(B^{-1}A^{-1})(AB) = (AB)(B^{-1}A^{-1}) = I$; per exemple, per associativitat, $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}IB = B^{-1}B = I$.

També resulta immediat, per comprovació multiplicant a dreta i esquerra, que, si A és invertible, també ho és A^{-1} i $(A^{-1})^{-1} = A$.

Transposada. Si $A = (a_{ij})$, es defineix la transposada A^T com la matriu obtinguda per simetria respecte de la diagonal principal de A. Equivalentment, correspon a intercanviar files per columnes. Si $A^T = (b_{ij})$, és $b_{ij} = a_{ji}$. És rutinari comprovar que $(A+B)^T = A^T + B^T$, $(AB)^T = B^T A^T$ i $(A^T)^T = A$.

→ 2

Preliminars: divisibilitat elemental i paritat

Aquest capítol tracta de conceptes bàsics de divisibilitat en els enters per tal de poder presentar exemples de poca complicació tècnica que siguin el vehicle expositiu de les idees de raonament, formalització i tècniques demostratives.

2.1. Divisió entera (a $\mathbb{Z}$)

Aquest és un concepte que té sentit en els nombres enters.

Teorema 2.1 *Siguin a, b nombres enters, on $b > 0$. Existeixen uns enters únics q, r tals que $a = bq + r$ i $0 \leq r < b$. La descomposició o expressió $a = bq + r$, amb la condició $0 \leq r < b$, és la divisió entera de a per b.*

Tenim diverses expressions del mateix:

a és el dividend de la divisió entera de a per b (o de a entre b)
b n'és el divisor
q n'és el quocient
r n'és el residu (el residu de la divisió entera de a per b).

Així, doncs, si r és el residu de la divisió entera d'a per b, és $0 \leq r < b$ o, equivalentment, $0 \leq r \leq b-1$, atès que $r \in \mathbb{Z}$. O també: $r \in \{0, 1, \cdots, b-1\}$; també es pot expressar: $r = 0 \vee r = 1 \vee \cdots \vee r = b-1$.

Exemples 2.1 Diversos exemples de divisió entera o de nodivisió entera.

Exemple 1. $10 = 3 \cdot 3 + 1$, amb $a = 10$, $b = 3$, $c = 3$, $r = 1$. ■

Exemple 2. (Exemples que no són divisió entera). No sempre la descomposició o expressió $a = bq + r$ és divisió entera. Cal que es compleixi la condició sobre el residu. Per exemple:

$$10 = 3 \cdot 4 - 2 = 3 \cdot 4 + (-2), \text{ on } a = 10,\ b = 3,\ r = -2, \quad \text{no és cap divisió entera.}$$
$$10 = 3 \cdot 2 + 4, \text{ on } a = 10,\ b = 3,\ r = 4, \quad \text{no és cap divisió entera.}$$

Cal la segona condició, sobre el residu, que no es satisfà en aquests exemples. ■

Exemple 3. $a = -13, b = 3$

$$-13 = 3 \cdot (-4) + 2 \qquad q = -5, r = 2.$$ ■

Exemple 4. No ho seria $-13 = 3(-4) - 1$ ■

La divisió entera es pot considerar, en general, per a qualsevol $b \neq 0$. Aleshores, cal fer la modificació següent: $a = bq + r$, amb $0 \leq r < |b|$.

Si el residu és zero, és a dir, $a = bq$, aleshores tenim una divisió entera *exacta*. També diem que "a és múltiple de b" (vegeu descripció posterior).

En la resolució de problemes, la consideració dels valors que pot prendre el residu és una base possible per a una demostració per casos. Vegem-ne exemples.

Exemples 2.2

Exemple 1. En el cas de la divisió entera de a entre $b = 2$, són possibles dos casos:

$$\begin{aligned} a &= 2q & (r = 0) \\ a &= 2q + 1 & (r = 1) \end{aligned}$$

O bé:

Cas 1: $r = 0$
Cas 2: $r = 1$ ■

Exemple 2. En el cas de la divisió entera de a entre $b = 3$, són possibles tres casos:

$$\begin{aligned} a &= 3q & (r = 0) \\ a &= 3q + 1 & (r = 1) \\ a &= 3q + 2 & (r = 2) \end{aligned}$$

O bé, a partir de $a = 3q + r$, tindríem:

Cas 1: $r = 0$
Cas 2: $r = 1$
Cas 3: $r = 2$ ■

Exemple 3. Per a $a = n, b = 4$, la divisió entera proporciona tots els casos possibles relatius als residus de la divisió entera:

$$n = 4q + r, \qquad 0 \leq r < 4, \qquad r \in \{0, 1, 2, 3\}$$

Per tant:

$$\begin{array}{lll} \text{Cas 1:} & n = 4q & (r = 0) \\ \text{Cas 2:} & n = 4q + 1 & (r = 1) \\ \text{Cas 3:} & n = 4q + 2 & (r = 2) \\ \text{Cas 4:} & n = 4q + 3 & (r = 3) \blacksquare \end{array}$$

Exemple 2.3 Vegem com a exemple que:

"tot nombre enter o bé és múltiple de 3, o bé és múltiple de 3 més 1, o bé és múltiple de 3 menys 1"

Avancem ja que els múltiples de 3 són de la forma $3q$, amb $q \in \mathbb{Z}$ (vegeu la secció següent).

Sigui n un nombre enter. Considerem la divisió entera de n per 3, és a dir, $n = 3q + r$, on $0 \leq r \leq 2$.

Així, tenim els casos:

Cas $r = 0$. És $n = 3q$ (múltiple de 3)
Cas $r = 1$. És $n = 3q + 1$ (múltiple de 3 més 1)
Cas $r = 2$. És $n = 3q + 2$ (múltiple de 3 més 2). Podem reescriure
$n = 3q + 2 = (3q + 2) + 1 - 1 = (3q + 3) - 1 = 3(q + 1) - 1$,
múltiple de 3 menys 1. $\blacksquare$

Exemple 2.4 Proveu que d'entre tres enters consecutius, exactament un d'ells és múltiple de 3. (ídem per a k en comptes de 3).

(com a conseqüència, el producte de tres enters consecutius és múltiple de 3).

$$n \in \mathbb{Z} \Rightarrow ((3 \mid n) \vee (3 \mid (n + 1)) \vee (3 \mid (n + 2))) \text{ (algun d'ells és múltiple de 3).}$$

(com a conseqüència: el producte de 3 enters consecutius és múltiple de 3).

Demostració. (s'introdueix una metodologia demostrativa, la demostració per casos).

Siguin $n, n + 1, n + 2$ els tres enters consecutius (observació: la demostració es podria fer similarment si es considerés $\{n - 1, n, n + 1\}$ o $\{n - 2, n - 1, n\}$, o $\{n + 1, n + 2, n + 3\}$ o altres ternes de nombres consecutius).

Considerem la divisió entera de n entre 3:

$$n = 3q + r, 0 \leq r < 3 \qquad (0 \leq r \leq 2)$$

Considerem els casos possibles (respecte de r):

Cas 1 $(r=0)$. $r=0 \Rightarrow n=3q$, múltiple de 3.
Cas 2 $(r=1)$. $r=1 \Rightarrow n=3q+1 \Rightarrow n+2=(3q+1)+2=3(q+1)$, múltiple de 3.
Cas 3 $(r=2)$. $r=2 \Rightarrow n=3q+2 \Rightarrow n+1=(3q+2)+1=3(q+1)$, múltiple de 3.

La divisió entera és única; els casos anteriors són mútuament excloents i, per tant només un dels $\{n,n+1,n+2\}$ és múltiple de 3.

Exercici. Proveu que, si $k \in \mathbb{N}, k \geq 2$ i $n \in \mathbb{Z}$, aleshores k divideix exactament un dels nombres consecutius:

$$n, n+1, \ldots, n+(k-1). \blacksquare$$

En relació amb la divisió entera, tenim que el quocient i el residu de la divisió entera es poden obtenir en termes de la funció part entera:

Teorema 2.2 *Si a,b,q,r són enters no negatius, $b>0$, tals que $a=bq+r$, amb $0 \leq r<b$, aleshores $q=\lfloor \frac{a}{b} \rfloor$ i $r=a-b\lfloor \frac{a}{b} \rfloor$.*

Teorema 2.3 *Si a,q,r són enters no negatius, $b<0$ (enter), tals que $a=bq+r$, amb $0 \leq r<b$, aleshores el quocient de la divisió entera de a per b és $q=\lceil \frac{a}{b} \rceil$ i el residu és $r=a-b\lceil \frac{a}{b} \rceil$.*

Aquest resultat pot ser interessant per a la programació o per a resoldre problemes.

2.2. Divisibilitat elemental (a $\mathbb{Z}$)

Definició 2.1 *Siguin a, b nombres enters. El nombre a és divisor de b si existeix k enter tal que $b=ka$.*

Expressions equivalents:

"a divideix b"
"b és múltiple de a"
"a és factor de b"
"b és divisible per a "

Tenim divisió entera exacta o bé divisió entera amb residu 0.

NOTACIÓ. La notació $a|b$ denota "a és divisor de b".

NOTACIÓ. La notació $a \nmid b$ denota "a no és divisor de b".

Exemples 2.5

Exemple 1. "6 és divisor de 18", ja que $18 = 3 \cdot 6$ (aquí $k = 3$). (Notació: $6|18$)

Exemple 2. $4|12$, ja que $12 = 4 \cdot 3$.

Exemple 3. $5|15$.

Exemple 4. $3 \nmid 14$.

Exemple 5. $5 \nmid 17$. ■

Fórmula de predicats:

$$\exists k(k \in \mathbb{Z} \land b = ka)$$
$$\exists k \in \mathbb{Z}(b = ka)$$

La negació $a \nmid b$ es pot expressar per la fórmula de predicats:

$$\forall k(k \in \mathbb{Z} \to b \neq ka)$$

Formulacions equivalents a $a|b$: $b = ka$ per a un k enter convenient, per a un enter k adequat, per a algun k enter.

Aleshores, $a|b$ si, i només si, la divisió entera de a per b és exacta, és a dir, amb residu 0. La divisibilitat de a per b correspon a residu *nul* en la divisió entera:

$$a = bc + r, \qquad r = 0.$$

Exemple 2.6 Quina forma tenen els múltiples de 3? Són els de la forma $3q$, per a q enter. Donat un enter a múltiple de 3, existeix un enter q tal que $a = 3q$.

Quina forma tenen els enters no múltiples de 3? Els casos de no-divisibilitat per 3 són $a = 3q + 1$, $a = 3q + 2$.

El conjunt dels múltiples de 3 és $\{3q | q \in \mathbb{Z}\} = \{n | \exists k \in \mathbb{Z} \land b = k3\}$. ■

Primers i compostos. Un nombre $p \in \mathbb{Z}, p \geq 2$ es diu que és *primer* si no té més divisors positius que 1 i p: $\pm 1, \pm p$, són els seus divisors.

En cas contrari, és compost.

Dos nombres són *primers relatius* o primers entre si, si no tenen divisors comuns diferents de 1 i -1.

Si $\frac{a}{b} \in \mathbb{Q}$, sempre podem simplificar els divisors comuns de a i b. Per exemple, si

$$\begin{aligned} a &= a'd \\ b &= b'd, \end{aligned}$$

aleshores $\dfrac{a}{b} = \dfrac{a'd}{b'd} = \dfrac{a'}{b'}$.

Si es fa la simplificació màxima, simplificant tots els divisors comuns, aleshores:

$$\frac{a}{b} = \frac{a''}{b''} \qquad (ab'' = ba'')$$

amb $\frac{a''}{b''}$ primers relatius. La fracció $\frac{a''}{b''}$ és irreductible.

Uns resultats útils d'aritmètica elemental: lemes de Gauss i d'Euclides

Tot i que es presentaran i es demostraran en el seu context, ja enunciem aquí, sense demostració, aquests importants resultats, que són molt útils per a determinades demostracions.

Teorema 2.4 (Lema de Gauss). *Siguin a, b, c nombres enters. Suposem que es compleix: $a|bc$ i $\operatorname{mcd}(a,b) = 1$. Aleshores $a|c$.*

És a dir, si un nombre divideix un producte de dos factors i és primer relatiu amb un d'ells, aleshores divideix l'altre.

Teorema 2.5 (Lema d'Euclides). *Siguin a, b, c nombres enters. Suposem que es compleix: p primer, $p|ab$. Aleshores $p|a$ o $p|b$.*

És a dir, si un nombre primer divideix un producte de dos factors, aleshores divideix algun dels factors.

2.3. Paritat: ser parell, ser senar

Parells i senars. Per què interessa tenir una descripció de la paritat? Per a poder fer raonaments, deduccions i manipulacions sobre nombres parells i senars, necessitat que es presenta amb freqüència, resulta molt útil veure com es pot expressar la condició de ser parell i de ser senar. Volem poder tractar amb fórmules les propietats de "ser parell" i "ser senar".

També necessitem enunciats de paritat, com ara "suma de parells és parell (és un nombre parell)", "suma de dos senars és parell" o similars, per a poder-nos-hi referir o utilitzar directament en les demostracions.

2.3.1. Com expressar que un nombre enter és parell?

Definició 2.2 *Un nombre enter n és parell si, i només si, és divisible per 2.*

Equivalentment, n és parell si, i només si, és múltiple de 2. És a dir, n és parell si, i només si, $2|n$. Això es pot expressar de diverses maneres equivalents:

existeix un nombre enter k tal que $n = 2k$
existeix $k \in \mathbb{Z}$ tal que $n = 2k$
$n = 2k$ per a algun enter k convenient
$n = 2k$ per a algun enter k adequat

o similars a les anteriors.

No és més que un cas particular de divisibilitat, la divisibilitat per 2.

Exemples 2.7

Exemple 1. $6 = 2k$, amb $k = 3 \in \mathbb{Z}$. ■

Exemple 2. $-14 = (-7)2$, amb $k = -7 \in \mathbb{Z}$. ■

També es diu que els nombres parells són de la forma $2k$, per a algun k enter.

En el llenguatge de predicats, $\exists k(k \in \mathbb{Z} \wedge n = 2k)$.

Observeu que k depèn de n, de manera que estrictament hauríem d'escriure $n = 2k_n$, cosa a la qual renunciem per no fer la notació massa feixuga.

Encara es por expressar d'una altra manera equivalent. Considerem la divisió entera de n per 2: existeixen k, r enters tals que $n = 2k + r$, amb $0 \leq r < 2$, és a dir, $0 \leq r \leq 2 - 1 = 1$. Hi ha divisibilitat de n per 2 si, i només si, $r = 0$, és a dir, si, i només si, el residu de la divisió entera de n per 2 és 0. També es pot dir que n és parell si, i només si, la divisió entera per 2 és exacta.

2.3.2. Com expressar que un nombre enter és senar?

Definició 2.3 *Un nombre és senar (o imparell) si, i només si, no és parell.*

Per tant, un nombre és senar si, i només si, no és divisible per 2, és a dir, si, i només si, no és múltiple de 2. En notació, seria $2 \nmid n$. Ara bé, un nombre n no és divisible per 2 si el residu de la divisió entera de n per 2 és no nul (altrament, seria múltiple de 2). Considerem la divisió entera $n = 2k + r$, amb $0 \leq r \leq 1$. Atès que $r \neq 0$, és $r = 1$.

Així doncs, si n és un nombre senar, s'expressa com $n = 2k + 1$, per a un k enter convenient. Recíprocament, si un nombre n s'expressa com $n = 2k + 1$, per a algun k enter, aleshores n és senar. Ho provem per *reducció a l'absurd*. En efecte, si fos parell i, per tant, de la forma $n = 2k'$, k' enter, seria $2k' = 2k + 1$, d'on $2(k' - k) = 1$. Ara bé, $2|2(k' - k)$ i, per tant, $2|1$, que és absurd. Per tant, n és senar.

Així, els nombres senars n són els que s'expressen com $n = 2k + 1$, per a un enter k convenient. Són de la forma $2k + 1$, per a algun k enter. Observeu que k depèn de n, de manera que estrictament hauríem d'escriure $n = 2k_n + 1$, cosa que no farem.

Un nombre n és senar si, i només si, es compleix alguna de les afirmacions equivalents següents:

existeix un nombre k enter tal que $n = 2k+1$
existeix $k \in \mathbb{Z}$ tal que $n = 2k+1$
$n = 2k+1$ per a algun k enter convenient
$n = 2k+1$ per a algun k enter adequat

o similars als anteriors.

Així:

Exemples 2.8

Exemple 1. $7 = 2k+1$, amb $k = 3 \in \mathbb{Z}$. ■

Exemple 2. $-13 = (-7)2+1$, amb $k = -7 \in \mathbb{Z}$. ■

En el llenguatge de predicats, $\exists k(k \in \mathbb{Z} \wedge n = 2k+1)$.

Resumint doncs, tenim que n és senar si, i només si, no és parell. És a dir, n és senar si, i només si, $2 \nmid n$. Els nombres senars són els que no són divisibles per 2.

Expressió alternativa. Els nombres senars són també els que s'escriuen com $n = 2q-1$, amb q enter. En efecte, si n és senar, existeix k enter tal que $n = 2k+1$. Imposem $2k+1 = 2q-1$ i veiem que es pot obtenir sempre un enter q convenient en funció de k, i viceversa: si $2k+1 = 2q-1$, és $2(q-k-1) = 0$, d'on $q-k-1 = 0$, és a dir, $q = k+1$ i $k = q-1$, i podem així passar d'una expressió a l'altra.

Exemples 2.9

Exemple 1. $17 = 2 \times 8 + 1$ $(k = 8)$. ■

Exemple 2. $17 = 9 \times 2 - 1$ $(q = 9)$. ■

Per què són útils les expressions anteriors? Per a poder operar, poder argumentar, poder manipular amb fórmules on intervé la paritat o es fan afirmacions en aquest sentit, o per a poder enunciar i demostrar propietats, fer problemes. També per a fer raonaments per casos segons la paritat.

Alguns trucs (nombres consecutius) De vegades, en el curs de demostracions relatives a divisibilitat, cal provar que alguna expressió o fórmula és parell. Per exemple, suposem que hem de veure que n^2+n, per tot n enter, és un nombre parell.

Escrivim $n^2+n = n(n+1)$, com a producte de dos nombres enters consecutius. Ara bé, si dos nombres enters són consecutius, aleshores un és parell i l'altre, senar. Un dels dos és múltiple de 2 i, per tant, el producte és múltiple de dos, parell. Per exemple, si $n = 2k$, aleshores $n(n+1) = 2k(n+1) = 2k'$, parell.

Donats dos nombres enters consecutius, exactament un és múltiple de 2 (parell) i l'altre, senar. L'afirmació és intuïtiva. Ara bé, podem aportar una demostració formal per casos, segons la paritat de n. En efecte:

Cas 1. Si n és parell, ja està.

Cas 2. Si n és senar, aleshores $n+1$, suma de dos senars, és parell.
O també: $n = 2k+1$ per a algun enter k; aleshores
$n+1 = (2k+1)+1 = 2k+2 = 2(k+1) = 2k'$, parell.

També es podrà afirmar per a tot producte de consecutius: $(n-1)n$, $(n+1)(n+2)$, $(n+13)(n+14)$, $(n-2)(n-1)$, $(n-4)(n-3)$ i infinits més. En general, $\forall m(m \in \mathbb{Z} \to 2|m(m+1))$.

Com escriure nombres enters consecutius? Si a,b són consecutius i a és el menor, aleshores $b = a+1$, de manera que sempre podem suposar que són parelles de la forma $a, a+1$. També tenim, equivalentment, $n-1, n$; $n-2, n-1$; $n+34, n+35$. I si volem escriure tres enters consecutius? Siguin a,b,c tres enters consecutius, amb $a < b < c$. Aleshores $b = a+1$, $c = b+1$. Així, $c = b+1 = (a+1)+1 = a+2$. Per tant, són de la forma $a, a+1, a+2$. També els podem expressar d'altres maneres: $n-2, n-1, n$; $n-1, n, n+1$. Com passar de l'un a l'altre? Per exemple, els nombres consecutius $a, a+1, a+2$ es poden escriure de la forma $n-2, n-1, n$ fent $a = n-2$ (d'on $n = a+2$).

Com escriure k enters consecutius? $n, n+1, n+1, \cdots, n+k$; $n-k, n-k+1, n-k+2, \cdots, n-1, n$ i altres formes o modalitats.

Una argumentació amb error. Indiqueu si hi ha un error a l'argumentació següent:

"Donats els nombres enters consecutius $n-1$, n, $n+1$, el nombre $(n-1)n(n+1)$ és múltiple de 4 pel motiu següent. El producte de dos consecutius és parell i, per tant, $n(n+1)$ aporta un factor 2 (al producte dels tres); el mateix podem afirmar per a $(n-1)n$, que també aporta un factor 2. Tenim, per tant, un factor 4 i, en conseqüència $(n-1)n(n+1)$ és múltiple de 4."

És fals: n'hi ha prou d'aportar un contraexemple: $5 \cdot 6 \cdot 7$. Perquè no és correcte el raonament? L'argument és incorrecte perquè pot ocórrer que hi hagi un sol factor 2, aportat pel terme central de la terna, n, que serveixi per a l'afirmació sobre les dues parelles.

2.3.3. Resultats bàsics de paritat

Vegem exercicis resolts sobre resultats bàsics.

PROBLEMA 2.1

"Parell més parell és parell"

a) *Demostreu que la suma de dos enters parells és un enter parell.*
b) *Demostreu que la diferència de dos nombres parells és parell.*
c) *Demostreu que la suma d'un nombre finit d'enters parells és parell.*

Solució. Establim la notació per als dos primers apartats: siguin a, b nombres enters.

a) Demostreu que la suma de dos enters parells és un enter parell.

Com que a és parell, podem escriure $a = 2k$ per a un k enter adequat. Anàlogament, $b = 2k'$, amb k' enter convenient. Volem veure que $a+b$ satisfà la mateixa propietat, és a dir, $a+b = 2\alpha$, per a un enter α convenient. Tenim $a+b = 2k+2k' = 2(k+k')$: prenem $\alpha = k+k'$.

Atenció: És un error freqüent escriure en el curs de la resolució d'aquest problema $a = 2k$, $b = 2k$, amb el *mateix* k. Atès que a i b intervenen a la mateixa demostració, res no ens permet suposar la igualtat de k, k', tot i que en aquest cas, s'arribaria a la conclusió buscada (però l'argumentació seria incorrecta).

b) Demostreu que la diferència de dos nombres parells és parell. La demostració és del tot anàloga a la de la suma de dos parells.

Demostreu que la suma d'un nombre finit d'enters parells és parell. La idea bàsica és la mateixa de les demostracions anteriors. El problema és essencialment notacional i de com expressar la situació.

En primer lloc, hem d'indicar quants nombres parells se sumen: *sigui r el nombre de sumands*. Denotem per $a_1, \cdots, a_r$ els sumands. Com que són parells, per a cada i $(1 \leq i \leq r)$, existeix un enter k_i tal que $a_i = 2k_i$. Aleshores $a_1 + a_2 + \cdots + a_r = 2k_1 + 2k_2 + \cdots + 2k_r = 2(k_1 + k_2 + \cdots + k_r) = 2k'$, parell, amb $k' = k_1 + k_2 + \cdots + k_r \in \mathbb{Z}$.

PROBLEMA 2.2

"Senar més senar és parell"

a) *Demostreu que la suma de dos enters senars és un enter parell.*
b) *Demostreu que la diferència de dos nombres senars és parell.*
c) *Com és la suma d'un nombre finit d'enters senars? (parell, senar).*

Solució

a) La suma de dos nombres enters senars és un enter parell.
Formalització:

$$\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge a \text{ senar i } b \text{ senar}) \Rightarrow a+b \text{ parell})$$

$$\forall a \forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2|a+b) \text{ (suposant } a \in \mathbb{Z} \wedge b \in \mathbb{Z}).$$

$$a \text{ senar} \Rightarrow a = 2k+1, \text{ per a un } k \in \mathbb{Z} \text{ adequat}$$

$$b \text{ senar} \Rightarrow b = 2k'+1, \text{ per a un } k' \in \mathbb{Z} \text{ convenient}$$

(de fet, $a = 2k_a + 1, b = 2k_b + 1$)

Aleshores:

$$a+b=(2k+1)+(2k'+1)=2(k+k')+2=2(k+k'+1), \text{ parell}$$

Observació. Podem fer servir expressions de la forma:

$$\begin{array}{ll} \textit{Variant 1}: & a=2k+1,\ b=2k'-1 \\ \textit{Variant 2}: & a=2k-1,\ b=2k'+1 \\ \textit{Variant 3}: & a=2k-1,\ b=2k'-1 \end{array}$$

Vegem que la demostració es pot realitzar amb qualsevol de les variants anteriors:

Variant 1: $a=2k+1, b=2k'-1$. Aleshores

$$a+b=(2k+1)+(2k'-1)=2k+2k'=2(k+k'), \text{ parell.}$$

Variant 2: (similar a l'anterior) $a=2k-1, b=2k'+1$. Aleshores

$$a+b=(2k-1)+(2k'+1)=2k+2k'=2(k+k'), \text{ parell.}$$

Variant 3: $a=2k-1, b=2k'-1$. Aleshores

$$a+b=(2k-1)+(2k'-1)=2k+2k'-2=2(k+k'-1), \text{ parell.}$$

b) Per a la diferència de dos senars, l'argumentació és similar (i també segons les diverses variants possibles per a l'expressió dels nombres senars, l'estudi del qual es deixa al lector):

$$a-b=(2k+1)-(2k'+1)=2k-2k'=2(k-k'), \text{ parell.}$$

c) Com és la suma de $m \geq 2$ nombres enters senars, des del punt de vista de la paritat?

És $n_i=2k_i+1$, per a un $k_i \in \mathbb{Z}$ convenient, per a tot $i=1,\ldots,m$.

Aleshores (vegeu el capítol posterior sobre sumatoris):

$$s=\sum_{i=1}^{m} n_i=\sum_{i=1}^{m}(2k_i+1)=\sum_{i=1}^{m}(2k_i)+\sum_{i=1}^{m}1=2\sum_{i=1}^{m}k_i+m=2k'+m,$$

amb $k'=\sum_{i=1}^{m} k_i$. Ara són possibles dos casos, segons la paritat de m:

Cas 1. m és parell, és a dir, $m=2m'$, per a algun $m' \in \mathbb{Z}$. Aleshores

$$s=2k'+m=2k'+2m'=2(k'+m'), \text{ parell.}$$

(o també fent servir que "la suma de dos parells és parell").

Cas 2. m és senar, és a dir, $m = 2m' + 1$, per a algun $m' \in \mathbb{Z}$ (o, equivalentment, $m = 2m'' - 1$ per a algun enter m''). Aleshores:

$$s = 2k' + m = 2k' + (2m' + 1) = 2(k' + m') + 1, \text{ senar.}$$

També com a conseqüència de "parell més senar és senar" aplicat a $2k' + m$ (vegeu un dels problemes posteriors de la secció).

El resultat, per tant, depèn de la paritat de m:

"La suma de m nombres enters senars és $\left\{ \begin{array}{c} \text{parell} \\ \text{senar} \end{array} \right\}$ si m és $\left\{ \begin{array}{c} \text{parell} \\ \text{senar} \end{array} \right\}$"

"La suma de m nombres enters senars és $\left\{ \begin{array}{l} \text{parell, si } m \text{ és parell} \\ \text{senar, si } m \text{ és senar} \end{array} \right.$"

Alternativa al desenvolupament anterior sense sumatoris:

$$\begin{aligned}
S &= n_1 + \overset{m}{\smile}\!\!\!\!\cdots + n_m = \\
&= (2k_1 + 1) + \overset{m}{\cdots} + (2k_m + 1) = \\
&= (2k_1 + \overset{m}{\cdots} + 2k_m) + (1 + \overset{m}{\cdots} + 1) \text{ (per associativitat i commutativitat de la suma)} \\
&= 2(k_1 + \overset{m}{\cdots} + k_m) + m \text{ (per la distributivitat del producte respecte de la suma)} \\
&= 2k' + m, \text{amb } k' = k_1 + \overset{m}{\cdots} + k_m.
\end{aligned}$$

PROBLEMA 2.3

"El producte de dos senars és senar"
"Senar per senar és senar"

a) *Demostreu que el producte de dos enters senars és un enter senar.*
b) *El producte d'un nombre finit d'enters senars és senar.*

Solució

$$\left. \begin{array}{l} a \text{ senar} \\ b \text{ senar} \end{array} \right\} \Rightarrow ab \text{ senar.}$$

En efecte:

$$a = 2k + 1, \text{ per a } k \in \mathbb{Z} \text{ convenient.}$$
$$b = 2k' + 1, \text{ per a } k' \in \mathbb{Z} \text{ convenient.}$$

Aleshores:

$$ab = (2k+1)(2k'+1) = 4kk' + 2k + 2k' + 1 = 2(2kk' + k + k') + 1, \text{ senar.}$$

Variant argumental 1:

$$\begin{aligned} a &= 2k+1, b = 2k'-1 \Rightarrow ab = (2k+1)(2k'-1) = 4kk' - 2k + 2k' - 1 = \\ &= 2(2kk' - k + k') - 1 = 2k'' - 1, \text{ senar } (k'' = 2kk' - k + k', \text{ enter}). \end{aligned}$$

Variant argumental 2 (de fet, per raons de simetria, aquest cas és essencialment l'anterior):

$$\begin{aligned} a &= 2k-1, b = 2k'+1 \Rightarrow ab = (2k-1)(2k'+1) = 4kk' + 2k - 2k' - 1 = \\ &= 2(2kk' - k - k') - 1 = 2k'' - 1, \text{ senar (amb } k'' = 2kk' - k - k', \text{ enter).} \end{aligned}$$

Variant argumental 3:

$$\begin{aligned} a &= 2k-1, b = 2k'-1 \Rightarrow ab = (2k-1)(2k'-1) = 4kk' - 2k - 2k' + 1 = \\ &= 2(2kk' - k - k') + 1 = 2k'' + 1, \text{ senar (amb } k'' = 2kk' - k - k', \text{ enter).} \end{aligned}$$

En el cas d'un producte de $r \geq 2$ factors senars, s'hauria de demostrar el resultat per inducció, utilitzant com a pas bàsic el resultat de l'apartat anterior.

PROBLEMA 2.4

"Producte amb un parell és parell"
Siguin a, b nombres enters. Proveu:

$$2|a \Rightarrow 2|ab$$

Solució

Hipòtesi: $2|a$. Completa: $a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2|a$.

Tesi: $2|ab$.

Per la hipòtesi, existeix un enter k tal que $a = 2k$. Vegem que ab és de la forma típica d'un nombre parell. En efecte, $ab = (2k)b = 2(kb) = 2k'$, parell, amb $k' = kb \in \mathbb{Z}$.

PROBLEMA 2.5

"Parell més senar és senar"
Siguin a, b nombres enters. Proveu:

$$a \text{ parell, } b \text{ senar} \Rightarrow a + b \text{ senar.}$$

Solució

Hipòtesi: $2|a \wedge 2 \nmid b$.

Tesi: $2 \nmid a + b$.

Com que a és parell, $a = 2k$ per a un enter k convenient. Per ser b senar, $b = 2k' + 1$ per a un enter k' adequat. Vegem que $a + b$ té la forma típica d'un nombre senar:

$$a + b = (2k) + (2k' + 1) = 2(k + k') + 1 = 2k'' + 1, \text{ senar, amb } k'' = k + k' \in \mathbb{Z}.$$

Variant argumental:

$$a+b=2k+(2q-1)=2(k+q)-1=2r-1, \text{ senar, amb } r=k+q\in\mathbb{Z}.$$

Els resultats anteriors es poden fer servir lliurement en argumentacions.

Exemple 2.10 Vegem que, per a tot enter n, és n^2+n-2 parell.

Mètode 1. Hem vist que $n^2+n=n(n+1)$, producte de dos enters consecutius, és parell. Atès que la diferència de dos parells és parell, en resulta l'afirmació.

Observi el lector que en el mètode següent es presenta una metodologia de demostració, la *demostració per casos*.

Mètode 2. Fem una distinció de casos segons la paritat de n i hi apliquem els resultats dels problemes anteriors.

- **Cas 1.** n és parell. Com que el producte de parells és parell, resulta $n^2=n\cdot n$ parell. Ara n^2+n és la suma de dos parells, que és parell. Considerem l'expressió $n^2+n-2=(n^2+n)-2$ com a diferència de parells: el resultat és parell.

- **Cas 2.** n és senar. Donat que el producte de senars és senar, resulta $n^2=n\cdot n$ senar. Ara n^2+n és la suma de dos senars, que és parell. Considerem l'expressió $n^2+n-2=(n^2+n)-2$ com a diferència de parells: el resultat és parell.

Mètode 3. Fem una distinció de casos segons la paritat de n i raonem per substitució directa, sense utilitzar els resultats dels problemes anteriors.

- **Cas 1.** n és parell. Aleshores $n=2k$ per a cert enter k. Substituïm: $n^2+n-2=(2k)^2+(2k)-2=2(2k^2+k-1)=2k'$, amb $k'=2k^2+k-1$ enter. Així, n^2+n-2 és parell.
- **Cas 2.** n és senar. Aleshores $n=2k+1$ per a un enter k. Substituïm: $n^2+n-2=(2k+1)^2+(2k+1)-2=(4k^2+4k+1)+(2k+1)-2=4k^2+6k=2(2k^2+3k)=2k'$, amb $k'=2k^2+3k$ enter. Així, n^2+n-2 és parell.

Observació: també es pot fer servir que $n=2q-1$ per a algun q enter. En efecte, $n^2+n-2=(2q-1)^2+(2q-1)-2=(4q^2-4q+1)+(2q-1)-2=4q^2-2q-2=2(2q^2-q-1)=2q'$, amb $q'=2q^2-q-1$ enter. ■

Exemple 2.11 Provem que, per a tot enter n, n^2-n+4 és parell.

Mètode 1. Per casos segons la paritat de n.

- **Cas 1.** n és parell. Aleshores n^2 és parell, per ser producte de dos parells. Aleshores n^2-n és parell perquè és la diferència de dos parells. Finalment, $n^2-n+4=(n^2-n)+4$, suma de dos parells, és parell. Alternativament, reescrivim $n^2-n+4=n(n-1)+4$. Aleshores $n(n-1)$ és parell, per ser producte de dos nombres enters consecutius. Així, $n(n-1)+4$ és suma de dos parells i, per tant, parell.

- **Cas 2.** n és senar. Aleshores $n^2 = n \cdot n$ és senar, perquè és el producte de dos senars. Restant dos senars, resulta $n^2 - n$ parell. Sumat amb 4, nombre parell, resulta que $n^2 - n + 4 = (n^2 - n) + 4$ és parell, com a suma de dos parells.

Mètode 2. Per casos segons la paritat de n, utilitzant la forma o expressió dels parells i senars.

- **Cas 1.** n és parell. Aleshores $n = 2k$, per a algun k enter adequat. Per tant, $n^2 - n + 4 = (2k)^2 - (2k) + 4 = 4k^2 - 2k + 4 = 2(2k^2 - k + 2) = 2k'$, que és parell, amb $k' = 2k^2 - k + 2 \in \mathbb{Z}$.
- **Cas 2.** n és senar. Aleshores existeix algun k enter tal que $n = 2k$. Per tant, $n^2 - n + 4 = (2k+1)^2 - (2k+1) + 4 = (4k^2 + 4k + 1) - (2k+1) + 4 = 2(2k^2 + k + 2) = 2k'$, que és parell, amb $k' = 2k^2 + k + 2 \in \mathbb{Z}$. ■

Exemple 2.12 Per a tot enter n, $3n^2 - n$ és parell.

Mètode 1. Per casos segons la paritat de n.

- **Cas 1.** n és parell. Aleshores $n^2 = n \cdot n$ és parell, per ser producte de dos parells. Per ser producte amb un factor parell, $3n^2 = 3 \cdot n^2$ és parell. Finalment, per ser diferència de dos parells, $3n^2 - n$ és parell.

  Alternativament, escrivim $3n^2 - n = n(3n - 1)$, que és parell perquè un dels factors, n, és parell.
- **Cas 2.** n és senar. Aleshores n^2 és senar, perquè és el producte de dos senars. Per ser producte de dos senars, $3n^2$ és senar (o directament per ser producte de tres senars). Finalment, per ser diferència de dos senars, $3n^2 - n$ és parell.
  Alternativament, escrivim $3n^2 - n = n(3n - 1)$, que és parell perquè un dels factors, $3n - 1$, és parell. En efecte, $3n$ és senar per ser producte de dos senars, d'on $3n - 1$ és parell, perquè és la diferència de dos senars.

Mètode 2. Per casos segons la paritat de n, amb substitució directa.

- **Cas 1.** n és parell. Aleshores $n = 2k$ per a un cert enter k. Substituïm a l'expressió $3n^2 - n = 3(2k)^2 - (2k) = 3(4k^2) - 2k = 2(6k^2 - k) = 2k'$, amb $k' = 6k^2 - k$ enter. Per tant, $3n^2 - n$ és parell.
- **Cas 2.** n és senar. Aleshores $n = 2k + 1$ per a un enter k convenient. Substituïm a l'expressió $3n^2 - n = 3(2k+1)^2 - (2k+1) = 3(4k^2 + 4k + 1) - (2k+1) = 12k^2 + 10k + 2 = 2(6k^2 + 5k + 1) = 2k'$, amb $k' = 6k^2 + 5k + 1$ enter. Per tant, $3n^2 - n$ és parell. ■

Exemple 2.13 El producte de dos nombres enters consecutius és parell. En efecte, exactament un dels dos és parell. El producte d'un nombre enter amb un nombre parell és parell.

El producte de tres nombres enters consecutius és múltiple de 6. En efecte, com a mínim un dels nombres és parell. Exactament un és múltiple de 3. El producte és múltiple de 6. ■

Exemple 1. Com veure que $2n+1$ no és múltiple de 2, amb $n \in \mathbb{Z}$? Fem una demostració per *reducció a l'absurd*.

Sigui $m = 2n+1$. Si m fos múltiple de 2, seria $m = 2k$ per a algun $k \in \mathbb{Z}$, d'on $2k = 2n+1$. D'aquí resulta $2k-2n = 1$, $2(k-n) = 1$ i, per tant, 1 és parell, divisible per dos, que és una conclusió absurda.

Argument alternatiu: si m fos parell, aleshores $1 = m-2n$ seria parell per ser diferència de parells. Per tant, 1 seria parell, absurd. ■

Exemple 2. Sigui n enter. Com veure que $2n-1$ no és múltiple de 2? L'argument pot ser similar a l'anterior, per reducció a l'absurd. Vegem una variant possible Suposem que és $2n-1$ múltiple de 2. Per a algun k enter és $2k = 2n-1$, d'on $2(k-n) = -1$, d'on $2(n-k) = 1$. Ara bé, $2|2(n-k)$ i, per tant, $2|1$, que és absurd. ■

Exemple 3. La suma de dos nombres enters consecutius no és múltiple de 2.

$$\begin{aligned} a+(a+1) &= 2a+1, \quad \text{senar} \\ (a-1)+a &= 2a-1, \quad \text{senar} \; ■ \end{aligned}$$

2.3.4. Problemes diversos (paritat i divisibilitat elemental)

PROBLEMA 2.6

Sigui n un nombre enter. Demostreu:

$$n \text{ senar} \Rightarrow n^2 \text{ senar}$$

Solució. (Vegem un estil expositiu diferent del problema següent, d'enunciat similar.)

Hipòtesi: $2 \nmid n$.

Tesi: $2 \nmid n^2$.

Mètode 1. Escrivint $n^2 = n \cdot n$, és senar per ser producte de senars.

Mètode 2. Escrivim la seqüència d'afirmacions següents:

P1: n senar.
P2: $\exists k \in \mathbb{Z}$ tal que $n = 2k+1$ (variant 1).
P3: $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(k^2+2k)+1$.
P4: $\exists k' \in \mathbb{Z}$ tal que $n^2 = 2k'+1$, amb $k' = 2k^2+2k$.
P5: n^2 és senar.

La marxa deductiva i demostrativa és:

$$P1 \Rightarrow P2 \Rightarrow P3 \Rightarrow P4 \Rightarrow P5. \text{ Consegüentment, } P1 \Rightarrow P5.$$

Idea de la demostració. La idea ha consistit a intentar expressar n^2 amb la forma típica d'un nombre senar.

Reescrivim alguns passos anteriors segons diverses variants:

P3′: $n^2 = 2(2k^2+2k)+1 = 2(2k^2+2k+1)-1$.
P4′: $\exists k'' \in \mathbb{Z}$ tal que $n^2 = 2k''-1 (k'' = 2k^2+2k+1)$.

O bé

P2′: $\exists \alpha \in \mathbb{Z}$ tal que $n = 2\alpha - 1$ (variant 2).
P3″: $n^2 = (2\alpha-1)^2 = 4\alpha^2 - 4\alpha + 1 = 2(\alpha^2 - 2\alpha) + 1$.

o bé (una altra variant)

$$n^2 = 4\alpha^2 - 4\alpha + 1 = 2(\alpha^2 - 2\alpha + 1) - 1.$$

PROBLEMA 2.7

Suposem que n és un nombre enter. Demostreu:
Si n és senar, aleshores n^3 és senar.

Solució

Mètode 1. Escrivim $n^3 = n \cdot n \cdot n$. Com a producte d'un nombre finit de senars, és senar, en aplicació d'un resultat al respecte (problemes anteriors).

Mètode 2. Sense utilitzar el resultat "producte de senars és senar". Essent n senar, s'-expressa com $n = 2k+1$, per a un cert enter k. Vegem que n^3 es pot expressar com a senar:

$$n^3 = (2k+1)^3 = (2k)^3 + 3(2k)^2 + 3(2k) + 1 = 2(4k^3+6k^2+3k)+1 = 2k'+1, \text{ senar,}$$

amb $k' = 4k^3 + 6k^2 + 3k$, enter.

Variant argumental: Utilitzant l'altra possible expressió $n = 2k' - 1$, per a algun enter k'.

PROBLEMA 2.9

Demostreu que els nombres senars es poden expressar de la forma $2k+3$ per a un enter k convenient.

De fet, és na nova possible expressió per als senars.

Solució. Observem que $2k$ és parell. Com a suma d'un parell i un senar, $2k+3$ és senar.

Vegem que tot senar es pot expressar d'aquesta forma. Si a és un nombre senar, existeix un enter q tal que $a = 2q+1$. Imposem $2q+1 = a = 2k+3$ per tal d'obtenir k. Resulta $2q - 2k = 2$, d'on $q - k = 1$. Així, només cal prendre $k = q - 1$.

Comprovació: $a = 2q+1 = 2(k+1)+1 = 2k+3$.

PROBLEMA 2.9

Sigui n un nombre enter. Comproveu que

a) $5|(5n+2)^2+1$

b) $5|(5n+3)^2+1$

c) $7|(7n+2)^2+(7n+2)+1$

d) $3|(3n+1)^2+(3n+1)+1$

Solució. Simplement desenvolupem rutinàriament les expressions i comprovem el que es demana.

a) $5|(5n+2)^2+1$

És $(5n+2)^2+1 = (25n^2+20n+4)+1 = 25n^2+20n+5 = 5(5n^2+4n+1) = 5k$, múltiple de 5, amb $k = 5n^2+4n+1 \in \mathbb{Z}$.

b) $5|(5n+3)^2+1$

És $(5n+3)^2+1 = (25n^2+30n+9)+1 = 25n^2+30n+10 = 5(5n^2+6n+2) = 5k$, múltiple de 5, amb $k = 5n^2+6n+2 \in \mathbb{Z}$.

c) $7|(7n+2)^2+(7n+2)+1$

És $(7n+2)^2+(7n+2)+1 = (49n^2+28n+4)+(7n+2)+1 = 49n^2+35n+7 = 7(7n^2+5n+1)$, múltiple de 7.

d) $3|(3n+1)^2+(3n+1)+1$

És $(3n+1)^2+(3n+1)+1 = (9n^2+6n+1)+(3n+1)+1 = 9n^2+9n+3 = 3(3n^2+3n+1)$, múltiple de 3.

PROBLEMA 2.10

Proveu que, per a n enter, $2 \nmid n \Rightarrow 8|n^2-1$.

Solució. *Què hem de veure?* Que existeix un enter s tal que $n^2-1=8s$.

Essent n senar, per a algun enter k és $n=2k+1$.

Aleshores $n^2-1 = (2k+1)^2-1 = (4k^2+4k+1)-1 = 4k^2+4k = 4(k^2+k)$.

Necessitem un factor addicional 2 per tal de poder escriure $n^2-1=8s$, per a un cert enter s. Analitzant k^2+k, s'observa que $k^2+k=k(k+1)$, producte de dos enters consecutius. Exactament un d'ells és parell, és a dir, múltiple de 2 (es podria provar per casos segons la paritat de k; en tot cas, el resultat s'ha comentat amb anterioritat) i, per tant, $k(k+1) = 2s$, amb s enter.

Així, finalment, $n^2-1 = 4(k^2+k) = 4(k(k+1)) = 4\cdot 2s = 8s$.

Variant argumental 2. Una altra variant argumental consistiria a escriure $n = 2q-1$ per a un enter q convenient. Aleshores $n^2-1 = (2q-1)^2-1 = (4q^2-4q+1)-1 = 4q^2-4q = 4(q^2-q) = 4q(q-1)$. Ara bé, $q(q-1)$ és un producte de dos enters consecutius; donat que un d'ells és parell, múltiple de 2, el producte és múltiple de 2 i així $q(q-1) = 2v$, per a v enter adequat. Finalment, $n^2-1 = 4q(q-1) = 4\cdot 2v = 8v$.

Variant argumental 3. Escrivim, com a diferència de quadrats, $n^2-1 = (n-1)(n+1)$.

Si dos enters són consecutius, un d'ells és parell. La parella $n-1, n$ és d'enters consecutius; atès que per hipòtesi n és senar, necessàriament $n-1$ és parell. Anàlogament, la parella $n, n+1$ és d'enters consecutius; atès que, per hipòtesi, n és senar, necessàriament $n+1$ és parell. De fet, només utilitzarem que $n-1$ és parell.

Així, $n-1, n+1$ són parells, i aportaran factors 2 al producte. Concretament, és $n-1 = 2k$, $n+1 = (n-1)+2 = 2k+2$, per a algun enter k. D'aquesta manera resulta $n^2-1 = (n-1)(n+1) = 2k(2k+2) = 4k(k+1)$. Ara bé, $k(k+1)$ és parell, perquè és producte de dos enters consecutius i, per tant, $k(k+1) = 2w$, w enter convenient. Així, $n^2-1 = 4k(k+1) = 4\cdot 2w = 8w$.

Observació. El fet més remarcable, segurament utilitzable en altres demostracions, és que, d'entre dos nombres enters consecutius, exactament un és parell (i l'altre senar). Pot considerar-se obvi, però també demostrable per molts mètodes: per exemple, per casos segons paritat de n. S'ha estudiat amb anterioritat.

PROBLEMA 2.11

Sigui n un enter. Proveu que, si n no és múltiple de 3 *i és senar, aleshores* $24 | n^2-1$.

Solució. Formalitzadament,

$$(3 \nmid n \wedge 2 \nmid n) \to 24 | n^2-1.$$

Què hem de veure? Que per a n satisfent la hipòtesi, podem expressar $n^2-1 = 24d$, per a algun enter d.

És $n^2-1 = (n-1)(n+1)$ ("diferència de quadrats $n^2-1 = n^2-1^2$ és suma per diferència").

Fem servir un resultat intuïtiu, però, d'altra banda, demostrat en altres exercicis, que cada tres nombres consecutius n'hi ha algun (de fet, exactament un) que és múltiple de 3 (de fet, això es pot demostrar per casos segons el residu de la divisió entera per 3: $n = 3q$, $n = 3q+1$, $n = 3q+2$). Considerant $n-1, n, n+1$, un dels nombres és múltiple de 3; atès que per hipòtesi n no és multiple de 3, necessàriament un dels altres dos ho és i, per tant, el producte $(n-1)(n+1)$ és múltiple de 3. És a dir, $3 | n^2-1$ (si n és no múltiple de 3).

Falta veure que és múltiple de 8.

Si n és senar, és $n = 2k+1$ per a algun k enter. Per tant, $n-1 = (2k+1)-1 = 2k$, $n+1 = (2k+1)+1 = 2k+2 = 2(k+1)$ i, en conseqüència, $n^2-1 = (n-1)(n+1) = 2k\cdot 2(k+1) = 4k(k+1)$.

Ens falta obtenir un factor 2 addicional. Fem servir que $k, k+1$ són dos enters consecutius: exactament un d'ells és parell, i, per tant, també el producte és parell (observeu que es pot demostrar per casos segons la paritat de k, tot i que està provat en altres llocs). Així, $k(k+1) = 2t$, amb t enter convenient.

Finalment, $n^2 - 1 = (n-1)(n+1) = 4k(k+1) = 4 \cdot 2t = 8t$. Per tant, $8|n^2 - 1$ (si n és senar).

Com a conclusió, en la hipòtesi del problema, $(3|n^2 - 1) \wedge (8|n^2 - 1)$ i, per tant $24 = 3 \cdot 8|n^2 - 1$.

Variant argumental sobre aquest últim pas. Fer servir l'expressió alternativa d'un nombre senar com $n = 2w - 1$, per a algun w enter.

Variant argumental per a provar $3|n^2 - 1$. Sobre la demostració que $n^2 - 1$ és múltiple de 3, podem argumentar de la forma següent, per casos segons el residu de la divisió entera de n per 3, que és $n = 3q + r$, amb $0 \leq r \leq 2$. Per la hipòtesi $3 \nmid n$, és $r \neq 0$ i, per tant, en resulten dos casos ($r = 1$ o $r = 2$).

- **Cas 1.** ($r = 1$). Aleshores $n = 3q + 1$ i, per tant, $n^2 - 1 = (3q+1)^2 - 1 = (9q^2 + 6q + 1) - 1 = 9q^2 + 6q = 3(3q^2 + 2q)$, múltiple de 3.
- **Cas 2.** ($r = 2$). Aleshores $n = 3q + 2$ i, per tant, $n^2 - 1 = (3q+2)^2 - 1 = (9q^2 + 12q + 4) - 1 = 9q^2 + 12q - 3 = 3(3q^2 + 6q - 1)$, múltiple de 3.

PROBLEMA 2.12

Sigui n un nombre natural. Demostreu que $8|9^n - 1$.
Inventeu enunciats de tipus similar.

Solució. Aquest problema es pot resoldre per diversos mètodes. Vegem aquí com podem utilitzar la fórmula del binomi de Newton.

Per a això, escrivim $9 = 8 + 1$. I així tindrem:

$$9^n - 1 = (8+1)^n - 1 = \left(\sum_{i=0}^{n} \binom{n}{i} 8^i \cdot 1^{n-i} \right) - 1 = \left(\sum_{i=0}^{n} \binom{n}{i} 8^i \right) - 1 =$$

$$= \left(1 + \sum_{i=1}^{n} \binom{n}{i} 8^i \right) - 1 = \sum_{i=1}^{n} \binom{n}{i} 8^i = 8 \left(\sum_{i=1}^{n} \binom{n}{i} 8^{i-1} \right) = 8k,$$

amb $k = \displaystyle\sum_{i=1}^{n} \binom{n}{i} 8^{i-1} \in \mathbb{Z}$.

Per tant, existeix algun k enter tal que $9^n - 1 = 8k$, és a dir, que $8|9^n - 1$.

D'acord amb el mètode de resolució, observem que es pot afirmar el mateix per a $8q+1$, per a q enter, és a dir, $8|(8q+1)^n-1$, ja que

$$\begin{aligned}(8q+1)^n-1 &= \left(\sum_{i=0}^{n}\binom{n}{i}(8q)^i\cdot 1^{n-i}\right)-1=\left(\sum_{i=0}^{n}\binom{n}{i}8^iq^i\right)-1=\\ &=\left(1+\sum_{i=1}^{n}\binom{n}{i}8^iq^i\right)-1=\sum_{i=1}^{n}\binom{n}{i}8^iq^i=8\left(\sum_{i=1}^{n}\binom{n}{i}8^{i-1}q^i\right)=8k,\end{aligned}$$

amb $k=\sum_{i=1}^{n}\binom{n}{i}8^{i-1}q^i\in\mathbb{Z}$.

I així, podrem afirmar, entre molts altres:

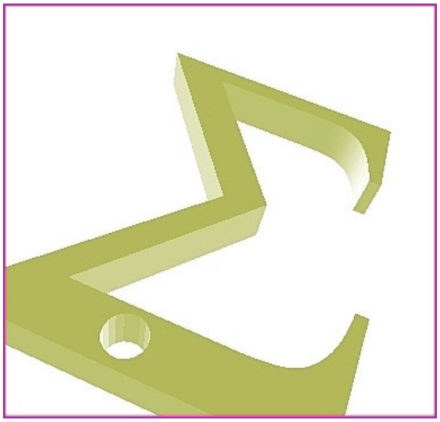
$$\begin{array}{ll} 8|9^n-1 & (q=1)\\ 8|17^n-1 & (q=2)\\ 8|25^n-1 & (q=3)\\ 8|(-7)^n-1 & (q=-1)\end{array}$$

Es pot generalitzar? Analitzant l'anterior, podem proveir un "generador d'enunciats": si n i m són nombres naturals, és $m|(mq+1)^n-1$, per a q nombre natural. En efecte, en desenvolupar pel binomi de Newton, sempre surt $(mq+1)^n-1$ múltiple de m. Així, per exemple:

$$\begin{array}{ll} 5|11^n-1 & (q=2);\\ 6|13^n-1 & (q=2).\end{array}$$

→ 3

Sumatoris



Saber treballar amb sumatoris i obtenir fórmules de sumació és absolutament imprescindible per a l'anàlisi d'algorismes; en aquest camp, estem interessats en la complexitat, en l'eficiència en cost computacional (temps d'execució) i, si escau, en espai d'emmagatzemament d'estructures de dades auxiliars, creades per l'execució d'algorismes. Moltes coses que aquí s'exposen calen també per a capítols posteriors i, en particular, per al capítol d'inducció (7).

Amb aquest estudi es volen assolir alguns objectius:

a) Eliminar l'ambigüitat dels punts suspensius a les fórmules amb sumes.

b) Escriure expressions compactes. Per exemple, la fórmula vectorial

$$\vec{w} = x_1\vec{e}_1 + \cdots + x_1\vec{e}_n \text{ es compacta a } \vec{w} = \sum_{k=1}^{n} x_k\vec{e}_k.$$

c) De vegades, convé de disposar d'una fórmula tancada per a una suma, expressada o no com a sumatori, és a dir, una fórmula com $\sum_{j=1}^{n} a_j = f(n)$, per a una funció f convenient. Per exemple, $\sum_{j=1}^{n} k = \dfrac{n(n+1)}{2}$, on ara $f(n) = \dfrac{n(n+1)}{2}$.

   És convenient tenir disponibles fórmules de sumació com l'anterior, sobretot per a anàlisi d'algorismes, en estimacions de costos computacionals; així podrem contestar a preguntes del tipus: de quin ordre és (fita superior) un algorisme el cost computacional del qual és $1+2+\cdots+n$ per a una entrada de mida n? Ja podem contestar, sabent que

$$\sum_{j=1}^{n} k = \frac{n(n+1)}{2} = \frac{1}{2}(n^2+n) = \frac{1}{2}n^2 + \frac{1}{2}n,$$

que és d'ordre quadràtic. Un dels objectius és obtenir aquestes fórmules de sumació, sobretot per a sumes de nombres naturals, com per exemple suma de quadrats, de cubs, de parells o de senars.

3.1. La notació de sumatori

El símbol sumatori. El símbol sumatori $\sum$ permet expressar sumes en forma compacta.

Exemples 3.1

Exemple 1. Per exemple, podem escriure $1+2+3+4+5$ com $\sum_{k=1}^{5} k$. Observeu que tenim un índex de sumació (o també un índex d'iteració o de control d'iteracions), nombre natural, que varia entre uns límits inferior i superior, amb increments d'una unitat: $1 \leq k \leq 5$, en aquest exemple. ■

Exemple 2. $\sum_{k=1}^{5} a_k = a_1+a_2+a_3+a_4+a_5$. ■

Punts suspensius. A l'últim exemple, podríem escriure $a_1+a_2+a_3+a_4+a_5 = a_1+\cdots+a_5$. Quan tenim sumes de n sumands, amb n nombre natural, $n \geq 1$, per exemple $a_1,\cdots,a_n$, podem escriure la suma com $a_1+a_2+\cdots+a_n$, amb la notació de punts suspensius, per donar a entendre que sumem segons l'ordre creixent del subíndex, des d'1 fins a n, d'un en un o tots els intermedis, de manera que l'índex i pren tots els valors del conjunt $\{m | m \in \mathbb{N} \wedge 1 \leq m \leq n\}$, creixentment. Això es pot expressar de més d'una manera, com per exemple escrivint el terme general a_k o a_i:

$$a_1+\cdots+a_n$$
$$a_1+a_2+\cdots+a_{n-2}+a_{n-1}+a_n$$
$$a_1+\cdots+a_i+\cdots+a_n$$

El problema dels punts suspensius és que no queda explícit què hi ha d'haver en comptes dels punts.

Índex de sumació o d'iteració. L'índex d'iteració pot ser substituït per qualsevol altre: $\sum_{j=1}^{5} j$ o $\sum_{i=1}^{5} i$. El subíndex és una "variable muda", intercanviable amb d'altres. Així, l'última suma $a_1+\cdots+a_i+\cdots+a_n$ es pot escriure també com:

$$a_1+\cdots+a_k+\cdots+a_n$$
$$a_1+\cdots+a_j+\cdots+a_n$$

La notació per a l'índex de variació és irrellevant; és substituïble per altres, com k, j, t, r, s, d, per exemple, i així la suma en forma de sumatori es pot reescriure com

$$\sum_{i=1}^{n} a_i \qquad \sum_{j=1}^{n} a_j \qquad \sum_{k=1}^{n} a_k \qquad \sum_{j=1}^{n} j \qquad \sum_{i=1}^{n} i.$$

La notació de sumatori. Ens pot interessar prescindir de la notació amb punts suspensius i adoptar una notació més compacta per a la fórmula sumatòria. Per a això, podem utilitzar el símbol "sumatori", és a dir, $\sum$, amb la sintaxi corresponent, de manera que la fórmula anterior seria, en termes de sumatori:

$$\textstyle\sum_{i=1}^{n} a_i, \text{ o bé } \displaystyle\sum_{i=1}^{n} a_i$$

on i és l'índex d'iteració, que varia en sentit creixent, d'un a un, des del valor inferior $i = 0$ al superior $i = n$. S'entén que pren tots els valors de $0, \cdots, n$, és a dir, de $\{x \in \mathbb{N} | 0 \leq x \leq n\}$. El *terme general* és a_i.

Per exemple, per a

$$1 + 2 + 3 + \cdots + n$$

el terme general és k ($a_k = k$), de manera que també podem escriure

$$1 + 2 + 3 + \cdots + n = \sum_{k=1}^{n} k.$$

Només amb el *terme general* podem expressar de manera precisa la suma, ja que la notació de "punts suspensius" realment no diu què hi ha en comptes dels punts!

Extrems o límits de variació de l'índex. Els valors inferior i superior dels índexs poden ser diferents, amb el mateix terme general (escrivint així una altra suma):

$$\begin{aligned}
\sum_{k=3}^{n-1} k &= 3 + 4 + \cdots + (n-2) + (n-1), \ n \geq 4 \ (n-1 \geq 3) \\
\sum_{k=4}^{n^2+1} k &= 4 + 5 + \cdots + (n-2) + (n-1) + n + \cdots + \\
&\quad + \ (n^2 - 1) + n^2 + (n^2 + 1), \ n \geq 2 \ (n \geq 2 \Rightarrow n^2 + 1 \geq 5)
\end{aligned}$$

Reindexació. O també podem considerar un nou índex $j = k + 1$ per a obtenir la mateixa suma $\displaystyle\sum_{k=1}^{n} k$, però aleshores haurà de ser amb el sumatori $\displaystyle\sum_{j=2}^{n+1} (j-1)$.

Fórmules en els subíndexs. Permeten triar selectivament només determinades posicions per a efectuar sumes o altres operacions.

Exemples 3.2

Exemple 1. Com escriure la suma dels termes de posició parella a la llista $a_1, a_2, \cdots$: $\sum_{i\geq 1} a_{2i}$; els de les posicions senars: $\sum_{i\geq 1} a_{2i+1}$; cada 3: $\sum_{i\geq 1} a_{3i}$; els de les posicions que són potències de 2: $\sum_{i\geq 1} a_{2^i}$; els de les posicions potències de 7: $\sum_{i\geq 1} a_{7^i}$. ■

Exemple 2. Suma de les potències de 3 d'exponent parell: $\sum_{k\geq 1} 3^{2k}$. ■

Exemple 3. Suma de les potències de 5 d'exponent senar: $\sum_{k\geq 1} 5^{2k-1}$ o $\sum_{k\geq 0} 5^{2k+1}$. ■

Exemple 4. Suma de les potències de 3 d'exponent potència de 2: $\sum_{k\geq 1} 3^{2^k}$. ■

Exemple 5. Suma de les potències de 3, cada 5: $\sum_{k\geq 1} 3^{5k}$. ■

Quants sumands té un sumatori? Aquesta és una qüestió que acostuma a plantejar més d'una dificultat. En general:

$$\sum_{i=r}^{s} a_i = a_r + a_{r+1} + \cdots + a_{s-1} + a_s = a_r + a_{r+1} + \cdots + a_{s-1} + a_{r+(s-r)},$$

amb $0 \leq r \leq s$, té $(s-r)+1$ sumands, ja que hi hem de comptar el sumand a_r.

Així, com a exemples, $\sum_{i=r}^{s} 1 = (s-r)+1$; $\sum_{i=r}^{s} 6 = 6((s-r)+1)$.

Vegem-ne alguns exemples addicionals.

Exemples 3.3

Exemple 1. $\sum_{k=1}^{n} 1 = 1+1+\overset{n}{\overbrace{\cdots}}+1 = n$ (quants sumands 1?). Nombre de sumands: n. ■

Exemple 2. $\sum_{k=1}^{n} 2 = 2+2+\overset{n}{\overbrace{\cdots}}+2 = 2n$ (quants sumands 2?). Nombre de sumands: n. ■

Exemple 3. $\sum_{k=5}^{n-1} 1 = 1+1+\overset{?}{\overbrace{\cdots}}+1 = 1+1+\overset{(n-1)-5+1}{\overbrace{\cdots}}+1 = (n-1)-5+1$ (des de 6 fins a $n-1$ són $(n-1)-5$; cal sumar el sumand corresponent a $i=5$). ■

Exemple 4. $\sum_{k=5}^{n-1} 3 = 3+3+\overset{?}{\overbrace{\cdots}}+3 = 3+3+\overset{(n-1)-5+1}{\overbrace{\cdots}}+3 = 3((n-1)-5+1)$ (des de 6 fins a $n-1$ són $(n-1)-5$. ■

Exemple 5. $\sum_{k=j}^{n} 1 = (n-j+1)$, ($n, j$ fixos, amb $n \geq j$). ■

Exemple 6. $\sum_{i=r}^{n^2+1} a_i = a_r + a_{r+1} + \cdots + a_{n^2} + a_{n^2+1}$ conté $((n^2+1)-r)+1$ sumands; n, r són fixos, $n^2+1 \geq r$. ■

Exemple 3.4 Considerem $\sum_{k=3}^{n+4}(2k-1)$ $(n \geq 0)$. Quins són el terme general, la variació de l'índex i el nombre de sumands?

El terme general és $2k-1$ i l'índex k varia de 3 a $n+4$. El nombre de sumands és $(n+4)-3+1 = n+2$. ■

Exemple 3.5 Podem expressar el sumatori anterior $\sum_{k=3}^{n+4}(2k-1)$ com a suma de terme general $2k+1$? Efectivament, introduïm el nou índex t tal que $2k-1 = 2t+1$. Operant, resulta $2k = 2t+2$, d'on $k = t+2$, o $t = k-2$. De $3 \leq k \leq n+4$ deduïm $3-2 \leq k-2 \leq (n+4)-2$, d'on $1 \leq t \leq n+2$, i així el sumatori anterior serà $\sum_{k=3}^{n+4}(2k-1) = \sum_{t=1}^{n+2}(2t+1)$.
■

Diversos exemples d'escriptura de sumatoris. Donem una frase descriptiva de la suma i demanem que s'expressi com a suma amb punts suspensius i com a sumatori (notació).

En un sumatori, hem de considerar l'índex de variació (iterador, d'iteració), els valors mínim i màxim de l'índex i el terme general.

Exemples 3.6 **Exemples d'escriptura de sumatoris**

Exemple 1. La suma dels quadrats dels n primers nombres naturals:

$$1^2+2^2+3^2+\cdots+k^2+\cdots+(n-1)^2+n^2 = \sum_{k=1}^{n} k^2$$

Terme general: k^2.

Índex de control de sumació (d'iteracions): k. Valor inicial (mínim): 1, valor final (màxim): n.

Nombre de sumands: n. ■

Exemple 2. La suma dels cubs dels n primers nombres naturals:

$$1^3+2^3+3^3+\cdots+k^3+\cdots+(n-1)^3+n^3=\sum_{k=1}^{n}k^3$$

Terme general: k^3.

Nombre de sumands: n. ■

Exemple 3. La suma dels n primers nombres naturals parells. Recordem que els nombres naturals parells són els de la forma $2k$, amb k nombre natural. Per tant:

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

Terme general: $2k$.

Nombre de sumands: n. ■

Exemple 4. La suma dels $n+1$ primers nombres naturals senars. Recordem que els nombres naturals senars són els de la forma $2k+1$, amb k nombre natural. Per tant:

$$1+3+5+\cdots+(2k+1)+\cdots+(2(n-1)+1)+(2n+1)=\sum_{k=0}^{n}(2k+1)$$

Terme general: $2k+1$.

Nombre de sumands: $n+1$. ■

Exemple 5. La suma dels n primers nombres naturals senars.

$$1+3+5+\cdots+(2k+1)+\cdots+(2(n-1)+1)=$$
$$1+3+5+\cdots+(2k+1)+\cdots+(2n-1)=\sum_{k=0}^{n-1}(2k+1)$$

Terme general: $2k+1$.

Nombre de sumands: n. ■

Exemple 6. La suma dels n primers nombres naturals senars. Recordem que els nombres naturals senars també són els de la forma $2k-1$, amb k nombre natural. Per tant:

$$1+3+5+\cdots+(2k-1)+\cdots+(2n-1)=\sum_{k=1}^{n}(2k-1)$$

Terme general: $2k-1$.

Nombre de sumands: n. ■

Exemple 7. La suma dels n primers naturals múltiples de 3. Els múltiples de 3 són els de la forma $3k$, amb k natural:

$$3+6+\cdots+3k+\cdots+3(n-1)+(3n)=\sum_{k=1}^{n}3k\ (n\geq 1)$$

Terme general: $3k$.

Nombre de sumands: n. ■

Exemple 8. Suma de les $n+1$ primeres potències de 3 (s'inclou $1=3^0$):

$$1+3+3^2+3^3+\cdots+3^k+\cdots+3^n=3^0+3^1+3^2+3^3+\cdots+3^k+\cdots+3^n=\sum_{k=0}^{n}3^k.$$

Terme general: 3^k.

Nombre de sumands: $n+1$. ■

Exemples 3.7 *Sumes alternades*:

Com obtenir alternança de signes: amb $(-1)^k=\begin{cases}1 & \text{si } k \text{ és parell}\\ -1 & \text{si } k \text{ és senar}\end{cases}$

Exemple 1. $1-1+1-1+1-1+\cdots+(-1)^k+\cdots+(-1)^n=\sum_{k=0}^{n}(-1)^k.$

Terme general: $(-1)^k$.

Nombre de sumands: $n+1$. ■

Exemple 2.

$$1-1+1-1+1-1+1-1+1-1+1-1+1-1+1-1=\sum_{k=0}^{15}(-1)^k.$$

$$=(-1)^0+(-1)^1+(-1)^2+\cdots+(-1)^{15}. \ ■$$

Exemple 3. Com obtenir $1-2+3-4+5-6+\cdots+(-1)^{n-1}n$?

Amb $\sum_{k=1}^{n}(-1)^{k-1}k$ ■

Exemples 3.8 Per a expressar límits del subíndex de sumatori pot ser convenient utilitzar la funció part entera (inferior):

Funció part entera i aplicacions. D'especial interès en algorísmica és la funció part entera (inferior) (*floor function*) i la part entera superior (*ceil function*).

La funció part entera (o, de manera més completa, funció part entera inferior) es defineix, en el conjunt dels nombres reals $\mathbb{R}$, com:

$$\lfloor x \rfloor = \text{màx}\{n \in \mathbb{Z} | n \leq x\}$$

És el nombre enter més gran que és menor o igual que x.

Vegem alguns exemples d'expressió dels límits amb la funció part entera.

Exemple 1. Donada la suma $a_1 + a_2 + \cdots + a_n$, escriviu la suma corresponent als sumands d'índex parell. Els sumands són de la forma a_{2i}, amb $i \geq 1$. Quin és el límit superior per a i? S'ha de complir $2i \leq n$, d'on $i \leq \frac{n}{2}$. Per tant, $i \leq \lfloor \frac{n}{2} \rfloor$. Així, $1 \leq i \leq \lfloor \dfrac{n}{2} \rfloor$, i finalment la suma s'expressa $\displaystyle\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} a_{2i}$.

Nombre de sumands: $(\lfloor \dfrac{n}{2} \rfloor - 1) + 1$. ■

Exemple 2. Suma dels nombres naturals senars menors o iguals que n. La suma és de la forma $\displaystyle\sum_{k\geq 0}(2k+1)$. Cal precisar el límit superior per a k, que és enter: ha de ser $2k+1 \leq n$, d'on $2k \leq n-1$, d'on $k \leq \dfrac{n-1}{2}$, d'on $k \leq \lfloor \dfrac{n-1}{2} \rfloor$. Així, $0 \leq k \leq \lfloor \dfrac{n-1}{2} \rfloor$. Finalment, $\displaystyle\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor}(2k+1)$.

Nombre de sumands: $(\lfloor \dfrac{n-1}{2} \rfloor - 0) + 1$. ■

Sumatoris i successions recurrents. Vegem-ne un exemple. Considerem l'exemple $1 + 2 + \cdots + n$. Podem formular la successió recurrent associada a la suma anterior definint $s_n = 1 + 2 + \cdots + n$. Aleshores, tenim el terme inicial i la relació de recurrència:

$$\begin{aligned} s_1 &= 1 && \text{(terme inicial o condició inicial)} \\ s_n &= s_{n-1} + n, && \text{per a } n \geq 2 \text{ (relació de recurrència)} \end{aligned}$$

A partir de mètodes per a obtenir el terme general d'una successió recurrent es poden obtenir sumes en forma tancada (cosa que depassa els objectius d'aquesta publicació).

Variació de l'índex: generalització. L'índex de variació també pot ser negatiu:

$$\sum_{j=-3}^{n} 4j \text{ (per a } n \geq -3).$$

Correspondria a $4(-3) + 4(-2) + 4(-1) + 4(0) + 4 \cdot 1 + \cdots + 4j + \cdots + 4n$.

Nombre de sumands: $n - (-3) + 1$.

De vegades, convé poder indexar sobre un conjunt i escriure

$$\sum_{i \in I} a_i,$$

on I és un conjunt d'índexs, com per exemple:

$$\begin{aligned} I &= \{1,2,3,4,\cdots,56\} = \{j \in \mathbb{Z} | 1 \leq j \leq 56\}, \\ I &= \{1,2,3,4,\cdots,n\} = \{j \in \mathbb{Z} | 1 \leq j \leq n\}, \\ I &= \{-1,1,3,6,7\}. \end{aligned}$$

Un altre exemple, amb una altra variant: "Un nombre natural m és "perfecte" si és igual a la suma de tots els seus divisors positius diferents d'ell mateix". Aquesta definició s'expressa mitjançant un sumatori: si

$$I_m = \{d | d \in \mathbb{N}, d \geq 1, d | n, d \neq m\}, \text{ aleshores } m = \sum_{x \in I_m} x.$$

3.2. Propietats bàsiques

Les propietats bàsiques són les que fan referència a la suma (i diferència) i al producte per algun nombre real.

Suma de sumatoris. "Suma de sumatoris és el sumatori de la suma" (vegem-ho per a dos):

Teorema 3.1 *Suposem que $a_1, \cdots, a_n$, $b_1, \cdots, b_n$ són nombres reals. Es compleix:*

$$\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \tag{3.1}$$

Demostració. Despleguem els sumatoris i hi apliquem les propietats de commutativitat i associativitat de la suma de nombres reals:

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = (a_1 + \cdots + a_n) + (b_1 + \cdots + b_n) = (a_1 + b_1) + \cdots (a_n + b_n) = \sum_{i=1}^{n} (a_i + b_i).$$

Es poden variar els valors inferior i superior dels índexs de variació.

Producte per escalars. Si multipliquem per un escalar, "l'escalar surt fora del sumatori":

Teorema 3.2 *Suposem que $a_1, \cdots, a_n$, $b_1, \cdots, b_n$, c són nombres reals. Es compleix*

$$\sum_{i=1}^{n} c a_i = c \sum_{i=1}^{n} a_i \tag{3.2}$$

Demostració. Despleguem el sumatori i hi apliquem la propietat distributiva del producte respecte de la suma (per a "treure factor comú"):

$$\sum_{i=1}^{n} ca_i = (ca_1 + \cdots + ca_n) = c(a_1 + \cdots + a_n) = \sum_{i=1}^{n} ca_i.$$

Podem variar, respecte de l'enunciat estàndard, els valors inferior i superior dels índexs de variació.

Exemples 3.9 Aquestes propietats permeten escriure, per exemple:

Exemple 1. $\sum_{k=1}^{n}(2k) = 2\sum_{k=1}^{n} k$. Si ara disposéssim d'una fórmula per a la suma $\sum_{k=1}^{n} k$ es podria substituir i hauríem obtingut una fórmula per a la suma dels n primers naturals parells. Avançant idees, tal com s'exposa més endavant en el capítol, és $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ i, substituint, $\sum_{k=1}^{n}(2k) = 2\sum_{k=1}^{n} k = 2\frac{n(n+1)}{2} = n(n+1)$. ■

Exemple 2. $\sum_{k=1}^{n}(2k+1) = \sum_{k=1}^{n}(2k) + \sum_{k=1}^{n} 1 = 2(\sum_{k=1}^{n} k) + n = 2(\frac{n(n+1)}{2} + n) = n(n+2)$.
■

Exemple 3. $\sum_{k=1}^{n}(2k+1)^2 = \sum_{k=1}^{n}(4k^2+4k+1) = \sum_{k=1}^{n} 4k^2 + \sum_{k=1}^{n} 4k + \sum_{k=1}^{n} 1 = 4\sum_{k=1}^{n} k^2 + 4\sum_{k=1}^{n} k + n$. ■

i, d'aquesta manera, sumar expressions a partir de sumes d'expressions més bàsiques, de suma coneguda.

Generalització a més sumatoris. Per exemple, amb tres sumatoris. Es fan servir el resultat bàsic i la propietat d'associativitat:

$$\sum_{i=1}^{n}(a_i + b_i + c_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i + \sum_{i=1}^{n} c_i$$

Atenció a l'ús del parèntesi: si volem escriure $\sum_{i=1}^{n}(a_i + b_i)$, seria incorrecte escriure $\sum_{i=1}^{n} a_i + b_i$, ja que s'interpretaria com $(\sum_{i=1}^{n} a_i) + b_i$.

Teorema 3.3 *(Generalitzacions). Es pot generalitzar, amb $\alpha, \beta \in \mathbb{R}$:*

$$\sum_{k=0}^{n}(\alpha a_k + \beta b_k) = \alpha \sum_{k=0}^{n} a_k + \beta \sum_{k=0}^{n} b_k$$

Com a cas particular ($\alpha = 1$, $\beta = -1$),

$$\sum_{k=0}^{n}(a_k - b_k) = \sum_{k=0}^{n} a_k - \sum_{k=0}^{n} b_k \text{ (diferència de sumatoris)}$$

I també, per a un nombre finit de sumatoris,

$$\sum_{k=0}^{n}(a_k + \cdots + t_k) = \sum_{k=0}^{n} a_k + \cdots + \sum_{k=0}^{n} t_k$$
$$\sum_{k=0}^{n} c(a_k + \cdots + t_k) = c\sum_{k=0}^{n} a_k + \cdots + c\sum_{k=0}^{n} t_k$$

Observació. El cas particular de diferència de sumatoris també admet demostració directa:

$$\begin{aligned}\sum_{k=0}^{n}(a_k - b_k) &= (a_1 - b_1) + \cdots + (a_n - b_n) = (a_1 + \cdots + a_n) - (b_1 + \cdots + b_n) = \\ &= \sum_{k=0}^{n} a_k - \sum_{k=0}^{n} b_k,\end{aligned}$$

aplicant les propietats commutativa i associativa de la suma en els nombres reals.

3.3. Sumes bàsiques/importants: sumes d'enters

És convenient disposar d'una llista de sumes que podem considerar bàsiques, per tal d'utilitzar-les directament o per a derivar-ne d'altres, depenent del problema.

Vegem uns mètodes específics per obtenir una fórmula tancada per a la suma dels n primers nombres naturals positius i de les seves potències (quadrat i cub, per exemple).

3.3.1. Sumes d'enters

Un dels resultats que es presenta sovint en anàlisi de costos computacionals d'algorismes és el de la suma dels n primers nombres naturals, és a dir, $1+2+\cdots+k+\cdots+n$. El càlcul d'aquesta suma exigiria la iteració:

$$\begin{array}{l} 1 \\ 1+2 \\ 1+2+3 \\ \vdots \end{array}$$

El problema, a part del càlcul, és que, amb l'expressió $S = 1+2+\cdots+k+\cdots n$, no sabem "com és de gran S", és a dir, quin és el seu ordre de magnitud (lineal?, quadràtic?, logarítmic?). Si la fórmula correspon al cost computacional d'un algorisme, no en podem saber l'eficiència ni si, per tant, és un algorisme interessant o bé és preferible descartar-lo i utilitzar-ne un altre.

Suma dels *n* primers naturals. Busquem una fórmula tancada amb què puguem substituir.

Teorema 3.4 *Sigui n un nombre natural, $n \geq 1$. Aleshores:*

$$1+2+3+\cdots+n = \frac{n(n+1)}{2} \tag{3.3}$$

Formulat com a sumatori, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Demostració. Vegem-ne diverses demostracions.

Mètode 1. Sigui $S = 1+2+3+\cdots+(n-2)+(n-1)+n$. Reescrivim la mateixa suma, però en ordre invers, és a dir, $S = n+(n-1)+(n-2)+\cdots+3+2+1$. Així, sumant membre a membre:

$$\begin{aligned} S &= 1+2+3+\cdots+(n-2)+(n-1)+n \\ S &= n+(n-1)+(n-2)+\cdots+3+2+1 \end{aligned}$$

s'obté:

$$2S = (n+1)+(n-1+2)+(n-2+3)+\cdots+(n-2+3)+(n-1+2)+(n+1),$$

és a dir,

$2S = (n+1)+(n+1)+\cdots+(n+1)+(n+1)$, suma de n sumands, tots iguals a $n+1$.

Així, $2S = n(n+1)$. Per tant, $S = \frac{n(n+1)}{2}$.

Mètode 2. Per inducció (vegeu el capítol corresponent).

Mètode 3. Partim de la fórmula $(k+1)^2 = k^2+2k+1$, reescrita com $2k+1 = (k+1)^2 - k^2$. D'aquí escrivim

$$\begin{aligned} \sum_{k=1}^{n}(2k+1) &= \sum_{k=1}^{n}((k+1)^2-k^2) = \\ &= (2^2-1^2)+(3^2-2^2)+\cdots+(n^2-(n-1)^2)+((n+1)^2-n^2) = \\ &= (n+1)^2-1^2 = (n+1)^2-1. \end{aligned}$$

D'altra banda, $\sum_{k=1}^{n}(2k+1) = \sum_{k=1}^{n}(2k) + \sum_{k=1}^{n} 1 = 2\sum_{k=1}^{n} k+n$

Per tant, $2\sum_{k=1}^{n} k+n = (n+1)^2-1$, d'on $\sum_{k=1}^{n} k = \frac{(n+1)^2-1-n}{2} = \frac{n(n+1)}{2}$.

Mètode 4 (d'inspiració geomètrica). Denotem $S = 1 + 2 + \cdots + n$. Considerem la quadrícula formada per $n \times n$ quadrats, distribuïts formant un quadrat (un quadrat de quadrats, que conté n^2 quadrats). Sigui $\mathscr{D}$ el conjunt dels quadrats de la diagonal principal, els que ocupen les posicions $i \times i$; és $|\mathscr{D}| = n$. La columna vertical inferior corresponent a cada quadrat (i,i) de la diagonal està formada per i quadrats, de manera que, en total, n'hi ha $1 + 2 + \cdots + n = S$. Considerem la zona triangular superior (exclosa la diagonal $\mathscr{D}$) i sigui Q el nombre de quadrats; anàlogament, la zona triangular inferior, exclosa $\mathscr{D}$, conté el mateix nombre Q de quadrats. Tenim $Q + Q + |\mathscr{D}| = n^2$, d'on $Q = \frac{n^2-n}{2}$. Ara bé, $S = Q + |\mathscr{D}| = \dfrac{n^2-n}{2} + n = \dfrac{n(n+1)}{2}$ ■.

Mètode 5. També és un cas particular de progressió aritmètica i s'hi podria aplicar, per tant, la fórmula general de la suma que es presenta més endavant. Seria $a_1 = 1$, $a_n = n$; per tant, la suma és $\frac{n(n+1)}{2}$.

Observació. Encara es podria plantejar un altre mètode, escrivint $a_n = 1 + 2 + \cdots + n$ com a successió recurrent: en efecte, $a_1 = 1; a_n = a_{n-1} + n$, amb $n \geq 2$. Es resoldria el problema resolent la successió recurrent, és a dir, trobant una fórmula tancada depenent de n, però aquesta possibilitat no es tractarà aquí.

Encara una altra, de gran importància, la de la **suma dels quadrats dels primers nombres naturals**:

Teorema 3.5 *Sigui n un nombre natural, $n \geq 1$. Aleshores:*

$$\sum_{k=1}^{n} k^2 = 1 + 2^2 + 3^2 + \cdots + k^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \tag{3.4}$$

Demostració:

Mètode 1. Utilitzem que $(k+1)^3 = k^3 + 3k^2 + 3k + 1$, que reescrivim com a $(k+1)^3 - k^3 = 3k^2 + 3k + 1$. Ara sumem:

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

Desenvolupem separadament els dos membres de la igualtat anterior:

A l'esquerra:

$$\sum_{k=1}^{n} ((k+1)^3 - k^3) = (2^3 - 1^3) + (3^3 - 2^3) + \cdots + (n^3 - (n-1)^3) + ((n+1)^3 - n^2) = (n+1)^3 - 1^3$$

A la dreta:

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

Obtenim separadament aquestes sumes:

$$\sum_{k=1}^{n} 3k^2 = 3\sum_{k=1}^{n} k^2 \quad \text{(conté la nostra “incògnita”)}$$

$$\sum_{k=1}^{n} 3k = 3\sum_{k=1}^{n} k = 3\frac{n(n+1)}{2}$$

$$\sum_{k=1}^{n} 1 = n$$

Per tant:

$$(n+1)^3 - 1^3 = 3\sum_{k=1}^{n} k^2 + 3\frac{n(n+1)}{2} + n.$$

Així:

$$\sum_{k=1}^{n} k^2 = \frac{1}{3}(((n+1)^3 - 1) - 3\frac{n(n+1)}{2} - n) =$$

$$= \frac{1}{3}(n^3 + 3n^2 + 3n - \frac{3n(n+1)}{2} - n) = \frac{n(n+1)(2n+1)}{6}$$

Observació: si el lector no pot establir deductivament l'última igualtat, també pot desenvolupar separadament les dues últimes fórmules fins a arribar a alguna fórmula coincident per a ambdues, a partir de la qual es deriva la igualtat.

Aquest mètode és aplicable a d'altres situacions similars.

Mètode 2. Més endavant en veurem també una demostració per inducció.

Suma dels cubs dels primers nombres naturals

Teorema 3.6 *Sigui n un nombre natural, $n \geq 1$. Aleshores:*

$$1 + 2^3 + \cdots + j^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + j + \cdots + n)^2 \tag{3.5}$$

$$\sum_{j=1}^{n} j^3 = (\sum_{j=1}^{n} j)^2 \tag{3.6}$$

Observeu que, a partir d'aquí, sabent que $1 + 2 + 3 + \cdots + j + \cdots + n = \frac{n(n+1)}{2}$, tindríem un resultat més concret per a la suma dels cubs dels n primers nombres naturals positius:

$$\sum_{j=1}^{n} j^3 = (\frac{n(n+1)}{2})^2 \tag{3.7}$$

Demostració. Encara que en problemes posteriors es presenta una altra demostració, aquí presentem una demostració per inducció.

Propietat a demostrar: $P(n) := \sum_{j=1}^{n} j^3 = (\sum_{j=1}^{n} j)^2$, per a tot $n \geq 1$, per inducció sobre n, amb $n_0 = 1$.

Pas bàsic: el que correspon a $n_0 = 1$. Cal provar que $P(1)$ és cert, és a dir, que $\sum_{j=1}^{1} j^3 = (\sum_{j=1}^{1} j)^2$. Vegem que els membres de la dreta (D) i de l'esquerra (E) de la igualtat anterior efectivament coincideixen:

$$E = \sum_{j=1}^{1} j^3 = 1^3 = 1$$

$$D = (\sum_{j=1}^{1} j)^2 = 1^2 = 1$$

Pas inductiu: Cal provar, per a tot $k \geq 1$, $P(k) \Rightarrow P(k+1)$, és a dir:

$$\sum_{j=1}^{k} j^3 \overset{HI}{=} (\sum_{j=1}^{k} j)^2 \Rightarrow \sum_{j=1}^{k+1} j^3 = (\sum_{j=1}^{k+1} j)^2.$$

Partim de $(\sum_{j=1}^{k+1} j)^2$.

$$(\sum_{j=1}^{k+1} j)^2 = [(\sum_{j=1}^{k} j) + (k+1)]^2 = (\sum_{j=1}^{k} j)^2 + 2(\sum_{j=1}^{k} j)(k+1) + (k+1)^2$$

Aplicant la hipòtesi d'inducció (HI) i el resultat $1+2+3+\cdots+j+\cdots+n = \dfrac{n(n+1)}{2}$, demostrat prèviament, escrivim l'ultima expressió com:

$$\begin{aligned}
&= \sum_{j=1}^{k} j^3 + 2\frac{k(k+1)}{2}(k+1) + (k+1)^2 = \\
&= \sum_{j=1}^{k} j^3 + k(k+1)(k+1) + (k+1)^2 = \sum_{j=1}^{k} j^3 + k(k+1)^2 + (k+1)^2 = \\
&= \sum_{j=1}^{k} j^3 + (k+1)^2(k+1) = \sum_{j=1}^{k} j^3 + (k+1)^3 = \sum_{j=1}^{k+1} j^3,
\end{aligned}$$

com s'havia de demostrar.

Suma de potències de nombres naturals. Per a completar la informació i els resultats sobre suma de potències de nombres naturals, que apareixen sovint en anàlisi d'algorismes, indiquem a continuació un resultat de [DGRU90]. Observem que es poden expressar les fórmules per a la suma dels n primers enters, la suma dels quadrats dels n primers enters, com un polinomi en n:

$$\begin{aligned} 1+2+\cdots+n &= \frac{n(n+1)}{2} = \frac{1}{2}n^2+\frac{1}{2}n \\ 1+2^2+\cdots+n^2 &= \frac{n(2n+1)}{6} = \frac{1}{6}n+\frac{1}{2}n^2+\frac{1}{3}n^3. \end{aligned}$$

És un resultat: Fixat un nombre natural p, existeix un polinomi

$$W(n) = a_1n+a_2n^2+\ldots+a_pn^p+a_{p+1}n^{p+1}$$

tal que

$$1^p+2^p+3^p+\cdots+n^p = W(n).$$

Els coeficients es poden obtenir a partir de:

$$\left.\begin{array}{rcl} \binom{1}{0}a_1+\binom{2}{0}a_2+\binom{3}{0}a_3+\ldots+\binom{p}{0}a_p+\binom{p+1}{0}a_{p+1} & = & \binom{p}{0} \\ \binom{2}{1}a_2+\binom{3}{1}a_3+\ldots+\binom{p}{1}a_p+\binom{p+1}{1}a_{p+1} & = & \binom{p}{1} \\ & \vdots & \\ \binom{p}{p-1}a_p+\binom{p+1}{p-1}a_{p+1} & = & \binom{p}{p-1} \\ \binom{p+1}{p}a_{p+1} & = & \binom{p}{p} \end{array}\right\}$$

A manca de demostració, podem obtenir així el possible polinomi com a candidat a una suma, per a una fórmula de sumació, per a després fer una prova per inducció.

Exemple 3.10 Per a $p=4$, el polinomi $W(n) = a_1n+a_2n^2+a_3n^3+a_4n^4+a_5n^5$ ve donat per $a_1 = -\dfrac{1}{30}$, $a_2 = 0$, $a_3 = \frac{1}{3}$, $a_4 = \dfrac{1}{2}$, $a_5 = \frac{1}{5}$, a partir de les equacions anteriors. De manera que

$$1^4+2^4+3^4+4^4+\cdots+k^4+\cdots+n^4 = -\frac{1}{30}n+\frac{1}{3}n^3+\frac{1}{2}n^4+\frac{1}{5}n^5,$$

que podríem demostrar per inducció. ■

3.3.2. Sumes derivades de les bàsiques: exemples

Vegem com podem utilitzar algunes de les sumes bàsiques o elementals anteriors per tal d'obtenir-ne d'altres, mitjançant les regles de manipulació bàsica de sumatoris. Les resolucions que veurem es poden considerar exemples de *l'estratègia demostrativa de reduir un problema a un altre ja resolt*. Amb pocs resultats bàsics, es poden resoldre gran quantitat de casos de sumació, reduint el problema a casos coneguts.

Considerem la fórmula de la suma dels n primers nombres naturals,

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

Aquesta fórmula és útil per ella mateixa, però també perquè és la base per a la demostració d'altres sumes de nombres enters, per exemple, de parells o senars. Vegem-ne alguns exemples:

Exemple 3.11 *Suma dels n primers nombres naturals parells*:

$$\sum_{k=1}^{n} 2k = 2+4+6+\cdots+2n.$$

Mètode 1. Vegem com podem reduir el problema a sumar els primers nombres naturals, problema ja resolt anteriorment.

Podem escriure $\sum_{k=1}^{n} 2k = 2\sum_{k=1}^{n} k = 2\frac{n(n+1)}{2} = n(n+1)$.

Mètode 2. Si volem obtenir una fórmula tancada per a la suma dels primers naturals parells, és a dir, $L = 2+4+6+\cdots+2(n-1)+2n$, ho podem fer pel mètode similar a un dels utilitzats per a sumar els n primers nombres naturals:

$$\begin{aligned} L &= 2+4+6+\cdots+2(n-2)+2(n-1)+2n \\ L &= 2n+2(n-1)+2(n-2)+\cdots+6+4+2. \end{aligned}$$

Sumant membre a membre:

$$\begin{aligned} 2L &= [2+2n]+[4+2(n-1)]+[6+2(n-2)]+\cdots+ \\ &+ [2(n-2)+6]+[2(n-1)+4]+[2n+2]. \end{aligned}$$

És la suma de n sumands, tots igual a $2n+2$. Per tant, $2L = n(2n+2)$, d'on $L = n(n+1)$.

Mètode 3. També es pot obtenir a partir del resultat anterior i la fórmula obtinguda per a la suma dels n primers nombres naturals:

$$L+1+3+5+\cdots+(2n-1) = 1+2+3+4+5+\cdots+(2n-1)+2n$$

Fent servir els resultats obtinguts anteriorment, $L+n^2 = \frac{(2n)(2n+1)}{2}$, d'on $L = n^2+n$.
■

Exemple 3.12 *Suma dels $n+1$ primers nombres naturals senars*:

$$\sum_{k=0}^{n} (2k+1) = 1+3+5+7+\cdots+(2n+1).$$

Mètode 1. Apliquem la mateixa estratègia que a l'exemple anterior (mètode 1):

$$\begin{aligned} \sum_{k=0}^{n}(2k+1) &= \sum_{k=0}^{n}(2k)+\sum_{k=0}^{n}1 = \sum_{k=0}^{n}(2k)+(n+1) = 2\sum_{k=0}^{n}k+(n+1) = \\ &= 2\sum_{k=1}^{n}k+(n+1) = 2\frac{n(n+1)}{2}+(n+1) = (n+1)^2. \end{aligned}$$

Mètode 2. La suma dels $n+1$ primers senars es pot obtenir també directament, expressant la suma per ordre creixent i per ordre decreixent:

$$\begin{aligned} S &= 1+3+5+7+\cdots+(2n-3)+(2n-1), \\ S &= (2n-1)+(2n-3)+\cdots+5+3+1. \end{aligned}$$

Sumant i agrupant els sumands:

$$\begin{aligned} 2S &= (1+(2n-1))+(3+(2n-3))+\cdots+((2n-3)+3)+((2n-1)+1)= \\ &= 2n+\cdots+2n = n(2n) = 2n^2, \quad \text{d'on } S=n^2. \end{aligned}$$

Observació. Utilitzant directament el resultat anterior, es poden obtenir altres resultats derivats, com per exemple

$$\begin{aligned} \sum_{k=1}^{n}(2k+1) &= \left(\sum_{k=0}^{n}(2k+1)\right)-\left(\sum_{k=0}^{0}(2k+1)\right)= \\ &= (n+1)^2-(2\cdot 0+1)=(n+1)^2-1=n^2+2n, \end{aligned}$$

d'on obtenim una fórmula tancada per a la suma dels n primers nombres senars:

$$\sum_{k=0}^{n}(2k+1)=n^2+2n+1=(n+1)^2. \blacksquare$$

Exemple 3.13 Calculeu $\sum_{k=4}^{n} k$, para $n \geq 4$. S'aplica la fórmula anterior:

$$\sum_{k=4}^{n}k=\sum_{k=1}^{n}k-\sum_{k=1}^{3}k=\frac{1}{2}n(n+1)-(1+2+3)=\frac{1}{2}n(n+1)-6.$$

També podem aplicar la fórmula dues vegades, com hauríem de fer si tinguéssim un índex inferior molt gran, en comptes de $k=4$:

$$\sum_{k=4}^{n}k=\sum_{k=1}^{n}k-\sum_{k=1}^{3}k=\frac{1}{2}n(n+1)-\frac{3(3+1)}{2}=\frac{1}{2}n(n+1)-6. \blacksquare$$

Exemple 3.14 Calculeu $\sum_{k=1}^{n-1} k$. S'aplica la fórmula general a aquestes dades:

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

Exemple 3.15 Calculeu $\sum_{k=1}^{n} 5k$. És

$$\sum_{k=1}^{n} 5k = 5\sum_{k=1}^{n} k = 5\frac{n(n+1)}{2}. \blacksquare$$

Exemple 3.16 Calculeu $\sum_{k=0}^{n}(7k+1)$. És

$$\sum_{k=0}^{n}(7k+1) = \sum_{k=0}^{n} 7k + \sum_{k=0}^{n} 1 = 7\sum_{k=0}^{n} k + \sum_{k=0}^{n} 1 = 7\sum_{k=1}^{n} k + (n+1) = 7\frac{n(n+1)}{2} + (n+1).$$
$\blacksquare$

Exemple 3.17 Calculeu $\sum_{k=1}^{2n-1} k^2 = 1^2+2^2+3^2+\cdots+(2n-1)^2$ ($2n-1 \geq 1$, és a dir, $n \geq 1$). És una aplicació de $\sum_{k=1}^{n} k^2 = 1+2^2+3^2+\cdots+k^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$:

$$\sum_{k=1}^{2n-1} k^2 = 1^2+2^2+3^2+\cdots+(2n-1)^2 = \frac{(2n-1)((2n-1)+1)(2(2n-1)+1)}{6}. \blacksquare$$

Exemple 3.18 Calculeu $\sum_{k=1}^{2^n} k = 1+2+3+4+\cdots+k+\cdots+(2^n-1)+2^n$. És

$$\sum_{k=1}^{2^n} k = \frac{2^n(2^n+1)}{2}. \blacksquare$$

Exemple 3.19 Calculeu $\sum_{k=1}^{n}(2k+1)^2$. És

$$\begin{aligned}\sum_{k=1}^{n}(2k+1)^2 &= \sum_{k=1}^{n}[4k^2+4k+1] = \sum_{k=1}^{n} 4k^2 + \sum_{k=1}^{n} 4k + \sum_{k=1}^{n} 1 = \\ &= 4\sum_{k=1}^{n} k^2 + 4\sum_{k=1}^{n} k + n = 4\frac{n(n+1)(2n+1)}{6} + 4\frac{n(n+1)}{2} + n.\end{aligned}$$

I anàlogament per a la suma d'altres potències de senars (i també per a $\sum_{k=1}^{n}(2k+1)^3$, $\sum_{k=1}^{n}(5k+1)^2$, $\sum_{k=1}^{n}(2k)^2$, $\sum_{k=1}^{n}(3k)^2$, $\sum_{k=1}^{n}(2k)^3$). $\blacksquare$

3.4. Sumes bàsiques/importants: progressions

3.4.1. Suma dels elements d'una progressió aritmètica

Definició 3.1 *La progressió aritmètica de primer element $a_0 \in \mathbb{R}$ i de raó d (diferència), nombre real no nul, és la successió (finita) de nombres reals*

$$a_0, a_1, a_2, \cdots, a_i, \cdots, \text{ on } a_{i+1} = d + a_i, \text{ per a tot } i \geq 0.$$

Els elements són de la forma a_0, $d + a_0$, $2d + a_0$, $\cdots$, $id + a_0$, $\cdots$, és a dir, $a_i = id + a_0$, per a tot $i \geq 0$.

La progressió també es pot indicar com la seqüència $a_1, a_2, \ldots, a_n$.

Teorema 3.7 *La suma dels termes de la progressió aritmètica $a_1, a_2, \cdots, a_n$, de raó d.*

És $a_1 + \cdots + a_n = n\dfrac{a_1 + a_n}{2}$. Amb sumatoris, $\displaystyle\sum_{i=1}^{n} a_i = n\frac{a_1 + a_n}{2}$.

Demostració:

$$\begin{aligned} a_n &= a_1 + (n-1)d \\ a_1 + a_n &= 2a_1 + (n-1)d, \end{aligned}$$

suma dels dos termes més distants.

Suma dels dos termes equidistants dels extrems:

$$a_{1+k} + a_{n-k}. \text{ És } a_{1+k} + a_{n-k} = (a_1 + kd) + (a_1 + (n-k-1)d) = 2a_1 + (n-1)d.$$

Per tant, les sumes anteriors són totes iguals i $a_{1+k} + a_{n-k} = 2a_1 + (n-1)d = a_1 + a_n$.

Escrivim $S = a_1 + a_2 + \cdots + a_{n-1} + a_n$. I ara en ordre invers; per la propietat commutativa, resulten iguals:

$$S = a_n + a_{n-1} + \cdots + a_2 + a_1.$$

Sumant membre a membre i reagrupant:

$$2S = (a_1 + a_n) + (a_2 + a_{n-1}) + (a_3 + a_{n-2}) + \cdots + (a_{n-2} + a_3) + (a_{n-1} + a_2) + (a_n + a_1).$$

Pel que s'ha dit abans, les sumes entre parèntesis són totes iguals a $a_1 + a_n$, i n'hi ha n (n sumands). Per tant, $2S = n(a_1 + a_n)$. Així, $S = n\dfrac{a_1 + a_n}{2}$.

Exemples 3.20 Vegem-ne alguns exemples d'aplicació, en què s'obtenen resultats ja coneguts.

Exemple 1. Suma dels n primers nombres naturals. També es pot obtenir com a cas particular de suma d'una progressió aritmètica, amb $a_1 = 1$, $a_n = n$, $d = 1$. Per tant, $1 + 2 + \cdots + n = \dfrac{(a_1 + a_n)n}{2} = \dfrac{(1+n)n}{2}$. ■

Exemple 2. Suma dels n primers nombres parells positius. Tot i que s'ha obtingut la fórmula anteriorment, es pot obtenir també com a cas particular de progressió aritmètica, amb $d = 2$, $a_1 = 2$, $a_n = 2n$. Per tant, la suma és $n\dfrac{2+(2n)}{2} = n(n+1)$. ■

Exemple 3. Suma dels $n+1$ primers nombres senars positius. Tot i que s'ha obtingut la fórmula anteriorment, es pot obtenir també com a cas particular de progressió aritmètica, amb $d = 2$, $a_0 = 1$, $a_n = 2n+1$. Per tant, la suma és $(n+1)\dfrac{1+(2n+1)}{2} = (n+1)(n+1) = (n+1)^2$. ■

Exemple 4. Suma dels n primers nombres múltiples de 3 positius. És també un cas particular de progressió aritmètica, amb $d = 3$, $a_1 = 3$, $a_n = 3n$. Aleshores la suma $\sum_{k=1}^{n} 3k$ és $n\dfrac{a_1+a_n}{2} = n\dfrac{3+3n}{2}$. ■

Exemple 5. Suma dels $n+1$ primers nombres positius de la forma $7k+1$. És a dir, $\sum_{k=0}^{n}(7k+1)$. És també un cas particular de progressió aritmètica, amb $d = (7(k+1)+1)-(7k+1) = 7$, $a_1 = 1$, $a_n = 7n+1$. Aleshores la suma $\sum_{k=0}^{n}(7k+1)$ és $(n+1)\dfrac{a_1+a_n}{2} = (n+1)\dfrac{1+(7n+1)}{2} = \dfrac{(n+1)(7n+1)}{2}$. ■

3.4.2. Suma dels elements d'una progressió geomètrica

Definició 3.2 *La progressió geomètrica de primer element $a_0 \in \mathbb{R}$ i de raó x, nombre real no nul, és la successió (finita) de nombres reals*

$$a_0, a_1, a_2, \cdots, a_i, \cdots, \text{ on } a_{i+1} = xa_i, \text{ per a tot } i \geq 0.$$

Els elements són de la forma a_0, xa_0, $x(xa_0) = x^2a_0$, $\cdots$, x^ia_0, $\cdots$, és a dir, $a_i = x^ia_0$, per a tot $i \geq 0$.

Considerem la suma

$$K = a_0 + a_1 + \cdots + a_i + \cdots + a_n = \sum_{i=0}^{n} a_i.$$

És $K = \sum_{i=0}^{n} x^i a_0 = a_0(1+x+x^2+x^3+\cdots+x^i+\cdots+x^n)$, de manera que, per a sumar els $n+1$ primers termes d'una progressió geomètrica de raó x, n'hi ha prou a saber sumar $1+x+x^2+x^3+\cdots+x^i+\cdots+x^n$:

Teorema 3.8 *La suma de* $1+x+x^2+x^3+\cdots+x^i+\cdots+x^n$, *amb* $x\neq 1$.

Sigui $x\neq 1$. *Aleshores,* $1+x+x^2+x^3+\cdots+x^i+\cdots+x^n=\dfrac{1-x^{n+1}}{1-x}=\dfrac{x^{n+1}-1}{x-1}$.

Si $x=1$, *la fórmula no és aplicable, però aleshores directament*

$$1+x+x^2+x^3+\cdots+x^i+\cdots+x^n=(n+1)1=n+1.$$

Demostració. Sigui $S=1+x+x^2+x^3+\cdots+x^i+\cdots+x^{n-1}+x^n$. Considerem $xS=x+x^2+\cdots+x^n+x^{n+1}$. Aleshores $S-xS=1-x^{n+1}$, d'on $(1-x)S=1-x^{n+1}$. Essent $1-x\neq 0$, resulta $S=\dfrac{1-x^{n+1}}{1-x}$.

Així, $1+x+x^2+x^3+\cdots+x^i+\cdots+x^{n-1}+x^n=\dfrac{1-x^{n+1}}{1-x}$.

Exemples 3.21 Vegem exemples d'aplicació immediata d'aquesta fórmula.

Exemple 1. $\sum_{k=0}^{n}2^k=1+2+2^2+\cdots+2^k+\cdots+2^n$. Correspon exactament a la fórmula bàsica amb $x=2$. Aleshores, $\sum_{k=0}^{n}2^k=\dfrac{1-2^{n+1}}{1-2}$. ■

Exemple 2. $\sum_{k=1}^{n}2^k$. És $x=2$. Aleshores, $\sum_{k=1}^{n}2^k=(\sum_{i=0}^{n}2^k)-1=\dfrac{1-2^{n+1}}{1-2}-1$. ■

Exemple 3. $\sum_{k=4}^{n}5^k$. $(n\geq 4)$. És $\sum_{k=4}^{n}5^k=\sum_{i=0}^{n}5^k-\sum_{k=0}^{3}5^k=\dfrac{5^{n+1}-1}{5-1}-\dfrac{5^{3+1}-1}{5-1}$. ■

Exemple 4. $\sum_{k=0}^{n}3^{k+1}=\sum_{k=0}^{n}3^k\cdot 3=3\sum_{k=0}^{n}3^k=3\dfrac{3^{n+1}-1}{3-1}$. ■

Exemple 5. $\sum_{k=0}^{n}(-5)^k=1-5+5^2-5^3+\cdots+(-1)^k5^k+\cdots+(-1)^n5^n$. Aquí és $x=-5$. Per tant, $\sum_{k=0}^{n}(-5)^k=\dfrac{1-(-5)^{n+1}}{1-(-5)}$. ■

Exemple 6. $\sum_{i=0}^{n}(-1)^k$. Aquí és $x=-1$. Per tant, $\sum_{k=0}^{n}(-1)^k=\dfrac{1-(-1)^{n+1}}{1-(-1)}$. ■

Exemple 7. $\sum_{k=0}^{n}(\sqrt{2})^k$. És $x=\sqrt{2}$. Per tant, $\sum_{k=0}^{n}(\sqrt{2})^k=\dfrac{1-(\sqrt{2})^{n+1}}{1-\sqrt{2}}$. ■

Exemple 8. $\sum_{k=0}^{n} \frac{1}{2^k}$. És $\sum_{k=0}^{n} \frac{1}{2^k} = \sum_{i=0}^{n} (\frac{1}{2})^k$. És $x = \frac{1}{2}$. Per tant, $\sum_{k=0}^{n} \frac{1}{2^k} = \frac{1-(\frac{1}{2})^{n+1}}{1-\frac{1}{2}}$. ■

Exemple 9. $\sum_{k=0}^{n} \frac{1}{(\sqrt{5})^k} = \sum_{k=0}^{n} (\frac{1}{\sqrt{5}})^k$. És $x = \frac{1}{\sqrt{5}}$. Per tant, la suma és $\frac{(\frac{1}{\sqrt{5}})^{n+1}-1}{\frac{1}{\sqrt{5}}-1}$. ■

Exemple 10. $\sum_{k=0}^{n^2+1} 2^k$. És $x = 2$. $\sum_{k=0}^{n^2+1} 2^k = \frac{2^{(n^2+1)+1}-1}{2-1}$. ■

Exemple 11. $\sum_{k=20}^{n} 2^k$ $(n \geq 20)$. És $\sum_{k=20}^{n} 2^k = \sum_{k=0}^{n} 2^k - \sum_{k=0}^{19} 2^k = \frac{2^{n+1}}{2-1} - \frac{2^{19+1}}{2-1}$. ■

Exemple 12. $\sum_{k=3}^{n} (-5)^k$, $(n \geq 3)$. $\sum_{k=3}^{n} (-5)^k = \sum_{k=0}^{n} (-5)^k - (1-5+5^2) = \frac{1-(-5)^{n+1}}{1-(-5)} - (1-5+5^2)$. ■

Exemple 13. $\sum_{k=0}^{n} 2(-3)^k$, $(n \geq 1)$. $\sum_{k=0}^{n} 2(-3)^k = 2\sum_{k=0}^{n} (-3)^k = 2\frac{1-(-3)^{n+1}}{1-(-3)}$. ■

Exemple 14. $\sum_{k=0}^{n} ((-1)^k + 1)$. És $\sum_{k=0}^{n} ((-1)^k + 1) = \sum_{k=0}^{n} (-1)^k + \sum_{k=0}^{n} 1 = \frac{1-(-1)^{n+1}}{1-(-1)} + (n+1)$. ■

Exemple 15. $\sum_{k=0}^{n} (7^k - 3^k)$. És $\sum_{k=0}^{n} (7^k - 3^k) = \sum_{k=0}^{n} (7^k) - \sum_{k=0}^{n} (3^k) = \frac{1-(7)^{n+1}}{1-7} - \frac{1-(3)^{n+1}}{1-3}$.
■

Exemple 16. $\sum_{k=0}^{n} (7^{k+2} - 3^{k+1})$. És $\sum_{k=0}^{n} (7^k \cdot 7^2) - \sum_{k=0}^{n} (3^k \cdot 3) = 7^2 \sum_{k=0}^{n} (7^k) - 3\sum_{k=0}^{n} (3^k)$. ■

Exemple 17. $\sum_{k=0}^{n} 3^{5k+2}$. És

$$\sum_{k=0}^{n} 3^{5k+2} = \sum_{k=0}^{n} 3^{5k} \cdot 3^2 = 3^2 \sum_{k=0}^{n} (3^5)^k = 3^2 \frac{1-(3^5)^{n+1}}{1-3^5} = 3^2 \frac{1-3^{5(n+1)}}{1-3^5}.$$ ■

Exemple 18. Sumeu $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n}$. S'observa que és un cas particular de suma d'elements consecutius de la progressió geomètrica de raó $x = \frac{1}{2}$, ja que es pot reescriure com $\sum_{k=1}^{n}(\frac{1}{2})^n$. Aleshores, aplicant la fórmula obtinguda anteriorment, podem escriure $\sum_{k=1}^{n}(\frac{1}{2})^n = \sum_{k=0}^{n}(\frac{1}{2})^n - 1 = \frac{1-(\frac{1}{2})^{n+1}}{1-\frac{1}{2}} - 1 = 1 - \frac{1}{2^n}$.

3.5. Algunes expressions útils amb sumatoris

Poden ser útils les fórmules amb sumatoris següents (suposant definides totes les a_i que calguin). Per exemple, algunes per a demostracions per inducció.

$$\sum_{k=1}^{n+1} a_k = (\sum_{k=1}^{n} a_k) + a_{n+1} \quad (n \geq 1)$$

$$\sum_{k=1}^{n+2} a_k = (\sum_{k=1}^{n} a_k) + a_{n+1} + a_{n+2} \quad (n \geq 1)$$

$$\sum_{k=1}^{n} a_k = (\sum_{k=1}^{n-1} a_k) + a_n \quad (n \geq 2)$$

$$\sum_{k=5}^{n} a_k = \sum_{k=1}^{n} a_k - \sum_{k=1}^{5} a_k \quad (n \geq 5)$$

$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{m} a_k + \sum_{k=m+1}^{n} a_k \quad (1 \leq m \leq n)$$

$$\sum_{k=r}^{s} a_k = \sum_{k=1}^{s} a_k - \sum_{k=1}^{r-1} a_k \quad (1 \leq r \leq s)$$

Concretem-ne algunes, per a $a_k = k$:

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1) \quad (n \geq 1)$$

$$\sum_{k=1}^{n+2} k = \sum_{k=1}^{n} k + (n+1) + (n+2) \quad (n \geq 1)$$

$$\sum_{k=1}^{n} k = \sum_{k=1}^{n-1} k + n \quad (n \geq 2)$$

$$\sum_{k=5}^{n} k = \sum_{k=1}^{n} k - \sum_{k=1}^{5} k = \frac{n(n+1)}{2} - \frac{5(5+1)}{2} \quad (n \geq 5)$$

$$\sum_{k=2000}^{5000} k = \sum_{k=1}^{5000} k - \sum_{k=1}^{1999} k = \frac{5000(5000+1)}{2} - \frac{1999(1999+1)}{2}.$$

A les dues últimes, s'ha aplicat $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

3.6. Dobles sumatoris

Vegem alguns exemples de sumatoris dobles:

$$\sum_{j=1}^{r}\sum_{i=1}^{s}(i+j)\ (r \geq 1,\, s \geq 1) \qquad \sum_{j=0}^{r}\sum_{i=1}^{s} ij\ (r \geq 0,\, s \geq 1)$$

$$\sum_{j=1}^{r}\sum_{i=1}^{s}(ij+1)\ (r \geq 1,\, s \geq 1) \qquad \sum_{j=1}^{r}\sum_{i=j}^{s} ij\ (r \geq 1,\, s \geq 1)$$

En tota aquesta secció, $n, m \in \mathbb{N}$, $n \geq 1, m \geq 1$, i tots els a_i són nombres reals, per a tot $a_i \leq n$, i per a tot $1 \leq j \leq m$.

Què signifiquen les expressions següents ("sumatori de sumatoris"):

$$\alpha = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}.$$

$$\beta = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}.$$

$$\gamma = \sum_{i,j=1}^{n} a_{ij}.$$

Se suposa que: $i = 1, \ldots, n$; $j = 1, \ldots, m$.

L'expressió α :

$$\alpha = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} = \sum_{i=1}^{n}\Big(\sum_{j=1}^{m} a_{ij}\Big).$$

Exemple 3.22

$$\sum_{j=1}^{4}\sum_{i=1}^{3} ij = \sum_{j=1}^{4}\Big(\sum_{i=1}^{3} ij\Big) = \sum_{j=1}^{4}(j+2j+3j) =$$

$$= (1+2\cdot 1+3\cdot 1)+(2+2\cdot 2+3\cdot 2)+(3+2\cdot 3+3\cdot 3)+(4+2\cdot 4+3\cdot 4).\blacksquare$$

Exemple 3.23 Aquesta suma pot correspondre a la suma de tots els termes d'una matriu de s files i r columnes, amb $a_{ij} = i \cdot j$.

$$\sum_{j=1}^{r}\sum_{i=1}^{s} ij = \sum_{j=1}^{r}(\sum_{i=1}^{s} ij)$$

Calculem primer $\sum_{i=1}^{s} ij$. En aquest sumatori, j juga el paper d'una constant. Per tant:

$$\sum_{i=1}^{s} ij = j\sum_{i=1}^{s} i = j\frac{s(s+1)}{2}, \text{ per un resultat ben conegut.}$$

Finalment:

$$\sum_{j=1}^{r}\sum_{i=1}^{s} ij = \sum_{j=1}^{r}(j\frac{s(s+1)}{2}) = \frac{s(s+1)}{2}\sum_{j=1}^{r} j = \frac{s(s+1)}{2}\frac{r(r+1)}{2}. \blacksquare$$

Als efectes del sumatori interior, $\sum_{j=1}^{m} a_{ij}$, l'índex i actua com a constant i només s'ha de considerar la variació de l'índex j. És:

$$\alpha = (\sum_{j=1}^{m} a_{1j}) + (\sum_{j=1}^{m} a_{2j}) + \overset{n}{\overbrace{\cdots}} + (\sum_{j=1}^{m} a_{nj}).$$

El mateix podem dir per a β:

$$\beta = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij} = \sum_{j=1}^{m}(\sum_{i=1}^{n} a_{ij}).$$

Als efectes del sumatori interior, l'índex de variació és i; j fa el paper de constant. Així:

$$\beta = (\sum_{i=1}^{n} a_{i1}) + (\sum_{i=1}^{n} a_{i2}) + \cdots + (\sum_{i=1}^{n} a_{im}).$$

Relació entre $\boldsymbol{\alpha}$ i $\boldsymbol{\beta}$. Són el mateix: $\alpha = \beta$.

Observació: Quan tenim un doble sumatori podem, si convé, canviar l'ordre dels sumatoris.

Això no és més que conseqüència de les propietats elementals de la suma i el producte ordinaris en $\mathbb{R}$ (commutativitat i associativitat). Correspon a sumar de maneres diferents **tots** els a_{ij}, distribuint els elements a_{ij} en una taula, per files i columnes, i sumant separadament per files i per columnes. El resultat és el mateix.

	a_{11}	a_{12}	a_{13}	$\dots$	a_{ij}	$\dots$	a_{1m}	$\sum_{j=1}^{m} a_{1j}$
	a_{21}	a_{22}	a_{23}	$\dots$	a_{ij}	$\dots$	a_{2m}	$\sum_{j=1}^{m} a_{2j}$
	a_{31}	a_{32}	a_{33}	$\dots$	a_{ij}	$\dots$	a_{3m}	$\sum_{j=1}^{m} a_{3j}$
	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
	a_{i1}	a_{i2}	a_{i3}	$\dots$	a_{ij}	$\dots$	a_{im}	$\sum_{j=1}^{m} a_{ij}$
	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
	a_{n1}	a_{n2}	a_{n3}	$\dots$	a_{nj}	$\dots$	a_{nm}	$\sum_{j=1}^{m} a_{nj}$
Suma columna	$\sum_{i=1}^{n} a_{i1}$	$\sum_{i=1}^{n} a_{i2}$	$\sum_{i=1}^{n} a_{i3}$	$\dots$	$\sum_{i=1}^{n} a_{ij}$	$\dots$	$\sum_{i=1}^{n} a_{im}$	Suma de les columnes
Suma de les files			$\sum_{j=1}^{m}(\sum_{i=1}^{n} a_{ij})$		$(=\beta)$			Suma de tots els a_{ij}

I, si no, analíticament:

$$\begin{aligned}
\alpha = (\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} &= (\sum_{j=1}^{m} a_{1j}) \quad +(\sum_{j=1}^{m} a_{2j}) \quad + \dots \quad +(\sum_{j=1}^{m} a_{mj}) \\
= & \quad (a_{11}+a_{12}+\dots+a_{1m}) \quad + \\
+ & \quad (a_{21}+a_{22}+\dots+a_{2m}) \quad + \\
+ & \quad \dots \quad \dots \quad \dots \quad \dots \quad + \\
+ & \quad (a_{n1}+a_{n2}+\dots+a_{nm}) \\
\\
= & \quad \text{(sumem agrupant per columnes)} \quad = \\
= & \quad (\sum_{i=1}^{n} a_{i1}) + (\sum_{i=1}^{n} a_{i2}) + \dots + (\sum_{i=1}^{n} a_{im}) \\
= & \quad \sum_{j=1}^{m}(\sum_{i=1}^{n} a_{ij}) = \beta
\end{aligned}$$

Els límits de variació dels índexs poden ser més generals, com per exemple:

$$\sum_{i=3}^{2^n}\sum_{j=8}^{m^2+1} a_{ij}.$$

Nombre total de sumands en el doble sumatori $\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}$:

el nombre de sumands és *nm*; és el producte del nombre de sumands del sumatori intern pel nombre de sumands corresponent al sumatori extern. Es pot generalitzar: el nombre de sumands de

$$\sum_{i=p}^{q}\sum_{j=r}^{s} a_{ij} = (q-p+1)(s-r+1).$$

En els casos i exemples anteriors, els índexs i, j varien independentment. Això no és necessàriament així.

$$\sum_{i=1}^{s}\sum_{j=i}^{r} ij$$

Observació: Els índexs i, j són substituïbles per altres, de manera que, per exemple:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} = \sum_{p=1}^{n}\sum_{q=1}^{m} a_{pq}$$

L'expressió γ : $\quad \gamma = \sum_{i,j=1}^{n} a_{ij} = \sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ij}) = \sum_{j=1}^{m}(\sum_{i=1}^{n} a_{ij})$

I anàlogament amb triples sumatoris.

Vegem-ne alguns exemples addicionals:

Exemple 3.24 Aquesta suma pot correspondre a la suma de tots els termes d'una matriu quadrada d'ordre n, amb $a_{ij} = i + j$.

$$\sum_{j=1}^{n}\sum_{i=1}^{n}(j+i) = \sum_{j=1}^{n}(\sum_{i=1}^{n}(j+i))$$

Calculem $a = \sum_{i=1}^{n}(j+i)$.

En primer lloc,

$$a = \sum_{i=1}^{n}(j+i) = (\sum_{i=1}^{n} j) + (\sum_{i=1}^{n} i) = j(\sum_{i=1}^{n} 1) + (\sum_{i=1}^{n} 1) = jn + \frac{n(n+1)}{2}.$$

Completem el càlcul:

$$\begin{aligned}\sum_{j=1}^{n}\sum_{i=1}^{n}(j+i) &= \sum_{j=1}^{n}(jn + \frac{n(n+1)}{2}) = (\sum_{j=1}^{n} jn) + (\sum_{j=1}^{n} \frac{n(n+1)}{2}) \stackrel{*}{=} \\ &\stackrel{*}{=} n(\textstyle\sum_{j=1}^{n} j) + \frac{n(n+1)}{2}(\sum_{j=1}^{n} 1) = n\dfrac{n(n+1)}{2} + \dfrac{n(n+1)}{2}n = n^2(n+1).\end{aligned}$$

(*): n és constant dintre de cada sumatori. ■

Exemple 3.25 Una generalització de l'anterior:

$$\begin{aligned}\sum_{j=1}^{r}\sum_{i=1}^{s}(j+i) &= \sum_{j=1}^{r}[(\sum_{i=1}^{s} j) + (\sum_{i=1}^{s} i)] = \sum_{j=1}^{r}[j(\sum_{i=1}^{s} 1) + \frac{s(s+1)}{2}] = \\ &= \sum_{j=1}^{r}[js + \frac{s(s+1)}{2}] == (\sum_{j=1}^{r} js) + (\sum_{j=1}^{r} \frac{s(s+1)}{2}) = \\ &= s(\sum_{j=1}^{r} j + \frac{s(s+1)}{2}(\sum_{j=1}^{r} 1) = s\frac{r(r+1)}{2} + \frac{s(s+1)}{2}r = \frac{rs}{2}(r+s+2).\end{aligned}$$ ■

Exemple 3.26 $\sum_{j=1}^{r}\sum_{i=j}^{s} ij$:

Al sumatori interior $\sum_{i=j}^{s} ij$, j fa el paper de constant.

$$\sum_{i=j}^{s} ij = \sum_{i=1}^{s} ij - \sum_{i=1}^{j-1} ij = j(\sum_{i=1}^{s} i) - j\sum_{i=1}^{j-1} i = j\frac{s(s+1)}{2} - j\frac{(j-1)((j-1)+1)}{2} =$$
$$= j\frac{s(s+1)}{2} - \frac{j(j-1)(j)}{2} = j\frac{s(s+1)}{2} - \frac{j^3}{2} + \frac{j^2}{2}$$

Així,

$$\sum_{j=1}^{r}\sum_{i=j}^{s} ij = \sum_{j=1}^{r}(j\frac{s(s+1)}{2} - \frac{j^3}{2} + \frac{j^2}{2}) = \sum_{j=1}^{r} j\frac{s(s+1)}{2} - \sum_{j=1}^{r}\frac{j^3}{2} + \sum_{j=1}^{r}\frac{j^2}{2}$$

Calculem separadament cada sumatori:

$$\sum_{j=1}^{r} j\frac{s(s+1)}{2} = \frac{s(s+1)}{2}\sum_{j=1}^{r} j = \frac{s(s+1)}{2}\frac{r(r+1)}{2}.$$

$$\sum_{j=1}^{r}\frac{j^3}{2} = \frac{1}{2}\sum_{j=1}^{r} j^3$$

Cal fer servir un resultat conegut: $\sum_{j=1}^{r} j^3 = (\frac{r(r+1)}{2})^2$.

$$\sum_{j=1}^{r}\frac{j^2}{2} = \frac{1}{2}\sum_{j=1}^{r} j^2$$

Cal fer servir un resultat conegut:

$$\sum_{j=1}^{r} j^2 = \frac{r(r+1)(2r+1)}{6}$$

Se substitueix i es completa el càlcul. ■

3.7. Productes ("productoris")

Un "productori" no és més que un artifici notacional per a escriure, de manera compacta, expressions com:

$$a_1 a_2 \dots a_n$$

S'escriu:

$$\prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n, \text{ amb } n \geq 1$$

Exemple 3.27 $\prod_{i=1}^{n} i = 1 \cdot 2 \ldots i \ldots n = n!$ (factorial), $n \geq 1$. ■

Se suposa que $1 \leq i \leq n$ i que l'índex de variació del producte creix amb increments d'una unitat: $i = 1, 2, \ldots, n$.

Els límits inferior i superior poden ser diferents dels anteriors:

$$\prod_{i=i_0}^{i_1} a_i = a_{i_0} \ldots a_{i_1}, \text{ amb } i_1 \geq i_0$$

Exemples 3.28

Exemple 1. $\prod_{i=3}^{2n} a_i = a_3 a_4 a_5 \ldots a_{2n}$, amb $2n \geq 3$ ■

Exemple 2. $\dfrac{2^2 \cdot 4^2 \cdot 6^2 \ldots (2n)^n}{3^3 \cdot 5^3 \cdots (2n+1)^3} = \dfrac{\prod_{k=1}^{n} (2k)^2}{\prod_{k=1}^{n} (2k+1)^3} = \prod_{k=1}^{n} \dfrac{(2k)^2}{(2k+1)^3}$ ■

Exemple 3. $\prod_{i=1}^{n} i^2 = 1^2 \cdot 2^2 \cdots n^2 = (1 \cdot 2 \cdots n)^2 = (\prod_{i=1}^{n} i)^2$

Aquest últim es pot reescriure com:

$$\prod_{i=1}^{n} i^2 = (\prod_{i=1}^{n} i)^2 = (n!)^2 \text{ ■}$$

3.8. Com resoldre problemes de sumació, de sumatoris

Problema: Obtenir una expressió tancada per a la suma en un sumatori

L'objectiu és obtenir resultats de suma i expressar-los de forma tancada, mitjançant alguna funció o expressió que eviti els punts suspensius o haver de calcular el resultat per iteració. Exemple: per a $1 + 2 + 3 + \cdots + n$ volem una fórmula $f(n)$ tal que $1 + 2 + 3 + \cdots + n = f(n)$.

Si és possible, i si escau,

a) Descompondre el problema en una col·lecció de subproblemes a resoldre separadament, cadascun d'ells més senzill que l'original. Com? Aplicant les propietats de suma de sumatoris i producte per escalar, enunciades anteriorment.

b) Cal identificar el patró o la tipologia del problema general o dels subproblemes, o veure si s'hi pot reduir.

Per exemple, totes les següents es poden reduir fàcilment a una suma dels termes d'una progressió geomètrica de raó x:

$$\sum_{j=1}^{n} 4^j \sum_{j=1}^{n} (-4)^j \sum_{j=1}^{n} (-1)^j 4^j \sum_{j=3}^{n} 4^j \sum_{j=3}^{2n} 4^j \sum_{j=1}^{n} 4^{j+2}$$

En efecte:

$$\sum_{j=1}^{n} 4^j \ (x=4)$$

$$\sum_{j=0}^{n} (-4)^j \ (x=-4)$$

$$\sum_{j=0}^{n} (-1)^j 4^j \ (x=-4, \text{ ja que } (-1)^j 4^j = (-4)^j)$$

$$\sum_{j=3}^{n} 4^j \ (x=4)$$

$$\sum_{j=3}^{2n} 4^j \ (x=4)$$

$$\sum_{j=1}^{n} 4^{j+2} = \sum_{j=1}^{n} 4^j 4^2 = 16 \sum_{j=1}^{n} 4^j = 16[(\sum_{j=0}^{n} 4^j) - 1] = 16(-1 + \frac{4^{n+1}-1}{4-1})$$

$$\sum_{j=0}^{n} (-1)^{j+1} 4^j = \sum_{j=0}^{n} (-1)^j (-1) 4^j = (-1) \sum_{j=0}^{n} (-1)^j 4^j = -\sum_{j=0}^{n} (-4)^j = -\frac{1-(-4)^{n+1}}{1-(-4)}.$$

c) Disposar d'una provisió de fórmules de sumació a punt per ser utilitzades, que es poden fer servir com a bàsiques.

d) Aplicar resultats que ja tinguem: suma dels naturals i potències, progressió aritmètica, progressió geomètrica, binomi de Newton, expressió de $x^n - y^n$ i altres.

e) Possiblement, s'hauran d'adaptar els índexs de variació i els valors ($x = 2$, $x = 1/2$, $x = -1$, $x = \sqrt{2}$, per exemple per a la fórmula d'una suma de la progressió geomètrica)

f) Cal identificar els valors mínim i màxim de l'índex, el terme general.

g) Cal saber calcular el nombre de sumands.

h) En casos especials, veure si s'ajusta el que s'ha de sumar al tipus de la fórmula de Newton o altres.

Fórmules molt útils s'expressen en termes de sumatoris, com la fórmula del binomi de Newton, que és:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \tag{3.8}$$

amb x, y nombres reals i n nombre natural.

Dediquem un capítol posterior a presentar exemples i exercicis relacionats amb aquesta fórmula important. L'aplicació en moltes ocasions exigeix veure si el problema de sumació que s'ha de resoldre resoldre correspon al patró de la fórmula o s'hi pot reduir. Per exemple, $\sum_{k=0}^{n} \binom{n}{k} 3^k$ n'és un cas particular, amb $x = 3$, $y = 1$.

Una altra fórmula important és:

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}),$$

per a x, y nombres reals i n nombre natural. També hi ha un capítol reservat a la fórmula.

En els exercicis de la secció següent, es veuran diversos exemples d'aquesta manera de procedir.

3.9. Problemes resolts

Observació important. Alguns dels problemes de sumació que segueixen es poden resoldre també per inducció. Per completar-ho, en diversos casos hem inclòs resolucions per inducció, encara que correspongui a un capítol específic posterior.

PROBLEMA 3.1

Sigui n un nombre natural positiu qualsevol.

a) Utilitzeu $(k+1)^2 - k^2$ *per a obtenir* $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

b) Utilitzeu $(k+1)^3 - k^3$ *per a obtenir* $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

c) Utilitzeu $(k+1)^4 - k^4$ *per a obtenir* $\sum_{k=1}^{n} k^3 = (\frac{n(n+1)}{2})^2$.

Observació: En aquest problema es presenta un mètode i, al mateix temps, s'obtenen demostracions alternatives per a resultats provats per altres mètodes.

Solució. Es plantegen equacions on les "incògnites" són els sumatoris que es demanen. És un exemple d'ús de sumes telescòpiques. S'utilitzen resultats dels apartats anteriors per a resoldre els posteriors al primer.

a) En primer lloc, $(k+1)^2 - k^2 = (k^2+2k+1) - k^2 = 2k+1$ i, per tant,

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

Aïllant la incògnita $\sum_{k=1}^{n} k$, resulta: $\displaystyle\sum_{k=1}^{n} k = \frac{(\sum_{k=1}^{n}((k+1)^2-k^2)) - n}{2}$.

Calculem per un altre mètode $\displaystyle\sum_{k=1}^{n}((k+1)^2-k^2)$; desplegant el sumatori, resulten clares les cancel·lacions que es produeixen entre els sumands:

$$\begin{aligned}\sum_{k=1}^{n}((k+1)^2-k^2) &= [(1+1)^2-1^2]+[(2+1)^2-2^2]+[(3+1)^2-3^2]+\cdots+\\ &+ [((n-1)+1)^2-(n-1)^2]+[(n+1)^2-n^2] = [2^2-1^2]+\\ &+ [3^2-2^2]+[4^2-3^2]+\cdots+[n^2-(n-1)^2]+[(n+1)^2-n^2] =\\ &= (n+1)^2-1^2.\end{aligned}$$

Així, $\displaystyle\sum_{k=1}^{n}((k+1)^2-k^2) = (n+1)^2-1^2 = n^2+2n+1-1 = n^2+2n$.

Finalment, $\displaystyle\sum_{k=1}^{n} k = \frac{(\sum_{k=1}^{n}((k+1)^2-k^2)) - n}{2} = \frac{(n^2+2n)-n}{2} = \frac{n^2+n}{2} = \frac{n(n+1)}{2}$.

b) D'una banda, tenim $(k+1)^3 - k^3 = (k^3+3k^2+3k+1) - k^3 = 3k^2+3k+1$, d'on

$$\begin{aligned}\sum_{k=1}^{n}((k+1)^3-k^3) &= \sum_{k=1}^{n}(3k^2+3k+1) = \sum_{k=1}^{n}(3k^2)+\sum_{k=1}^{n}(3k)+\sum_{k=1}^{n}1 =\\ &= 3\textstyle\sum_{k=1}^{n}k^2 + 3\sum_{k=1}^{n}k + n.\end{aligned}$$

Utilitzant el resultat de l'apartat (a):

$$\sum_{k=1}^{n}((k+1)^3-k^3) = 3\sum_{k=1}^{n}k^2 + 3\frac{n(n+1)}{2} + n.$$

A partir d'aquí, aïllem la suma que cal obtenir. Però primer hem de calcular

$$\sum_{k=1}^{n}((k+1)^3-k^3)$$

d'una manera alternativa, desplegant el sumatori i observant com es produeix la simplificació dels sumands:

$$\begin{aligned}\sum_{k=1}^{n}((k+1)^3-k^3) &= [(1+1)^3-1^3]+[(2+1)^3-2^3]+[(3+1)^3-3^3]+\cdots+\\&+[((n-1)+1)^3-(n-1)^3]+[(n+1)^3-n^3]=\\&=[2^3-1^3]+[3^3-2^3]+[4^3-3^3]+\cdots+[n^3-(n-1)^3]+\\&+[(n+1)^3-n^3]=(n+1)^3-1^3=\\&=n^3+3n^2+3n+1-1=n^3+3n^2+3n.\end{aligned}$$

Així, $n^3+3n^2+3n=3\sum_{k=1}^{n}k^2+3\frac{n(n+1)}{2}+n$. Aïllant el que ens interessa,

$$\begin{aligned}\sum_{k=1}^{n}k^2 &= \frac{1}{3}[(n^3+3n^2+3n)-3\frac{n(n+1)}{2}-n]=\frac{1}{3}[(n^3+3n^2+2n)-3\frac{n(n+1)}{2}]=\\&=\frac{n(n+1)(2n+1)}{6}\end{aligned}$$

c) En primer lloc, $(k+1)^4-k^4=(k+1)^3(k+1)-k^4=4k^3+6k^2+4k+1$, d'on

$$\sum_{k=1}^{n}((k+1)^4-k^4)=\sum_{k=1}^{n}(4k^3+6k^2+4k+1).$$

Desplegant el sumatori i simplificant, el membre de l'esquerra es pot escriure com:

$$\begin{aligned}\sum_{k=1}^{n}((k+1)^4-k^4) &= (n+1)^4-1^4=(n^4+4n^3+6n^2+4n+1)-1=\\&=n^4+4n^3+6n^2+4n.\end{aligned}$$

El membre de la dreta és

$$4\sum_{k=1}^{n}k^3+6\sum_{k=1}^{n}k^2+4\sum_{k=1}^{n}k+\sum_{k=1}^{n}1=4\sum_{k=1}^{n}k^3+6\frac{n(n+1)(2n+1)}{6}+4\frac{n(n+1)}{2}+n,$$

aplicant els resultats dels dos apartats anteriors.

Així, $n^4+4n^3+6n^2+4n=4\sum_{k=1}^{n}k^3+n(n+1)(2n+1)+2n(n+1)+n$, d'on, efectuats els càlculs pertinents,

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

PROBLEMA 3.2

Siguin n, r, s nombres naturals, $n \geq 1, r \geq 1, s \geq 1$. Hem demostrat fórmules per a la suma dels primers nombres naturals, els seus quadrats i els seus cubs. Apliqueu-les per a obtenir:

a) $\sum_{k=0}^{n}(2k+1), \sum_{k=1}^{n}(2k-1)$.

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

c) $\sum_{k=1}^{n}(5k)^3$.

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

e) $\sum_{k=0}^{n}(3k+2)$.

f) $\sum_{i=1}^{n}\sum_{j=1}^{i} j$. *Aquesta suma pot correspondre a la suma dels termes d'una matriu quadrada d'ordre n, situats sota la diagonal principal, amb la diagonal inclosa:* $\sum_{i=1}^{n}\sum_{j=1}^{i} a_{ij}$, *amb* $a_{ij} = j$. *Enunciats alternatius:* $a_{ij} = ij$, $a_{ij} = 2j+1$, $a_{ij} = i+j$. *Sense incloure la diagonal, seria* $\sum_{i=1}^{n}\sum_{j=1}^{i-1} j$.

g) $\sum_{k=1}^{n} k(k+1)$

h) $\sum_{k=0}^{n} 3^{2k+1}$

Solució

a) **Mètode 1:**

$$\sum_{k=0}^{n}(2k+1) = \sum_{k=0}^{n}(2k) + \sum_{k=0}^{n} 1 = \sum_{k=1}^{n}(2k) + (n+1) = n(n+1) + (n+1) = (n+1)^2.$$

Mètode 2. Sumant parells i senars, obtenim la suma dels $2n+1$ primers nombres naturals i aleshores apliquem les fórmules anteriors:

$$\sum_{k=1}^{n}(2k) + \sum_{k=0}^{n}(2k+1) = \sum_{i=1}^{2n+1} i,$$

és a dir,

$$\begin{aligned} \sum_{k=0}^{n}(2k+1) &= \sum_{i=1}^{2n+1} i - \sum_{k=1}^{n}(2k) = \frac{(2n+1)(2n+2)}{2} - n(n+1) = \\ &= (2n+1)(n+1) - n(n+1) = (n+1)^2. \end{aligned}$$

L'altre és similar:

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

b) $\displaystyle\sum_{k=1}^{n}(2k)^2=\sum_{k=1}^{n}4k^2=4\sum_{k=1}^{n}k^2=4\frac{n(n+1)(2n+1)}{6}.$

c) $\displaystyle\sum_{k=1}^{n}(5k)^3=\sum_{k=1}^{n}5^3k^3=5^3\sum_{k=1}^{n}k^3=5^3(\frac{n(n+1)}{2})^2.$

d) $\displaystyle\sum_{k=0}^{n}(2k+1)^3$. És $(2k+1)^3=(2k)^3+3(2k)^2+3(2k)+1=8k^3+12k^2+6k+1.$

Llavors:

$$\begin{aligned}\sum_{k=0}^{n}(2k+1)^3 &= \sum_{k=0}^{n}(8k^3+12k^2+6k+1)=\\ &= \sum_{k=0}^{n}8k^3+\sum_{k=0}^{n}12k^2+\sum_{k=0}^{n}6k+\sum_{k=0}^{n}1=\\ &= 8\sum_{k=0}^{n}k^3+12\sum_{k=0}^{n}k^2+6\sum_{k=0}^{n}k+(n+1)=\\ &= 8(\frac{n(n+1)}{2})^2+12\frac{n(n+1)(2n+1)}{6}+6\frac{n(n+1)}{2}+(n+1).\end{aligned}$$

e) $$\begin{aligned}\sum_{k=0}^{n}(3k+2) &= \sum_{k=0}^{n}(3k)+\sum_{k=0}^{n}2=\sum_{k=1}^{n}(3k)+2(n+1)=\\ &= 3\sum_{k=1}^{n}k+2(n+1)=\frac{3n(n+1)}{2}+2(n+1)=\frac{3n+4}{2}(n+1).\end{aligned}$$

f) $$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{i}j &= \sum_{i=1}^{n}\frac{i(i+1)}{2}=\sum_{i=1}^{n}[\frac{1}{2}i^2+\frac{1}{2}i]=\frac{1}{2}(\sum_{i=1}^{n}i^2+\sum_{i=1}^{n}i)=\\ &= \frac{1}{2}(\frac{n(n+1)(2n+1)}{6})+\frac{n(n+1)}{2}).\end{aligned}$$

g) $\displaystyle\sum_{k=1}^{n}k(k+1)$. És

$$\sum_{k=1}^{n}k(k+1)=\sum_{k=1}^{n}(k^2+k)=\sum_{k=1}^{n}k^2+\sum_{k=1}^{n}k=\frac{n(n+1)(2n+1)}{6}+\frac{n(n+1)}{2}.$$

h) $\displaystyle\sum_{k=0}^{n} 3^{2k+1} = \sum_{k=0}^{n} 3^{2k} \cdot 3 = 3\sum_{k=0}^{n} 3^{2k} = 3\sum_{k=0}^{n} (3^2)^k = 3\sum_{k=0}^{n} 9^k = 3\frac{9^{n+1}-1}{9-1}$

(suma d'una progressió geomètrica, $x = 9$).

PROBLEMA 3.3

Si $n \geq 1$ és un nombre natural:

a) Demostreu per inducció que

$$\sum_{j=1}^{n} j^3 = \frac{n^2(n+1)^2}{4}$$

b) Apliqueu la fórmula anterior al càlcul de

$$\sum_{j=2}^{n+1} ((4j)^3 + 1)$$

Expliciteu-ne detalladament tots els passos.

Solució

a) La propietat $P(n)$ que es vol demostrar és $\displaystyle\sum_{j=1}^{n} j^3 = \frac{n^2(n+1)^2}{4}$, per a tot $n \geq 1$.

i) *Pas base*. Cal demostrar $P(1)$; en aquest cas, es redueix a una simple comprovació. Es calculen els valors corresponents a $n = 1$ dels membres de la dreta (D) i de l'esquerra (E) de la igualtat i es comprova que coincideixen. En efecte, $E = \displaystyle\sum_{j=1}^{1} j^3 = 1^3 = 1$ i, substituint $n = 1$ a $D = \dfrac{n^2(n+1)^2}{4}$, resulta $D = \dfrac{1^2(1+1)^2}{4} = 1$. Queda demostrada la igualtat i, per tant, $P(1)$.

ii) *Pas inductiu*. Hem de provar $P(n) \Rightarrow P(n+1)$, per a $n \geq 1$. Suposem, doncs, que $P(n)$ es compleix (HI, hipòtesi d'inducció) i provem $P(n+1)$. Explícitament, cal provar la implicació ($n \geq 1$):

$$\sum_{j=1}^{n} j^3 = \frac{n^2(n+1)^2}{4} \Rightarrow \sum_{j=1}^{n+1} j^3 = \frac{(n+1)^2((n+1)+1)^2}{4}$$

Expressem $\displaystyle\sum_{j=1}^{n+1} j^3 = \sum_{j=1}^{n} j^3 + (n+1)^3$ i apliquem la HI (hipòtesi d'inducció) substituint a l'expressió anterior:

$$\sum_{j=1}^{n+1} j^3 = \sum_{j=1}^{n} j^3 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3.$$

Ara només cal provar que el membre de la dreta coincideix amb

$$\frac{(n+1)^2((n+1)+1)^2}{4} = \frac{(n+1)^2(n+2)^2}{4}.$$

És una comprovació rutinària:

$$\frac{n^2(n+1)^2}{4} + (n+1)^3 = (n+1)^2(\frac{n^2}{4} + (n+1)) = (n+1)^2(\frac{n^2+4n+4}{4}) =$$
$$= \frac{(n+1)^2(n+2)^2}{4}.$$

b) $$\sum_{j=2}^{n+1}((4j)^3+1) = \sum_{j=2}^{n+1}(4j)^3 + \sum_{j=2}^{n+1}1 = \sum_{j=2}^{n+1}(4^3 j^3) + ((n+1)-2+1) =$$
$$= 4^3\sum_{j=2}^{n+1}(j^3) + n = 4^3(\frac{(n+1)^2(n+2)^2}{4} - 1^3) + n.$$

PROBLEMA 3.4

Si $n \geq 1$ és un nombre natural, demostreu:

$$1+4+7+\cdots+(3k-2)+\cdots+(3n-2) = \frac{1}{2}(3n^2-n)$$

a) Per inducció.

b) Sense utilitzar el mètode d'inducció.

Expliciteu-ne detalladament tots els passos.

Solució

a) La propietat que es vol demostrar és:

$$P(n): \quad \sum_{k=1}^{n}(3k-2) = \frac{1}{2}(3n^2-n), \quad n \geqslant 1$$

Pas base: Provem $P(1)$ comprovant que el membre de la dreta (D) i el de l'esquerra (E) de la igualtat anterior coincideixen en substituir n per 1:

$$E = \sum_{k=1}^{1}(3k-2) = 3\cdot 1 - 2 = 1 \qquad D = \frac{1}{2}(3\cdot 1^2 - 1) = 1$$

Per tant, $E = D$.

Pas inductiu: Cal provar $P(n) \Rightarrow P(n+1)$, $\forall n \geqslant 1$, és a dir:

$$\sum_{k=1}^{n}(3k-2) = \frac{1}{2}(3n^2-n) \Rightarrow \sum_{k=1}^{n+1}(3k-2) = \frac{1}{2}(3(n+1)^2-(n+1))$$

Suposem, doncs, que la propietat és certa per a n, és a dir, $P(n)$ és cert (HI), és a dir, $\sum_{k=1}^{n}(3k-2) = \frac{1}{2}(3n^2-n)$, i hem de provar que

$$\sum_{k=1}^{n+1}(3k-2) = \frac{1}{2}(3(n+1)^2-(n+1)).$$

Desenvolupem adequadament per a poder aplicar la HI (hipòtesi d'inducció):

$$\sum_{k=1}^{n+1}(3k-2) = \sum_{k=1}^{n}(3k-2) + (3(n+1)-2) \overset{\text{HI}}{=} \frac{1}{2}(3n^2-n) + (3(n+1)-2)$$

Fent els càlculs:

$$\sum_{k=1}^{n+1}(3k-2) = \frac{3n^2+5n+2}{2} = \frac{1}{2}(3(n+1)^2-(n+1))$$

Aquesta darrera igualtat es pot veure sense cap problema desenvolupant $3(n+1)^2-(n+1)$.

b) Podem utilitzar $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$:

$$\begin{aligned}\sum_{k=1}^{n}(3k-2) &= \sum_{k=1}^{n}3k - \sum_{k=1}^{n}2 = 3\sum_{k=1}^{n}k - \sum_{k=1}^{n}2 = 3\frac{n(n+1)}{2} - 2n = \\ &= \frac{3n^2+3n-4n}{2} = \frac{1}{2}(3n^2-n)\end{aligned}$$

Observació: També es pot resoldre per progressions aritmètiques: amb la fórmula $\sum_{i=1}^{n} a_i = n\frac{a_1+a_n}{2} = n\frac{1+(3n-2)}{2} = \frac{3n^2-n}{2}$.

PROBLEMA 3.5

Sigui $a_n = 2^n+1$, $n \geq 1$. *Calculeu:* $\sum_{i=10}^{2000} a_i$

Solució. Volem calcular $\sum_{i=10}^{2000} a_i$. Tenint en compte que el "sumatori d'una suma és suma de sumatoris":

$$\sum_{i=10}^{2000} a_i = \sum_{i=10}^{2000}\left(2^i+1\right) = \sum_{i=10}^{2000} 2^i + \sum_{i=10}^{2000} 1$$

Sumem separadament (i després substituirem).

$$\sum_{i=10}^{2000} 1 = 2000 - 10 + 1$$

A partir de la fórmula de la suma d'una progressió geomètrica

$$\sum_{k=0}^{n} 2^k = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$$

podem escriure

$$\sum_{i=10}^{2000} 2^i = \sum_{i=0}^{2000} 2^i - \sum_{i=0}^{9} 2^i = (2^{2001} - 1) - (2^{10} - 1) = 2^{2001} - 2^{10}$$

Finalment:

$$\sum_{i=10}^{2000} a_i = \sum_{i=10}^{2000} 2^i + \sum_{i=10}^{2000} 1 = 2^{2001} - 2^{10} + 2000 - 10 + 1$$

PROBLEMA 3.6

a) Demostreu per inducció que

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}, \textit{ per a tot nombre natural } n,\ n \geq 1.$$

b) Demostreu la igualtat anterior a partir de la igualtat:

$$\frac{1}{k} - \frac{1}{k+1} = \frac{1}{k(k+1)},\ k \geq 1.$$

c) Calculeu:

$$\sum_{k=2}^{n} (5\frac{1}{k(k+1)} + k + 3),\ \textit{on } n \in \mathbb{N}, n \geq 2$$

Solució

a) La propietat $P(n)$ és la igualtat

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1} \qquad n \geqslant 1$$

O bé:
$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$$

Pas base: Provem $P(1)$. En aquest cas, a l'esquerra tenim

$$E=\sum_{k=1}^{1}\frac{1}{k(k+1)}=\frac{1}{1(1+1)}=\frac{1}{2}.$$

I, a la dreta, $D=\dfrac{1}{1+1}=\dfrac{1}{2}$. Per tant, $E=D$, d'on resulta que $P(1)$ és cert.

Pas inductiu: Hem de demostrar $P(n)\Rightarrow P(n+1),\quad \forall n\geqslant 1$. Equivalentment:

$$\sum_{k=1}^{n}\frac{1}{k(k+1)}=\frac{n}{n+1}\Rightarrow\sum_{k=1}^{n+1}\frac{1}{k(k+1)}=\frac{n+1}{(n+1)+1}$$

Observem que suposar que $P(n)$ és cert és la hipòtesi d'inducció, *HI*. En aquest supòsit, vegem que $P(n+1)$ és cert:

$$\begin{aligned}\sum_{k=1}^{n+1}\frac{1}{k(k+1)}&=\sum_{k=1}^{n}\frac{1}{k(k+1)}+\frac{1}{(n+1)(n+2)}\overset{(HI)}{=}\frac{n}{n+1}+\frac{1}{(n+1)(n+2)}=\\&=\frac{1}{n+1}\left(n+\frac{1}{n+2}\right)=\frac{1}{n+1}\frac{n(n+2)+1}{n+2}=\\&=\frac{1}{n+1}\frac{n^2+2n+1}{n+2}=\frac{(n+1)^2}{(n+1)(n+2)}=\frac{n+1}{n+2}\end{aligned}$$

b) És una comprovació rutinària que $\dfrac{1}{k}-\dfrac{1}{k+1}=\dfrac{1}{k(k+1)}$.

Escrivint el sumatori corresponent, es produeixen simplificacions en cadena:

$$\begin{aligned}\sum_{k=1}^{n}\frac{1}{k(k+1)}&=\sum_{k=1}^{n}(\frac{1}{k}-\frac{1}{k+1})=\\&=(\frac{1}{1}-\frac{1}{2})+(\frac{1}{2}-\frac{1}{3})+(\frac{1}{3}-\frac{1}{4})+(\frac{1}{4}-\frac{1}{5})+\cdots+\\&+(\frac{1}{n-2}-\frac{1}{n-1})+(\frac{1}{n-1}-\frac{1}{n})+(\frac{1}{n}-\frac{1}{n+1})=\\&=1-\frac{1}{n+1}=\frac{n}{n+1}.\end{aligned}$$

c)
$$S=\sum_{k=2}^{n}(5\frac{1}{k(k+1)}+k+3)=5\sum_{k=2}^{n}\frac{1}{k(k+1)}+\sum_{k=2}^{n}k+\sum_{k=2}^{n}3$$

Calculem separadament:

$$\alpha=\sum_{k=2}^{n}\frac{1}{k(k+1)}=\sum_{k=1}^{n}\frac{1}{k(k+1)}-\sum_{k=1}^{1}\frac{1}{k(k+1)}\overset{\text{a)}}{=}\frac{n}{n+1}-\frac{1}{2}$$

$$\beta = \sum_{k=2}^{n} k = \sum_{k=1}^{n} k - \sum_{k=1}^{1} k = \sum_{k=1}^{n} k - 1 = \frac{n(n+1)}{2} - 1$$

$$\gamma = \sum_{k=2}^{n} 3 = 3\sum_{k=2}^{n} 1 = 3((n-2)+1)$$

Finalment:

$$S = 5\alpha + \beta + \gamma = \frac{5n}{n+1} - \frac{5}{2} + \frac{n(n+1)}{2} - 1 + 3(n-1)$$

PROBLEMA 3.7

Contesteu **raonadament** *les preguntes següents:*

a) Demostreu per inducció

$$\sum_{k=1}^{n} (2k-1)3^k = (n-1)3^{n+1} + 3, \qquad , \forall n \in \mathbb{N}, n \geq 1.$$

b) Calculeu directament $\sum_{k=1}^{n} k3^k, \forall n \in \mathbb{N}, n \geq 1$ *(utilitzeu el resultat anterior).*

Solució

a) Per inducció sobre n. Aquí $n_0 = 1$. La propietat $P(n)$ que es vol demostrar és:

$$\sum_{k=1}^{n} (2k-1)3^k = (n-1)3^{n+1} + 3$$

Pas base: Demostrem $P(n_0)$, és a dir, $P(1)$. El membre de l'esquerra de la igualtat per a $n = 1$ és:

$$E \overset{n=1}{=} \sum_{k=1}^{1} (2k-1)3^k = (2 \cdot 1 - 1)3^1$$

El membre de la dreta:

$$D \overset{n=1}{=} (1-1)3^{1+1} + 3 = 3. \quad \text{Coincideixen.}$$

Pas inductiu: Cal provar $P(n) \Rightarrow P(n+1), \qquad n \geq 1.$

És a dir, que si es compleix el següent (hipòtesi d'inducció, HI):

$$\sum_{k=1}^{n} (2k-1)3^k = (n-1)3^{n+1} + 3,$$

també es compleix:

$$\sum_{k=1}^{n+1}(2k-1)3^k = ((n+1)-1)3^{(n+1)+1}+3,$$

és a dir:

$$\sum_{k=1}^{n+1}(2k-1)3^k = n3^{n+2}+3$$

Vegem-ho:

Reescrivim:

$$\sum_{k=1}^{n+1}(2k-1)3^k$$

de manera que es pugui aplicar la HI (fent aparèixer com a subfórmula la fórmula de la HI):

$$\sum_{k=1}^{n+1}(2k-1)3^k = \sum_{k=1}^{n}(2k-1)3^k + (2(n+1)-1)3^{n+1} \overset{HI}{=}$$

$$\overset{HI}{=} ((n-1)3^{n+1}+3)+(2(n+1)-1)3^{n+1} = (n-1)3^{n+1}+3+(2n+1)3^{n+1} =$$

$$= 3^{n+1}(n-1+2n+1)+3 = n3\cdot 3^{n+1}+3 = n3^{n+1+1}+3 = n3^{n+2}+3$$

b) Vegem com es pot relacionar amb el resultat anterior.

$$\sum_{k=1}^{n}(2k-1)3^k = \sum_{k=1}^{n}2k3^k - \sum_{k=1}^{n}3^k = 2(\sum_{k=1}^{n}k3^k) - \sum_{k=1}^{n}3^k$$

Per tant:

$$2\sum_{k=1}^{n}k3^k = \sum_{k=1}^{n}(2k-1)3^k + \sum_{k=1}^{n}3^k = ((n-1)3^{n+1}+3)+\sum_{k=1}^{n}3^k$$

d'on:

$$\sum_{k=1}^{n}k3^k = \frac{1}{2}[((n-1)3^{n+1}+3)+\sum_{k=1}^{n}3^k]$$

Només resta sumar $\sum_{k=1}^{n}3^k$, suma del tipus:

$$1+x+x^2+\cdots+x^n = \frac{1-x^{n+1}}{1-x} \text{ (progressió geomètrica, amb } x=3).$$

Per tant, $\sum_{k=1}^{n}3^k = (\sum_{k=0}^{n}3^k)-3^0 = (\sum_{k=0}^{n}3^k)-1 = \dfrac{1-3^{n+1}}{1-3}-1$

Finalment:

$$\sum_{k=1}^{n} k3^k = \frac{1}{2}[(n-1)3^{n+1} + 3 + \frac{1-3^{n+1}}{-2} - 1].$$

PROBLEMA 3.8

a) *Demostreu per inducció que, per a tot $n \in \mathbb{N}, n \geq 1$:*

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

b) *Calculeu:*

$$\sum_{k=3}^{n} (6^k - 4k^2 - 5), n \geq 3, n \in \mathbb{N}$$

Solució

a) La propietat $P(n)$ que es vol demostrar per inducció és la igualtat:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

El valor més petit de n per al qual s'afirma la propietat és $n_0 = 1$. Hem de seguir els dos passos:

i) **Pas base.** Demostració de $P(n_0)$, és a dir, de $P(1)$. Vegem que els dos membres de $P(n)$ coincideixen per a $n = n_0 = 1$. Calculem separadament el membre de l'esquerra (E) i el de la dreta (D).

$$E \overset{n=1}{=} \sum_{k=1}^{1} k^2 = 1^2 = 1$$

$$D \overset{n=1}{=} \frac{1(1+1)(2 \cdot 1+1)}{6} = \frac{6}{6} = 1.$$

Per tant, $E = D$.

ii) **Pas inductiu.** Cal provar que

$$P(n) \Rightarrow P(n+1), \ \forall n \geq 1.$$

És a dir, que suposant certa $P(n)$ (hipòtesi d'inducció, HI), hem de veure que $P(n+1)$ és certa. O bé, concretant:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \Rightarrow \sum_{k=1}^{n+1} k^2 = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$$

Reescrivim $\sum_{k=1}^{n+1} k^2$ de manera que hi aparegui com a subfórmula $\sum_{k=1}^{n} k^2$ i s'hi pugui aplicar la HI, substituint la subfórmula per $\frac{n(n+1)(2n+1)}{6}$:

$$\sum_{k=1}^{n+1} k^2 = \left(\sum_{k=1}^{n} k^2\right) + (n+1)^2 \overset{HI}{=} \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

Ara, mitjançant desenvolupaments rutinaris, hem de provar que l'expressió de la dreta és igual a $\dfrac{(n+1)(n+2)(2n+3)}{6}$.

En efecte:

$$\begin{aligned}
\frac{n(n+1)(2n+1)}{6} + (n+1)^2 &= (n+1)\left[\frac{n(2n+1)}{6} + (n+1)\right] \\
&= (n+1)\left[\frac{n(2n+1)+6(n+1)}{6}\right] = \\
&= \frac{n+1}{6}(2n^2+7n+6)
\end{aligned}$$

Però també $(n+2)(2n+3) = 2n^2+7n+6$. Queda provada, doncs, la igualtat buscada.

b)
$$\sum_{k=3}^{n} (6^k - 4k^2 - 5) = \left(\sum_{k=3}^{n} 6^k\right) - \left(\sum_{k=3}^{n} 4k^2\right) - \left(\sum_{k=3}^{n} 5\right)$$

Calculem per separat els sumands de la fórmula anterior. $\alpha = \sum_{k=3}^{n} 6^k$ és un cas particular de $1+x+x^2+\cdots+x^n$, amb $x=6$, per a la qual disposem de la fórmula:

$$1+x+x^2+\ldots+x^n = \frac{x^{n+1}-1}{x-1}, \quad x \neq 1$$

Adaptada al nostre cas, en què $k \geq 3$, és

$$\alpha = \sum_{k=3}^{n} 6^k = \left(\sum_{k=0}^{n} 6^k\right) - (1+6+6^2) = \frac{6^{n+1}-1}{6-1} - (1+6+6^2) = \frac{6^{n+1}-216}{5}$$

$$\beta = \sum_{k=3}^{n} 4k^2 = 4\left(\sum_{k=3}^{n} k^2\right)$$

i ara apliquem la fórmula deduïda a l'apartat (a).

$$\begin{aligned}
\sum_{k=3}^{n} k^2 &= \left(\sum_{k=1}^{n} k^2\right) - (1^2+2^2) \\
&= \frac{n(n+1)(2n+1)}{6} - (1+4) = \frac{n(n+1)(2n+1)-30}{6},
\end{aligned}$$

d'on $\beta = 4\dfrac{n(n+1)(2n+1)-30}{6}$.

$$\gamma = \sum_{k=3}^{n} 5 = 5 \sum_{k=3}^{n} 1 = 5((n-3)+1) = 5(n-2)$$

Substituint:

$$\sum_{k=3}^{n} (6^k - 4k^2 - 5) = \alpha - \beta - \gamma.$$

Observació. En alguns dels desenvolupaments anteriors, es pot procedir diferentment. Per exemple, $\alpha = \sum_{k=3}^{n} 6^k = \left(\sum_{k=0}^{n} 6^k\right) - (1+6+6^2) = \cdots$ es pot escriure de manera més sistemàtica:

$$\alpha = \sum_{k=3}^{n} 6^k = \left(\sum_{k=0}^{n} 6^k\right) - (\sum_{k=0}^{2} 6^k),$$

i fer servir la fórmula sumatòria per als dos sumatoris:

$$\alpha = \sum_{k=3}^{n} 6^k = \left(\sum_{k=0}^{n} 6^k\right) - (\sum_{k=0}^{2} 6^k) = \frac{6^{n+1}-1}{6-1} - \frac{6^{2+1}-1}{6-1}.$$

PROBLEMA 3.9

Sigui n un nombre natural qualsevol, amb $n \geq 2$. Calculeu:

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

Solució. Es pot resoldre de diverses maneres.

Mètode 1. Com a suma d'una progressió aritmètica, amb $a_1 = 9$, $a_n = 2(n^2+1)+1$, $d = 2$ (diferència).

Mètode 2. Escrivint el sumatori com a suma de sumatoris:

$$\sum_{k=4}^{n^2+1} (2k+1) = \sum_{k=4}^{n^2+1} 2k + \sum_{k=4}^{n^2+1} 1 = \alpha + \beta,$$

on $\alpha = \sum_{k=4}^{n^2+1} 2k$, $\beta = \sum_{k=4}^{n^2+1} 1$, que es calcularan separadament:

$$\alpha = \sum_{k=4}^{n^2+1} 2k = 2\sum_{k=4}^{n^2+1} k = 2(\sum_{k=1}^{n^2+1} k - \sum_{k=1}^{3} k) = 2(\frac{(n^2+1)((n^2+1)+1)}{2} - (1+2+3)),$$

aplicant el resultat $\sum_{k=1}^{m} k = \frac{m(m+1)}{2}$. Més sistemàticament, també es pot aplicar la fórmula $\sum_{k=1}^{3} k = \frac{3(3+1)}{2}$, en comptes de la suma $1+2+3$.

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

PROBLEMA 3.10

Sigui n un nombre natural, $n \geq 2$. Calculeu:

$$\sum_{k=3}^{n^2} (2^{k+1} + 10k - (-1)^k - 5)$$

Solució. Escrivim el sumatori com a suma de sumatoris:

$$S = \sum_{k=3}^{n^2} (2^{k+1} + 10k - (-1)^k - 5) = \sum_{k=3}^{n^2} 2^{k+1} + \sum_{k=3}^{n^2} 10k - \sum_{k=3}^{n^2} (-1)^k - \sum_{k=3}^{n^2} 5$$

Calcularem separadament cada sumatori.

Càlcul de $\alpha = \sum_{k=3}^{n^2} 2^{k+1}$:

En primer lloc,

$$\alpha = \sum_{k=3}^{n^2} 2^{k+1} = \sum_{k=3}^{n^2} 2 \cdot 2^k = 2\sum_{k=3}^{n^2} 2^k$$

Adaptarem la fórmula bàsica (suma dels m primers termes de la progressió geomètrica):

$$1 + x + x^2 + \cdots + x^m = \sum_{k=0}^{m} x^k = \frac{(x^{m+1} - 1)}{(x-1)}, x \in \mathbb{R}, x \neq 1,$$

amb $x = 2$ i $m = n^2$:

$$\sum_{k=3}^{n^2} 2^k = \sum_{k=0}^{n^2} 2^k - \sum_{k=0}^{2} 2^k = \sum_{k=0}^{n^2} 2^k - (2^0 + 2^1 + 2^2) = \frac{2^{(n^2+1)} - 1}{2-1} - 7 = 2^{n^2+1} - 8.$$

Per tant, $\alpha = 2(2^{n^2+1} - 8) = 2^{n^2+2} - 16$.

Càlcul de $\beta = \sum_{k=3}^{n^2} 10k$:

$$\beta = \sum_{k=3}^{n^2} 10k = 10\sum_{k=3}^{n^2} k$$

Adaptarem la fórmula bàsica $\sum_{j=1}^{m} j = \frac{m(m+1)}{2}$:

$$\sum_{k=3}^{n^2} k = \sum_{k=1}^{n^2} k - (\sum_{k=1}^{2} k) = \sum_{k=1}^{n^2} k - (1+2) = \frac{n^2(n^2+1)}{2} - 3 = \frac{n^2(n^2+1)-6}{2}$$

Per tant:

$$\beta = 10\sum_{k=1}^{n^2} k = 10\left(\frac{n^2(n^2+1)-6}{2}\right) = 5(n^2(n^2+1)-6) = 5n^4+5n^2-30.$$

Càlcul de $\gamma = \sum_{k=3}^{n^2}(-1)^k$:

És un cas particular de la fórmula anterior (progressió geomètrica), amb $x=-1$ i $m=n^2$. Així:

$$\begin{aligned}
\gamma &= \sum_{k=3}^{n^2}(-1)^k = \sum_{k=0}^{n^2}(-1)^k - \sum_{k=0}^{2}(-1)^k = \\
&= \sum_{k=0}^{n^2}(-1)^k - ((-1)^0+(-1)^1+(-1)^2) = \frac{(-1)^{n^2+1}-1}{(-1)-1} - (1-1+1) = \\
&= -\frac{(-1)^{n^2+1}-1}{2} - 1 = \frac{(-1)^{n^2+2}+1-2}{2} = \frac{(-1)^{n^2+2}-1}{2} = \frac{(-1)^{n^2}-1}{2}.
\end{aligned}$$

Càlcul de $\delta = \sum_{k=3}^{n^2} 5$:

El nombre de sumands és $(n^2-3)+1 = n^2-2$. Per tant:

$$\delta = \sum_{k=3}^{n^2} 5 = 5(n^2-2) = 5n^2-10.$$

Finalment, substituint:

$$\begin{aligned}
S &= (2^{n^2+2}-16)+(5n^4+5n^2-30) - \frac{(-1)^{n^2}-1}{2} - 5n^2+10 = \\
&= 2^{n^2+2}+5n^4+\frac{(-1)^{n^2+1}+1}{2} - 36.
\end{aligned}$$

PROBLEMA 3.11

a) Demostreu per inducció que, per a tot $n \in \mathbb{N}, n \geq 1$*:* $\sum_{k=1}^{n}(4k+1) = n(2n+3)$

b) Demostreu la igualtat anterior sense utilitzar el mètode d'inducció.

Solució

a) Per inducció sobre n. La propietat que s'ha de demostrar és:

$$P(n): \sum_{k=1}^{n}(4k+1) = n(2n+3), \text{ amb } n_0 = 1$$

Pas base. Provem $P(n_0)$, és a dir, $P(1)$. Comprovem que els membres de la dreta $D(1)$ i de l'esquerra $E(1)$ coincideixen:

$$E(1) \stackrel{(n=1)}{=} \sum_{k=1}^{1}(4k+1) = 4\cdot 1+1 = 5$$
$$D(1) \stackrel{(n=1)}{=} 1\cdot(2\cdot 1+3) = 5$$

Tenim $E(1) = D(1)$ i, per tant, $P(1)$ és cert.

Pas inductiu. Cal provar la implicació

$$P(n) \Rightarrow P(n+1), \forall n \geq 1$$

És a dir, cal provar:

$$\sum_{k=1}^{n}(4k+1) = n(2n+3) \Rightarrow \sum_{k=1}^{n+1}(4k+1) = (n+1)(2(n+1)+3)$$

En efecte:

$$\sum_{k=1}^{n+1}(4k+1) = (\sum_{k=1}^{n}(4k+1)) + (4(n+1)+1) \stackrel{(HI)}{=} n(2n+3) + (4(n+1)+1)$$

Desenvolupem els termes respectius de la dreta de les dues últimes igualtats per a comprovar que coincideixen:

$$\begin{aligned} (n+1)(2(n+1)+3) &= 2(n+1)^2 + 3(n+1) = 2(n^2+2n+1) + 3n + 3 = \\ &= 2n^2 + 7n + 5 \\ n(2n+3) + 4(n+1) + 1 &= 2n^2 + 3n + 4n + 5 = 2n^2 + 7n + 5 \end{aligned}$$

b)
$$\begin{aligned} \sum_{k=1}^{n}(4k+1) &= \sum_{k=1}^{n}4k + \sum_{k=1}^{n}1 = (4\sum_{k=1}^{n}k) + \sum_{k=1}^{n}1 = \\ &= 4\frac{n(n+1)}{2} + n = 2n(n+1) + n = n(2n+3). \end{aligned}$$

PROBLEMA 3.12

Si $n \in \mathbb{N}$, $n \geq 2$, calculeu:

$$\sum_{k=2}^{n^3-1}(-5k+(-6)^{k+12}\log_2 3+1)$$

Solució. Descomponem la suma

$$S=\sum_{k=2}^{n^3-1}(-5k+(-6)^{k+12}\log_2 3+1)$$

en $S=\alpha+\beta+\gamma$, on

$$\alpha=\sum_{k=2}^{n^3-1}(-5k),$$

$$\beta=\sum_{k=2}^{n^3-1}(-6)^{k+12}\log_2 3,$$

$$\gamma=\sum_{k=2}^{n^3-1}1$$

que calculem separadament i finalment sumem.

Càlcul de α:

$$\alpha=(-5)\sum_{k=2}^{n^3-1}k=(-5)(\sum_{k=1}^{n^3-1}k-\sum_{k=1}^{1}k)=(-5)(\sum_{k=1}^{n^3-1}k-1)$$

Apliquem

$$\sum_{i=1}^{m}i=\frac{m(m+1)}{2}$$

$$\alpha=(-5)(\frac{1}{2}(n^3-1)((n^3-1)+1)-1)=(-5)(\frac{1}{2}(n^3-1)n^3-1)$$

Càlcul de β:

$$\beta=\sum_{k=2}^{n^3-1}(-6)^{12}\log_2 3(-6)^k=(-6)^{12}\log_2 3\sum_{k=2}^{n^3-1}(-6)^k$$

Per a sumar $\sum_{k=2}^{n^3-1}(-6)^k$, utilitzem $1+x+x^2+\cdots+x^n=\frac{1-x^{m+1}}{1-x}$, amb $x=-6$:

$$\sum_{k=2}^{n^3-1}(-6)^k=\sum_{k=0}^{n^3-1}(-6)^k-((-6)^0+(-6^1))=\frac{1-(-6)^{(n^3-1)+1}}{1-(-6)}-(1-6)$$

Càlcul de γ:

$$\gamma = \sum_{k=2}^{n^3-1} 1 = (n^3 - 1) - 2 + 1 = n^3 - 2$$

PROBLEMA 3.13

Sigui n un nombre natural, $n \geq 1$. Calculeu:

$$\sum_{k=4}^{2n+6} (7k + 5(-2)^{k+3} - \lfloor n \rfloor)$$

Solució. Denotem $S = \sum_{k=4}^{2n+6} (7k + 5(-2)^{k+3} - \lfloor n \rfloor)$.

Escrivim S com a suma de sumatoris, que calculem separadament:

$$S = \sum_{k=4}^{2n+6} (7k) + \sum_{k=4}^{2n+6} 5(-2)^{k+3} - \sum_{k=4}^{2n+6} \lfloor n \rfloor$$

Denotem:

$$\alpha = \sum_{k=4}^{2n+6} (7k),\ \beta = \sum_{k=4}^{2n+6} 5(-2)^{k+3},\ \gamma = \sum_{k=4}^{2n+6} \lfloor n \rfloor$$

Càlcul de α:

$$\alpha = 7 \sum_{k=4}^{2n+6} k.$$

Utilitzem $\sum_{i=1}^{m} i = \frac{m(m+1)}{2}$. En aquest cas:

$$\sum_{k=4}^{2n+6} k = (\sum_{k=1}^{2n+6} k) - (\sum_{k=1}^{3} k) = \frac{(2n+6)((2n+6)+1)}{2} - (1+2+3) = \frac{(2n+6)(2n+7) - 12}{2}$$

Així, $\alpha = 7 \frac{(2n+6)(2n+7) - 12}{2}$.

Càlcul de β:

$$\beta = \sum_{k=4}^{2n+6} 5(-2)^3(-2)^k = -5 \cdot 8 \sum_{k=4}^{2n+6} (-2)^k$$

Utilitzem $\sum_{k=0}^{m} x^k = \frac{1 - x^{m+1}}{1 - x}$ per a $x = -2$.

$$\begin{aligned}
\sum_{k=4}^{2n+6}(-2)^k &= \sum_{k=0}^{2n+6}(-2)^k - \sum_{k=0}^{3}(-2)^k = \\
&= \frac{1-(-2)^{2n+6+1}}{1-(-2)} - ((-2)^0+(-2)+(-2)^2+(-2)^3) = \\
&= \frac{1-(-2)^{2n+6+1}}{3} - (1-2+4-8) = \frac{1-(-2)^{2n+7}}{3} + 5 = \\
&= \frac{1-(-2)^{2n+7}+15}{3}
\end{aligned}$$

Per tant:

$$\beta = 5\cdot 8\frac{(-2)^{2n+7}-16}{3}$$

Càlcul de γ:

$$\gamma = \sum_{k=4}^{2n+6}\lfloor n\rfloor.$$

En aquesta fórmula l'índex de variació és k i $\lfloor n\rfloor$ actua com a constant dins del sumatori. Per tant,

$$\gamma = \lfloor n\rfloor\sum_{k=4}^{2n+6}1 = \lfloor n\rfloor((2n+6)-4+1) = \lfloor n\rfloor(2n+3) = n(2n+3).$$

Finalment:

$$S = \alpha+\beta-\gamma = 7\frac{(2n+6)(2n+7)-12}{2} + 5\cdot 8\frac{(-2)^{2n+7}-16}{3} - n(2n+3)$$

Variant de resolució: Observem que el sumatori $\sum_{k=4}^{2n+6}k$ és la suma de termes consecutius d'una progressió aritmètica, de terme general a_i, on el sumatori consta de $m=(2n+6)-4+1=2n+3$ sumands; aplicant la fórmula que ens permet calcular directament aquesta suma, resulta: $\sum_{k=4}^{2n+6}k = \frac{[4+(2n+6)](2n+3)}{2}$. Fórmula de la suma: $\frac{(a_1+a_m)m}{2}$.

Observem que el sumatori $\sum_{k=4}^{2n+6}(-2)^k$ és la suma de termes consecutius d'una progressió geomètrica, de terme general a_i, de raó $r=-2$, on el sumatori consta de $m=(2n+6)-4+1=2n+3$ sumands; aplicant la fórmula que ens permet calcular directament aquesta suma resulta: $\sum_{k=4}^{2n+6}(-2)^k = \frac{(-2)^{2n+6}\cdot(-2)-(-2)^4}{(-2)-1}$. Fórmula de la suma: $\frac{a_m r - a_1}{r-1}$.

PROBLEMA 3.14

Sigui $A=(a_{ij})$ una matriu de m files i n columnes en què l'element situat a la fila i i columna j és $a_{ij}=2i+j$. Calculeu la suma dels elements de A.

Solució. Si S és la suma dels elements de A, és:

$$S=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}$$

Tenim $S=\sum_{i=1}^{m}(\sum_{j=1}^{n}(2i+j))$.

Calculem separadament $S_1=\sum_{j=1}^{n}(2i+j)$.

Atès que $\sum_{k=1}^{p}(a_k+b_k)=(\sum_{k=1}^{p}a_k)+(\sum_{k=1}^{p}b_k)$, és:

$$S_1=\sum_{j=1}^{n}(2i+j)=(\sum_{j=1}^{n}2i)+(\sum_{j=1}^{n}j)=2i\sum_{j=1}^{n}1+\sum_{j=1}^{n}j=2in+\frac{n(n+1)}{2};$$

És $\sum_{j=1}^{n}j=\frac{n(n+1)}{2}$, com a suma dels n primers elements de la progressió aritmètica de primer element $a_1=1$ i raó 1 (també es pot obtenir per altres mètodes).

Substituint:

$$\begin{aligned}S &= \sum_{i=1}^{m}(2in+\frac{n(n+1)}{2})=\sum_{i=1}^{m}2in+\sum_{i=1}^{m}\frac{n(n+1)}{2}=\\ &= 2n(\sum_{i=1}^{m}i)+\frac{n(n+1)}{2}\sum_{i=1}^{m}1=2n\frac{m(m+1)}{2}+\frac{n(n+1)}{2}m=\frac{nm}{2}(2m+n+3)\end{aligned}$$

Observació. També es pot procedir en ordre invers:

$$\sum_{j=1}^{n}\sum_{i=1}^{m}a_{ij}=\sum_{j=1}^{n}(\sum_{i=1}^{m}a_{ij})$$

El resultat és el mateix.

PROBLEMA 3.15

Sigui n un nombre natural, $n\geq 1$. Calculeu:

$$\sum_{k=4}^{n+7}(8k+7(-2)^{k+3}-4n)$$

Solució. Descomponem el sumatori

$$S=\sum_{k=4}^{n+7}(8k+7(-2)^{k+3}-4n)$$

en suma de sumatoris: $S = \alpha + \beta + \gamma$, on

$$\alpha = \sum_{k=4}^{n+7} 8k, \quad \beta = \sum_{k=4}^{n+7} 7(-2)^{k+3}, \quad \gamma = \sum_{k=4}^{n+7} (-4n),$$

que calculem separadament.

Càlcul de α: En primer lloc, $\alpha = \sum_{k=4}^{n+7} 8k = 8\sum_{k=4}^{n+7} k$

Mètode 1. $\sum_{k=4}^{n+7} k$ es pot sumar com a progressió aritmètica, de primer terme $a_1 = 4$, diferència $d = 1$, amb $p = (n+7) - 4 + 1 = n+4$ sumands i últim terme $a_p = n+7$.

Per tant, $\sum_{k=4}^{n+7} k = \dfrac{(a_1 + a_p)p}{2} = \dfrac{(4+(n+7))(n+4)}{2} = \dfrac{n^2+15n+44}{2}$.

Mètode 2. Recordant que $\sum_{k=1}^{m} k = \dfrac{m(m+1)}{2}$ (demostrable per inducció, o bé com a cas particular de progressió aritmètica, o bé per algun mètode directe, com s'ha vist anteriorment), podem escriure:

$$\begin{aligned} \sum_{k=4}^{n+7} k &= \sum_{k=1}^{n+7} k - \sum_{k=1}^{3} k = \frac{(n+7)((n+7)+1)}{2} - (\frac{3\cdot 4}{2}) = \\ &= \frac{(n+7)(n+8)}{2} - 6 = \frac{n^2+15n+44}{2} \end{aligned}$$

Per tant, $\alpha = 4(n^2+15n+44) = 4n^2+60n+176$.

Càlcul de β:

$$\beta = \sum_{k=4}^{n+7} 7(-2)^{k+3} = \sum_{k=4}^{n+7} 7(-2)^3(-2)^k = 7(-2)^3 \sum_{k=4}^{n+7} (-2)^k = -56\sum_{k=4}^{n+7} (-2)^k$$

Calculem $\sum_{k=4}^{n+7} (-2)^k$.

Mètode 1. Aplicant la fórmula de la suma dels elements d'una progressió geomètrica $a_1 + \cdots + a_p$, de primer terme a_1, últim terme a_p, raó r, nombre de termes p, segons diverses versions possibles:

$$a_1 + \cdots + a_p = \frac{a_1 - a_1 r^p}{1-r} = \frac{a_1 r^p - a_1}{r-1},$$

$$a_1 + \cdots + a_p = \frac{a_1 - a_p r}{1-r} = \frac{a_p r - a_1}{r-1}$$

amb primer terme $a_1 = (-2)^4$, raó $r = -2$, nombre de termes $p = (n+7)-4+1 = n+4$, últim terme $a_p = (-2)^{n+7}$.

Variant argumental. També es pot sumar directament: $\beta = 7\sum_{k=4}^{n+7}(-2)^{k+3}$, i aleshores cal sumar $\sum_{k=4}^{n+7}(-2)^{k+3}$; però aquesta és la suma d'una progressió geomètrica, que es descriu a continuació.

$\sum_{k=4}^{n+7}(-2)^{k+3}$, en què el primer terme és $a_1 = (-2)^{4+3}$, raó $r = -2$, nombre de termes $p = (n+7)-4+1 = n+4$, últim terme $a_p = (-2)^{n+7+3}$.

El lector hi aplicarà les substitucions de valors corresponents i en completarà els càlculs.

Mètode 2. És la suma d'una progressió geomètrica de raó $x = -2$. Apliquem

$$1+x+x^2+\cdots+x^m = \tfrac{x^{m+1}-1}{x-1},\ x \neq 1$$

En aquest cas:

$$\begin{aligned}
\sum_{k=4}^{n+7}(-2)^k &= \sum_{k=0}^{n+7}(-2)^k - \sum_{k=0}^{3}(-2)^k = \\
&= \frac{(-2)^{(n+7)+1}-1}{(-2)-1} - \frac{(-2)^{3+1}-1}{(-2)-1} = \frac{(-2)^{n+8}-1}{-3} - \frac{(-2)^4-1}{-3} = \\
&= -\frac{1}{3}[256(-2)^n - 1 - 16 + 1] = -\frac{1}{3}(256(-2)^n - 16).
\end{aligned}$$

Per tant, $\beta = \dfrac{56}{3}(256(-2)^n - 16)$.

Càlcul de γ: L'índex de variació del sumatori és k; n actua com a constant. Per tant:

$$\gamma = \sum_{k=4}^{n+7}(-4n) = (-4n)\sum_{k=4}^{n+7}1 = -4n((n+7)-4+1) = -4n(n+4) = -4n^2 - 16n.$$

Finalment, cal sumar $S = \alpha + \beta + \gamma$.

$$\begin{aligned}
S &= (4n^2+60n+176) + (\frac{56}{3}(256(-2)^n - 16)) + (-4n^2 - 16n) = \\
&= 44n + 176 + \frac{56}{3}(256(-2)^n - 16)
\end{aligned}$$

PROBLEMA 3.16

a) Demostreu per inducció: per a tot $n \in \mathbb{N}$, $n \geq 1$,

$$3 + 11 + 19 + \cdots + (8k-5) + \cdots + (8n-5) = 4n^2 - n$$

b) Demostreu el mateix resultat directament sense inducció.

Solució

a) Sigui $P(n) :=$ "$\sum_{k=1}^{n}(8k-5) = 4n^2 - n$" la propietat que volem demostrar per inducció sobre n, amb $n_0 = 1$.

Pas base. Cal provar $P(n_0)$, és a dir, $P(1)$.

El membre de la dreta per a $n_0 = 1$ val $4 \cdot 1^2 - 1 = 3$

El membre de l'esquerra per a $n_0 = 1$ val

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

Atès que coincideixen, $P(1)$ es compleix.

Pas inductiu. Cal provar la implicació $P(n) \Rightarrow P(n+1), \forall n \geq 1$. És a dir:

$$\sum_{k=1}^{n}(8k-5) = 4n^2 - n \overset{?}{\Rightarrow} \sum_{k=1}^{n+1}(8k-5) = 4(n+1)^2 - (n+1)$$

En efecte: escrivim $\sum_{k=1}^{n+1}(8k-5)$ de forma que aparegui com a subfórmula $\sum_{k=1}^{n}(8k-5)$ i puguem aplicar $P(n)$, és a dir, la hipòtesi d'inducció (HI):

$$\begin{aligned}\sum_{k=1}^{n+1}(8k-5) &= \sum_{k=1}^{n}(8k-5) + (8(n+1)-5) \overset{HI}{=\!=} (4n^2-n) + (8(n+1)-5) = \\ &= 4n^2 + 7n + 3\end{aligned}$$

Vegem que aquesta última expressió coincideix amb $4(n+1)^2 - (n+1)$. En efecte:

$$4(n+1)^2 - (n+1) = 4(n^2 + 2n + 1) - (n+1) = 4n^2 + 7n + 3.$$

b) $\displaystyle\sum_{k=1}^{n}(8k-5) = \sum_{k=1}^{n} 8k - \sum_{k=1}^{n} 5 = 8\sum_{k=1}^{n} k - 5n = 8\frac{n(n+1)}{2} - 5n = n(4n-1).$

Mètode alternatiu: com a suma dels elements d'una progressió aritmètica, amb $a_1 = 3$, $a_n = 8n-5$, terme general $a_k = 8k-5$, diferència $d = 8$. La suma seria

$$n\frac{a_1+a_n}{2} = n\frac{3+(8n-5)}{2} = n(4n-1).$$

3.10. Qüestions diverses

1. El nombre de sumands de:

a) $\displaystyle\sum_{k=n_o}^{n^3+3} a_i$ és ...

b) $\displaystyle\sum_{k=s+1}^{r+3} a_i$ és ...

c) $a_{s+5}+\ldots+a_{r+7}$ és ...

d) $\displaystyle\sum_{2\leq k\leq n} k$ és ...

2. Escriviu com a sumatori:

a) La suma dels nombres naturals múltiples de 5 menors o iguals que $n \in \mathbb{N}$.

b) La suma dels nombres naturals parells menors o iguals que $n \in \mathbb{N}$.

3. Sumeu:

a) $\displaystyle\sum_{i=s}^{r} 1,\ r \geq s.$

b) $\displaystyle\sum_{k=n_0}^{n^2+1} (-3),\ n^2+1 \geq n_0.$

c) $\displaystyle\sum_{k=6}^{n} 3\log_2 n,\ n \in \mathbb{N}, n \geq 6.$

d) $\displaystyle\sum_{k=1}^{n} \log_2(n+1),\ n \in \mathbb{N},\ n \geq 1.$

4. Sigui $n \in \mathbb{N}, n \geq 1$. És $\displaystyle\sum_{j=1}^{n^2} \frac{1}{j} =$

a) $\displaystyle\sum_{p=2}^{n^2+1} \frac{1}{p-1}$

b) $\displaystyle\sum_{p=2}^{(n+1)^2} \frac{1}{p-1}$

c) $\displaystyle\sum_{p=2}^{n^2-1} \frac{1}{p-1}$

d) $\displaystyle\sum_{p=2}^{(n-1)^2} \frac{1}{p-1}$

e) $\displaystyle\sum_{p=1}^{n^2+1} \frac{1}{p-1}$

f) Cap de les anteriors.

5. Considerem $\displaystyle\sum_{i=1}^{n} a_i \ldots$. És:

a) $a_1+\ldots+a_n$

b) $\displaystyle\sum_{1\leq i\leq n,\ i\in\mathbb{N}} a_i$

c) $\sum_{i\in\{1,\ldots,n\}} a_i$

d) $\sum_{j=1}^{n} a_j$

e) Cap de les anteriors.

6. Considerem $\sum_{i=1}^{n} n^2(i-1),\ n\in\mathbb{N},\ n\geq 1$. A l'expressió $n^2(i-1)$:

a) n té la consideració de constant pel que fa al sumatori.
b) Per a la sumació, n i i es consideren variables.
c) n^2 pot sortir fora del sumatori.
d) i pot sortir fora del sumatori.
e) Cap de les anteriors.

7. Si $n\in\mathbb{N},\ r\geq 1,\ s\geq 1, a_i,\ldots\in\mathbb{R}$, indiqueu quines de les afirmacions següents són certes.

a) $\sum_{i=1}^{rs} a_i = \sum_{i=1}^{r} a_i + \sum_{i=1}^{s} a_i$

b) $\sum_{i=1}^{rs} a_i = (\sum_{i=1}^{r} a_i)(\sum_{i=1}^{s} a_i)$

c) $\sum_{i=1}^{rs} a_i = a_1 + a_2 + \ldots + a_{rs}$

d) $\sum_{i=1}^{rs} a_i = a\sum_{i=1}^{rs} i$

e) $\sum_{i=1}^{rs} a_i = \sum_{i=1} \frac{rs}{2} a_i + \sum_{i=\frac{rs}{2}+1}^{rs} a_i$

f) Cap de les anteriors.

8. Siqui $x\in\mathbb{R}, x\neq 1, n\in\mathbb{N}, n\geq n_0\geq 0$. Indiqueu si hi ha alguna afirmació certa.

a) $\sum_{k=n_0}^{n} x^k = \sum_{k=0}^{n} x^k - \sum_{k=0}^{n_0-1} x^k$

b) $\sum_{k=n_0}^{n} x^k = \sum_{k=0}^{n} x^k - \sum_{k=0}^{n_0} x^k$

c) $\sum_{k=n_0}^{n} x^k = \dfrac{x^{n+1}-x^{n_0}}{x-1}$

d) Cap de les anteriors.

9. Escriviu els sumands de:

a) $\sum_{i=1}^{n} a_{2i} \qquad (n\geq 1)$

b) $\sum_{i=0}^{n+1} a_{3i} \qquad (n\geq 0)$

c) $\sum_{i=0}^{n} a_{2^i} \qquad (n\geq 0)$

d) $\sum_{i=1}^{n} a_{2^{(2^i)}} \qquad (n\geq 1)$

e) $\sum_{i=1}^{n} a_{(2i+1)} \qquad (n\geq 1)$

f) $\sum_{i=3}^{n^2} a_i \qquad (n\geq 2)$

10. Si $n\in\mathbb{N}, n\geq 1$ i $a_1,\ldots,a_n\in\mathbb{R}$, indiqueu si alguna de les igualtats següents és certa.

$\sum_{i=0}^{(n-1)(n+1)} a_i =$

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

b) $= (\sum_{i=0}^{n-1} a_i)(\sum_{i=0}^{n+1} a_i)$

c) $= (n-1)(n+1)\sum_{i=1}^{1} a_i$

d) $= \sum_{i=0}^{n^2-1} a_i$

e) $= a_1 + a_2 + a_3 + \ldots + a_{n-1}$

f) $= \sum_{i=0}^{n-1} a_i + \sum_{i=n}^{n^2-1} a_i$

g) Cap de les anteriors.

11. Sigui $n \in \mathbb{N}, n \geq 1$. Siguin $a_1, \ldots a_n \in \mathbb{R}$. Indiqueu quines afirmacions són certes:

a) $\sum_{i=1}^{n^2} a_i = (\sum_{i=1}^{n} a_i) + (\sum_{i=1}^{n} a_i)$

b) $\sum_{i=1}^{n^3} a_i = (\sum_{i=1}^{n} a_i) + (\sum_{i=1}^{n} a_i) + (\sum_{i=1}^{n} a_i)$

c) $\sum_{i=1}^{n} {a_i}^3 = (\sum_{i=1}^{n} a_i)^3$

d) $\sum_{i=1}^{n^3} a_i = \sum_{i=1}^{n} (a_i)^3$

e) $\sum_{i=1}^{n^3} a_i = \sum_{i=1}^{n} a_{(i^3)}$

f) Cap de les anteriors.

12. Indiqueu si són certes o no:

a) $\sum_{i=1}^{n} (3a_i + 5b_i) = 3(\sum_{i=1}^{n} a_i) + 5(\sum_{i=1}^{n} b_i)$

b) $\sum_{i=1}^{n} (4a_i) = \sum_{i=1}^{4n} a_i$

c) $\sum_{i=1}^{n} 6 \sum_{i=1}^{n+6} a_i$

d) $\sum_{i=1}^{n} 7a_i = (\sum_{i=1}^{n} 7)(\sum_{i=1}^{n} a_i)$

e) $\sum_{i=1}^{n} 8a_i = (\sum_{i=1}^{n} 8) + (\sum_{i=1}^{n} a_i)$

f) $\sum_{i=1}^{n} 7a_i = \sum_{i=1}^{n} (7 \sum_{i=1}^{n} a_i)$

g) $\sum_{i=1}^{n} (-a_2) = -\sum_{i=1}^{n} a_i$

h) $\sum_{i=1}^{n} (-1)^n a_i = (-1)^n \sum_{i=1}^{n} a_i$

i) $\sum_{i=1}^{n} (-1)^i a_i = \sum_{k=1}^{n} (-1)^k a_k$

j) $\sum_{i=1}^{n} (-1)^i a_i = (-1)^i \sum_{i=1}^{n} a_i$

k) $\sum_{i=1}^{n} (-1)^i a_i = (-1)^n \sum_{i=1}^{n} a_i$

13. Indiqueu si són certes o no:

a) $\sum_{i=1}^{n}(4a_i+9b_i)=4\sum_{j=1}^{n}a_j+9\sum_{k=1}^{n}b_k$

b) $\sum_{i=1}^{n}(4a_i-3b_i)=4\sum_{j=1}^{n-1}a_{j+1}-3\sum_{k=2}^{n+1}b_{k-1}$

c) $\sum_{i=1}^{n}(4a_i-3b_i)=4\sum_{j=0}^{n+1}a_{j+1}-3\sum_{k=2}^{n11}b_{k-1}$

d) $\sum_{i=1}^{n}(a_i+b_i)=\sum_{i=1}^{n}b_i+\sum_{i=1}^{n}a_i$

e) $(\sum_{i=1}^{n}a_i)^2=\sum_{i=1}^{n}{a_i}^2$

f) $\sum_{i=1}^{n}(a_ib_i)=(\sum_{i=1}^{n}a_i)(\sum_{i=1}^{n}b_i)$

g) $\sum_{i=1}^{n}(\frac{1}{\lambda}a_i+\frac{1}{\mu}b_i)=\frac{1}{\lambda\mu}\sum_{i=1}^{n}(\mu a_i+\lambda b_i)$

h) $\lambda\mu\sum_{i=1}^{n}(\frac{1}{\lambda}a_i+\frac{1}{\mu}b_i)=\mu(\sum_{i=1}^{n}a_i)+\lambda(\sum_{i=1}^{n}b_i)$

i) $\sum_{i\in\{1,2,\ldots,n^2\}} i=\sum_{k=1}^{n^2}k$

j) $\sum_{i\in\{1,2,\ldots,n^2\}} i\stackrel{?}{=}\sum_{k=1}^{n}k^2$

14. Calculeu:

a) $\sum_{k=15}^{2n+1}3^k.\ \ (n\geq 15).$

b) $\sum_{k=1}^{n-1}3^k.\ \ (n\geq 2).$

c) $\sum_{k=0}^{2n}3^k.\ \ (n\geq 0).$

d) $\sum_{k=0}^{2^n}3^k.\ \ (n\geq 0).$

e) $\sum_{k=0}^{n}(5^{k+1}-5^k).$

3.11. Aplicació de fórmules sumatòries per a analitzar dos algorismes elementals

L'algorisme d'ordenació per inserció no és eficient

Comentem, per exemple, l'*algorisme d'inserció* per a ordenar per ordre creixent una col·lecció $\{a_1,\cdots,a_n\}$ de n nombres (o objectes ordenables en una ordenació total). L'algorisme funciona de la manera següent:

Descripció i anàlisi (per a l'anàlisi de costos, només considerem les operacions de comparació):

a) Primeres operacions. Es considera el segon element a_2 i es compara amb el primer. Si $a_2 < a_1$, s'intercanvien a_1, a_2 i en resulta la nova llista $a_2, a_1, \ldots$, amb els dos primers elements en l'ordre correcte; es passa a considerar l'element a_3. Si $a_1 < a_2$, aleshores ja estan ordenats i no cal fer cap intercanvi; els passa a considerar l'element a_3. Comparem, per ordre, a_3 amb la subllista ordenada dels dos anteriors i, si és menor que algun d'ells, s'insereix immediatament davant seu (en aquest cas, en el cas pitjor, s'hauran de fer 2 $(= 3-1)$ comparacions. Si no s'ha de fer cap inserció, queda la subllista dels tres primers nombres ordenada i es passa a considerar l'element a_4.

b) Operació genèrica. Suposem que estem analitzant l'element j–èsim, amb $1 < j \leq n$. La subllista formada pels $j-1$ elements que té al davant ja està ordenada. Ara hem de comparar a_j amb aquests elements, ordenadament des del principi; inserim a_j davant del primer que trobem que sigui més gran que a_j o no fem res si no en trobem cap. Això obligarà, en el cas pitjor, a comparar amb tots els $j-1$ anteriors, és a dir, un cost de $j-1$ operacions.

En aquesta taula, presentem una execució de l'algorisme per a una llista concreta: 9,7,8,2,1.

Resultat	Pas	Element actiu	Comparacions
9,7,8,2,1			
7,9,8,2,1	1	7	1
7,8,9,2,1	2	8	2
2,7,8,9,1	3	2	1
1,2,7,8,9	4	1	1

Observem que és possible que no s'hagin de fer totes les comparacions previstes en el cas pitjor. Si la llista ja és ordenada (1,2,7,8,9), s'hauran de fer el màxim de comparacions possibles, i estarem en el cas pitjor.

Per tant, els costos en el cas pitjor seran: $1+2+\cdots+(j-1)+\cdots+(n-1)$.

Com és de gran $1+\cdots+n$*?*. A part de tenir una fórmula explícita que ens "alliberi dels punts suspensius", és útil també per tenir, d'aquesta manera, una avaluació de l'ordre de magnitud de $1+\cdots+n$, en termes de n, cosa que és important per tenir una idea qualitativa dels costos computacionals algorísmics: en efecte, aquesta suma és d'ordre quadràtic en n, no és lineal en n, ja que $\dfrac{n(n+1)}{2} = \dfrac{1}{2}n^2 + \dfrac{1}{2}n$, expressió on el terme dominant és n^2, que és el que compta quan n es fa molt gran.

Per tant, reprenent l'anàlisi de l'algorisme d'ordenació per inserció, el cost en el cas pitjor serà $1+2+\cdots+(j-1)+\cdots+(n-1) = \dfrac{(n-1)n}{2}$, cost quadràtic. Un bon consell: no utilitzeu aquest algorisme, és un mal algorisme ...

L'algorisme d'ordenació per selecció simple no és eficient

Un exemple addicional. Vegem que l'*algorisme d'ordenació per selecció simple* tampoc no és gaire eficient (i, per tant, atès que hi ha alternatives millors, poc recomanable).

Descripció i anàlisi de costos. L'anàlisi de costos el basarem únicament en el nombre de comparacions (el cost real seria superior, però aquesta és la part essencial, la que pot ser dominant en el cost global).

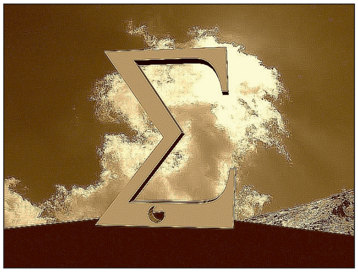
Suposem que tenim inicialment la llista d'elements $a_1, \cdots, a_n$, elements d'un conjunt amb un ordre total.

a) Obteniu el màxim *max* dels elements. Això significa efectuar una inspecció de tots els elements amb les corresponents comparacions. El nombre de comparacions és $n-1$.
b) Intercanvieu aquest valor màxim amb l'últim de la llista (és a dir, que si $max = a_{i_0}$, a partir d'ara a_n ocupa la posició i_0 i $max = a_{i_0}$ ocupa la posició n. Aquesta posició, contenint el màxim, ja no s'haurà de tornar a examinar en el que resta.
c) D'entre les posicions $1, 2, \ldots, n-1$ obtenim el màxim fent $n-2$ comparacions. S'intercanvien els valors de la posició que conté el màxim i el valor de la posició $n-1$ (que passa a contenir el valor màxim de la subllista); aquesta posició $n-1$ ja no es tornarà a considerar.
d) Es continua el procés fins que tota la llista estigui ordenada.

Per exemple, si hem d'ordenar per aquest procediment la llista 3,9,7,5,2,6, els resultats intermedis corresponents a l'execució de l'algorisme seran:

3,9,7,5,2,6
3,6,7,5,2,9
3,6,2,5,7,9
3,5,2,6,7,9
3,2,5,6,7,9
2,3,5,6,7,9

El cost computacional corresponent a les comparacions és $(n-1)+(n-2)+\cdots+2+1$. Però aquesta suma és, d'acord amb el resultat que hem vist anteriorment, $\frac{n(n-1)}{2}$ al teorema 3.3, quadràtic en n, mida de l'*input*. Per tant, l'algorisme no és gaire recomanable, llevat que n sigui molt petit.



→ 4

Lògica de proposicions. Llenguatge de proposicions

Observació preliminar. Encara que el capítol està dedicat al llenguatge de proposicions, en algun cas es presenten exemples d'enunciats amb variables, que pertanyen al llenguatge de predicats.

4.1. Oracions, enunciats i proposicions

4.1.1. Oracions i enunciats

Considerem el llenguatge ordinari, que ampliem per incloure-hi expressions com a fórmules, com per exemple "$3+4=7$". D'acord amb regles lèxiques i sintàctiques (gramàtica), que inclou gramàtica específica de fórmules (que no tractarem), formem cadenes de caràcters, amb signes de puntuació. Algunes d'aquestes cadenes no són oracions, no estan ben formades; altres estan ben formades i són oracions.

Exemple 4.1 Feu la distinció entre oració i enunciat. Doneu-ne exemples.

Un enunciat és una oració on es fa una afirmació que és certa o falsa. Tot enunciat és oració, però no tota oració és enunciat: per exemple, una ordre no és cap enunciat.

a) Enunciat: "L'aigua destil·lada bull a cent graus"
b) Enunciat: "2+2=4"
c) Enunciat: "1=0"
d) No enunciat (és una ordre): "Estudieu!"
e) Enunciat: "Tots els homes són mortals"
f) Enunciat: "Existeix l'arrel quadrada de tot nombre real no negatiu"
g) No enunciat (podria ser un títol, però no afirma res): "Els polifenols i tu"
h) No enunciat (no és cap afirmació): "Com millorar les condicions de vida de la població del Kazakhstan"
i) Enunciat: "Les gallines van a jóc quan es pon el sol". ■

PROBLEMA 4.1

Indiqueu quines de les oracions següents són enunciats:

a) $2+2=5$ *(fórmula corresponent a l'oració "dos més dos és igual a cinc").*
b) Set de nou *és un personatge de* Star Trek Voyager.

c) *Menja!* *d)* *Plou i fa sol.* *e)* *Neva?*

f) *Ramsès II el Gran establí un tractat de pau amb els hittites.*
g) *La suma d'un nombre senar de nombres senars és senar.*
h) *Guillem el Conqueridor vencé el rei Harold a la batalla de Hastings.*
i) *Aquesta frase no està escrita en hittita.*
j) *Aquest enunciat és fals.*
k) $\displaystyle\sum_{n=1}^{200}\binom{\prod_{i=0}^{\lfloor n/2\rfloor}\binom{\lceil\frac{i+1}{i}\rceil}{\lfloor\frac{2}{3}\rfloor}^{2}}{2}$ *no és un jeroglífic egipci.*
l) $2+7=$
m) *Treballes o estudies?*

Solució. El criteri de decisió és si se li pot assignar un valor de veritat o no:

a) És enunciat/proposició (fals).
b) És enunciat (cert). La veracitat és relativa al context de l'univers de ficció de *Star Trek*.
c) No és enunciat (és una ordre, no un enunciat).
d) És enunciat (la veracitat és contextual).
e) No és enunciat (és una pregunta, no una afirmació).

f) És enunciat (cert).
g) És enunciat (cert).
h) És enunciat (cert).
i) És enunciat (cert).

j) No és un enunciat. Vegeu que s'arriba a una contradicció amb qualsevol assignació de veracitat.
k) És enunciat (cert, és una fórmula matemàtica, no un jeroglífic egipci, per més que ho pugui semblar).
l) No és oració.
m) No, és una pregunta (és una oració).

PROBLEMA 4.2

Doneu exemples d'oracions (llenguatge ordinari ampliat amb llenguatge de fórmules) que no són enunciats.

Solució

a) Que no et vegi més per aquí! (és una ordre).
b) És $5 \leq 7$? (és una pregunta).
c) $0 = 1$? (és una pregunta).
d) 3=7 si 0=1? (és una pregunta).
e) Treballar, treballar i més treballar (no afirma res; de fet, no és ni tan sols una oració).

PROBLEMA 4.3

Doneu exemples de construccions del llenguatge que no són oracions.

Solució. Els exemples següents, encara que alguns s'entenen, no són correctes gramaticalment; no són oracions.

Gelats per a la calor!

Mi gustar coco.

El vaca dóna llet.

Podrida dolenta molt ser carn la.

$!5 <<>=< 3$ (suposant el llenguatge ordinari ampliat a llenguatge de fórmules).

PROBLEMA 4.4

Doneu exemples d'oracions (amb llenguatge ampliat per fórmules) que són enunciats.

Solució

a) Si $0 = 1$, aleshores $3 = 7$.
b) Existeixen homes mortals. Comentari: és cert o fals, encara que no se sàpiga.
c) $4 = 5$ només si $0 = 1$.
d) $1 = 0$.
e) $3 \neq 4$.
f) Les gallines són mortals.

PROBLEMA 4.5

Indiqueu quines de les següents cadenes de caràcters del llenguatge ordinari són oracions, enunciats, no oracions, no enunciats.

a) "La Melaleuca alternifolia és un plant austrolià"
b) "T'agraden els moniatos?"
c) "L'estramoni és tòxic"
d) "L'alfàbrega és aromàtica, però no és medicinal"

e) *"Aneu amb compte!"*

f) *"Mi no voler menjar"*

g) "$3+4$"

h) "$3+6=10$"

i) "3"

j) *"3>"*

Solució

a) No és una oració, té errors lèxics. Errors: "un plant austrolià" en comptes d'"una planta australiana".

b) Oració que no és enunciat. És una pregunta.

c) Oració, enunciat.

d) Oració, enunciat.

e) Oració, no és enunciat. És una ordre.

f) No és cap oració. No és sintàcticament correcta.

g) No és una oració; és una cadena de caràcters, és una expressió en format de fórmula de "tres més quatre".

h) Oració, enunciat ("tres i sis fan deu", "tres i sis són deu", "tres més sis és igual a deu", "tres i sis és igual a deu").

i) No és una oració; és una cadena de caràcters.

j) No és una oració; és una cadena de caràcters.

4.1.2. Enunciats simples i compostos

Els enunciats *simples* són els que tenen l'estructura subjecte-predicat, com per exemple:

"el gat dorm" "el gos borda" "en Joan canta" "la Maria balla" $3 > 2$

Podem combinar amb "operacions lògiques" enunciats simples per tal d'obtenir-ne de més complexos, els enunciats *compostos*. Hem d'indicar quines serien les operacions lògiques (*connectives lògiques*) que utilitzaríem, d'entre diversos jocs de connectives possibles. Escollim el joc estàndard en matemàtiques:

"no ..."
"... i ..."
"... o ..."
"si ..., aleshores ..."
"... si, i només si, ..."

Per exemple:

"el gat dorm i el gos borda"

"en Joan no balla" [no en Joan balla]
"en Joan balla i la Maria canta"
$(3 > 2)$ i $(0 < 1)$

Tot això ho sistematitzem a l'apartat següent.

Ara vegem-ne alguns exemples:

PROBLEMA 4.6

Indiqueu quins són enunciats simples i quins són enunciats compostos:

a) *Plou.*
b) *Si* $1 = 0$*, aleshores* $2 < 1$.
c) *No fa sol.*
d) *Plou i no fa sol.*
e) $1 \neq 0$.
f) *Ni plou ni fa sol [és: no plou i no fa sol].*
g) *En Joan estudia, la Maria toca el piano i el gat dorm [és: En Joan estudia i la Maria toca el piano i el gat dorm].*

Solució

a) Simple. Plou.
b) Compost. Si $1 = 0$, aleshores $2 < 1$.
c) Compost. No fa sol.
d) Compost. Plou i no fa sol.
e) Simple. $1 \neq 0$. Això si s'accepta com a primitiu el símbol $\neq$. En cas que s'hagués d'escriure $\neg(1 = 0)$, aleshores seria compost.
f) Compost. Ni plou ni fa sol.
g) Compost. En Joan estudia, la Maria toca el piano i el gat dorm.

PROBLEMA 4.7

Escriviu diversos enunciats simples i diversos enunciats compostos.

Solució

a) $3 + 4 = -1$ (simple).
b) En Jordi menja un gelat i una *Mantis religiosa* volta pel jardí (compost).
c) Si 1=0, aleshores 2=4 (compost).
d) $3 = 5 \rightarrow 0 > 1$ (compost) (versió verbal: si $3 = 5$, aleshores $0 > 1$).
e) $1 = 0$ (simple).
f) La iguana dorm (simple).

g) $(4 > -1) \wedge (1 = 0)$ (compost) (versió verbal: $(4 > -1)$ i $(1 = 0)$).
h) El curare és neurotòxic (simple).

PROBLEMA 4.8

Indiqueu quins són els enunciats simples i els compostos d'entre els següents. En el cas dels compostos, analitzeu-ne l'estructura i expresseu-la en termes de simples (lletres proposicionals o fórmules atòmiques).

a) *"La sang de drago és una planta medicinal del tròpic i la farigola és una planta medicinal mediterrània".*
b) *"La patata és una solanàcia i la seva fruita és verinosa ".*
c) *"L'alfàbrega és aromàtica, però no és medicinal".*
d) *"El peròxid d'hidrogen és molt tòxic, però la catalasa el neutralitza".*
e) *"No neva ni plou".*
f) *"El taxol és un antitumoral".*
g) "Mandrake el mag *és un personatge de còmic".*

Solució

a) Compost. És $p \wedge q$, on $p =$"la sang de drago és una planta medicinal del tròpic" i $q =$"la farigola és una planta medicinal mediterrània".
b) Compost. Per poder escriure-ho com a conjunció d'enunciats independents, s'ha de reformular equivalentment com: "La patata és una solanàcia i la fruita de la patata és verinosa". Aleshores és $p \wedge q$, on $p =$"la patata és una solanàcia" i $q =$"la fruita de la patata és verinosa".
c) Compost. S'ha de reformular per poder-ne distingir els enunciats simples independents. El sentit antagònic del "però" es perd amb la simbolització. La frase és equivalent a: "L'alfàbrega és aromàtica i l'alfàbrega no és medicinal". Aleshores, es pot simbolitzar mitjançant $p \wedge \neg q$, amb $p =$"l'alfàbrega és aromàtica" i $q =$"l'alfàbrega és medicinal".
d) Compost. Per a formalitzar-la bé, cal refer la frase: "El peròxid d'hidrogen és molt tòxic i la catalasa neutralitza el peròxid d'hidrogen". És $p \wedge q$, on $p =$"el peròxid d'hidrogen és molt tòxic" i $q =$"la catalasa neutralitza el peròxid d'hidrogen".
e) Compost. És $\neg p \wedge \neg q$, on $p =$"neva", $q =$ "plou".
f) Simple. No conté connectives. Subjecte: "el taxol"; predicat: "és un antitumoral".
g) Simple. Subjecte: "Mandrake el mag"; predicat: "és un personatge de còmic".

Tot això ho sistematitzem a l'apartat següent.

4.1.3. Connectives

Vegem els noms i símbols per a les connectives:

$\neg$	no	negació
$\vee$	o	disjunció ("o" no exclusiu)
$\wedge$	i	conjunció
$\rightarrow$	condicional	si ..., aleshores ... (i altres relacionades: condició necessària, condició suficient, només si)
$\leftrightarrow$	bicondicional	... si, i només si, ... (i altres variants com: condició necessària i suficient)

Aquestes són les connectives bàsiques. N'hi ha d'altres, que no considerarem: $|$ (NAND), $\downarrow$ (NOR), $\oplus$ (XOR, o exclusiu).

Descripció conceptual

Definició 4.1 (negació) ***¬p és cert si, i només si, p és fals***. *Correspon conceptualment a la negació del que s'afirma en una proposició; és a dir, correspon al "no" lògic. Notació: si p és una proposició, aleshores s'indica per $\neg p$, "no p". Nom alternatiu: NOT (porta lògica en circuits).*

Definició 4.2 (conjunció) ***p i q és cert si, i només si, p, q són ambdós certs***. *Correspon al "i" lògic. Notació: $\wedge$, $p \wedge q$. Nom alternatiu: AND (porta lògica en circuits).*

Definició 4.3 (disjunció) *La proposició $p \vee q$* ***és certa si qualsevol de les dues, p o q, és certa****, inclòs el cas en què totes dues ho siguin; per tant, només serà falsa en cas que ho siguin totes dues. Correspon a "o" . Notació : $\vee$, $p \vee q$. Nom alternatiu: OR (en circuits lògics).*

Pel que fa a la resta, passem ja directament a la descripció per mitjà de la taula.

Descripció tabular

Suposem que tenim una connectiva o operació lògica de n proposicions, que a aquest efecte anomenarem ***operands***. Una taula de veritat de n operands és una taula de $n+1$ columnes; les n primeres corresponen als operands i inclouen totes les possibilitats per a valors de veritat dels operands, i l'última és el resultat de la veracitat o la falsedat per a cada una de les files.

La connectiva corresponent seria n–ària.

OP_1	OP_2	OP_3	$\cdots$	OP_n	RESULTAT
1	0	1	$\cdots$	1	1
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Per exemple, un cas concret podria ser el de la taula següent:

A	B	C	RESULTAT
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Aquesta taula descriu una operació lògica que depèn de tres operands: el resultat és cert exactament en cas que hi hagi un mínim de dos operands certs. Es pot pensar la situació següent "de la vida real" en què convingui considerar una operació lògica o connectiva com el cas que s'acaba de descriure: tres votants d'una comissió per a decidir un assumpte poden accionar sengles dispositius de votació amb dos valors (1 per a vot afirmatiu, 0 per a vot negatiu); la proposta que es vota s'aprovarà si, i només si, rep un mínim de dos vots (és a dir, dos o tres vots afirmatius). Es pot pensar una altra variant: un circuit elèctric amb tres interruptors de dues posicions deixa passar el corrent exactament quan un mínim de dos interruptors estan accionats. La taula anterior descriu totes les situacions possibles i, per tant, descriu funcionalment el circuit, tot i que no físicament o materialment.

La taula següent (dreta) és un resum de totes les connectives binàries indicades anteriorment:

p	$\neg p$
0	1
1	0

p	q	$\vee$	$\wedge$	$\rightarrow$	$\leftrightarrow$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

PROBLEMA 4.9

Considerem la fórmula proposicional $(p \vee \neg q) \wedge \neg r$. Quin és el valor de veritat (0,1) de la fórmula si els valors de veritat de les "variables" (lletres proposicionals) són:

a) $p := 0, q := 1, r := 1.$

b) $p := 1, q := 1, r := 1.$

c) $p := 1, q := 0, r := 1.$

d) $p := 0, q := 1, r := 0.$

Solució. Fent un abús notacional:

a) "$(0 \vee \neg 1) \wedge \neg 1$", que és "$(0 \vee 0) \wedge 0$", que és "$0 \wedge 0$", que és "0".

b) 0. En efecte, $(1 \vee \neg 1) \wedge \neg 1 \equiv (1 \vee 0) \wedge 0 \equiv 1 \wedge 0 \equiv 0$.

c) 0. En efecte, $(1 \vee \neg 0) \wedge \neg 1 \equiv (1 \vee 1) \wedge 0 \equiv 1 \wedge 0 \equiv 0$.

d) 0. En efecte, $(0 \vee \neg 1) \wedge \neg 1 \equiv (0 \vee 0) \wedge 0 \equiv 0 \wedge 0 \equiv 0$.

PROBLEMA 4.10

Considerem la fórmula proposicional $(p \vee \neg q) \wedge \neg r$. *Si el valor de veritat (0,1) de la fórmula és 1, aleshores:*

a) Què podem deduir sobre r i sobre $p \vee \neg q$*?*

b) Si $p := 0$*, què podem deduir?*

Solució

a) Podem escriure o considerar la taula de veritat parcial (vegeu taules de veritat), restringida al cas que el valor de veritat sigui cert per a la fórmula.

También podem fer una deducció directa: la fórmula és una conjunció $\wedge$. Si és certa, això significa que els dos operands prenen el valor "cert", d'on $\neg r$ "és" 1 i, per tant, $r = 0$; com que $p \vee \neg q$ és cert, és $p = 1$ o $q = 0$.

b) Aleshores, $r = 0$ i $q = 0$, per deducció directa o per la taula de veritat.

Observació. Notacionalment seria preferible fer servir una funció v d'assignació de valors de veritat i escriure, per exemple, $v(r) = 0$ i $v(q) = 0$, etc. Que el lector refaci l'enunciat i la solució en aquests termes.

També es poden definir connectives ternàries (o de més operands). Vegem-ne un exemple.

Exemple 4.2 Definim amb la taula noves connectives ternàries: $M, m, \oplus^3, \star$.

p	q	r	$M(p,q,r)$	$m(p,q,r)$	$\oplus^3(p,q,r)$	$\star(p,q,r)$
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	0	1	1	1
1	0	0	0	1	1	1
0	1	1	1	0	0	0
1	0	1	1	0	0	0
1	1	0	1	0	0	0
1	1	1	1	0	1	0

Descrivim-ne el comportament.

Connectiva ternària "majoria (M)", que és certa si, i només si, la majoria dels operands prenen el valor "cert" (en cas contrari, és falsa). Denotem-la per $M(p,q,r)$.

Connectiva ternària "minoria (m)", que és certa si, i només si, la minoria dels operands prenen el valor "cert" (en cas contrari, és falsa). Denotem-la per $m(p,q,r)$.

Connectiva ternària “$\oplus^3$”, que és certa si, i només si, un nombre senar dels operands prenen el valor “cert” (en cas contrari, és falsa). Denotem-la per $\oplus^3(p,q,r)$.

Connectiva ternària “$\star$”, que és certa si, i només si, exactament una de les lletres és “certa” (en cas contrari, és falsa). Denotem-la per $\star(p,q,r)$. ■

PROBLEMA 4.11

Estudieu quines de les afirmacions següents són certes i quines són falses.

a) $1=0\to 3=5$

b) $1\neq 0\to 3=5$

c) $1=0\leftrightarrow 3=5$

d) $1\neq 0\to 3\neq 5$

e) $1=0\to 3\neq 5$

f) $1\neq 0\leftrightarrow 3\neq 5$

Solució

a) Certa. És el cas “$F\to F$”.

b) Falsa. És el cas “$V\to F$”.

c) Certa. És el cas “$F\leftrightarrow F$”.

d) Certa. És el cas “$V\to V$”.

e) Certa. És el cas “$F\to V$”.

f) Certa. És el cas “$V\leftrightarrow V$”.

PROBLEMA 4.12

Si p i q són lletres proposicionals, indiqueu quin és el valor de veritat de p si

a) *q és cert i $p\wedge q$ és cert.*

b) *q és fals i $p\vee q$ és cert*

c) *q és fals i $p\wedge q$ és fals.*

d) *q és cert i $p\wedge q$ és fals.*

e) *q és fals i $p\to q$ és fals.*

f) *q és cert i $p\to q$ és cert.*

g) *q és fals i $p\to q$ és cert.*

h) *q és fals i $p\wedge(\neg q)$ és fals.*

Solució

a) p cert.

b) p cert.

c) Res es pot afirmar.

d) p fals.

e) p cert.

f) p cert.

g) p fals.

h) p fals.

PROBLEMA 4.13

Donades les lletres proposicionals p,q, indiqueu si són compatibles o no les afirmacions següents (cadascuna per separat):

a) *$p\vee q$ cert, p fals, q fals.*

b) *$p\wedge q$ fals, p cert, q cert.*

c) *$p\vee q$ cert, p cert, q fals.*

d) *$p\wedge q$ cert, p cert, q fals.*

e) *$p\wedge q$ cert, p cert, q cert.*

f) *$p\vee q$ fals, $p\wedge q$ cert, p fals.*

g) *$p\vee q$ fals, $p\wedge q$ cert.*

h) *$p\vee q$ cert, $p\wedge q$ fals, p fals, q fals.*

Solució

a) No, incompatible.
b) No, incompatible.
c) Sí, compatible.
d) No, incompatible.
e) Sí, compatible.
f) No, incompatible.
g) No, incompatible.
h) No, incompatible.

4.1.4. Condicionals i bicondicionals: condició necessària, suficient, i necessària i suficient

La fórmula $p \rightarrow q$ correspon a un condicional i es llegeix de moltes maneres equivalents en el llenguatge ordinari. Correspon a l'estructura condicional (connectiva) "Si ..., aleshores ...", que, en aquest cas, seria "Si *p*, aleshores *q*". En aquesta estructura:

p és l'antecedent, la hipòtesi, la premissa,
q és el conseqüent, la tesi, la conseqüència.

Ara bé, hi ha altres maneres de dir el mateix:

Si *p*, *q*

q si *p*

p és una condició suficient per a *q*, i
q és una condició necessària de/per a *p*.

Vegem amb exemples l'ús de "condició necessària", de "condició suficient", de "condició necessària i suficient".

▹ Exemples sense variables, amb formulació només verbal:

Exemple 4.3 El quadrat d'un enter parell.

a) Condició suficient:

- "Si un nombre natural és parell, aleshores el quadrat [del nombre] és parell".
- "Condició suficient perquè el quadrat d'un nombre natural sigui parell és que el nombre sigui parell [també ho sigui]".
- "Que un nombre natural sigui parell és condició suficient perquè el seu quadrat sigui parell [també ho sigui]".
- "És [condició] suficient que un nombre natural sigui parell perquè [també] ho sigui el seu quadrat".
- "Un nombre natural és parell" és condició suficient per tal que "el seu quadrat sigui parell".

b) Condició necessària:

- "Que el quadrat d'un nombre natural sigui parell és condició necessària perquè el nombre natural sigui parell".

- "És necessari (condició necessària) que el quadrat d'un nombre natural sigui parell per tal que el nombre ho sigui".
- "El quadrat d'un nombre natural parell és parell".
- "És parell el quadrat d'un nombre natural parell".
- "El quadrat d'un nombre natural és parell si el nombre és parell".
- "Si un nombre natural és parell, el seu quadrat és parell".

c) *Condició necessària i suficient, "... si, i només si, ...", condicions equivalents*:

- "Un nombre natural és parell si, i només si, el seu quadrat és parell".
- "El quadrat d'un nombre natural és parell si, i només si, el nombre és parell".
- "Que un nombre natural sigui parell és condició necessària i suficient per tal que el quadrat sigui parell".
- "Que el quadrat d'un nombre natural sigui parell és condició necessària i suficient per tal que el nombre sigui parell".
- "Per a un nombre natural són equivalents:
  - el nombre és parell,
  - el quadrat del nombre és parell".
- "Que el quadrat d'un nombre natural sigui parell és equivalent que el nombre sigui parell". ■

Exemple 4.4 No tots han de ser necessàriament exemples matemàtics. En aquest cas, no se sol utilitzar "condició ...", però si "és suficient que ... per tal que ..." o "és necessari que ... per tal que ...".

"Si estic malalt, no vaig a treballar". ■

▷ Resulta més clar l'ús de "condició necessària", "condició suficient", "condició necessària i suficient" amb afirmacions amb *fórmules*, de resultats matemàtics, encara que sigui amb variables (corresponent al *llenguatge de predicats* del capítol següent), com podem veure a continuació.

Exemple 4.5 (amb **condicional**) Considerem l'exemple (on suposem que n és un nombre enter):

"Si n és senar, aleshores n^3 és senar",

n és senar $\rightarrow n^3$ és senar.

$2 \nmid n \rightarrow 2 \nmid n^3$.

Es pot reformular de diverses maneres:

a) "n^3 és senar si n és senar".

b) En termes de *condició suficient*:

"n senar és condició suficient per tal que n^3 sigui senar".

"Que n sigui senar és condició suficient perquè n^3 sigui senar".

"És condició suficient que n sigui senar perquè n^3 també ho sigui".
"Una condició suficient perquè n^3 sigui senar és que n sigui senar".
"Una condició suficient perquè n^3 sigui senar és que n també ho sigui".

c) Ara, en termes de *condició necessària*:

"Que n^3 sigui senar és una condició necessària perquè n sigui senar".
"Una condició necessària perquè n sigui senar és que n^3 sigui senar".
"És condició necessària que n^3 sigui senar perquè n sigui senar".
"n^3 senar és condició necessària perquè n sigui senar".

A totes les expressions anteriors, podem substituir "n senar" per $2 \nmid n$, i "n^3 senar" per $2 \nmid n^3$. ■

La fórmula $a \leftrightarrow b$ és un bicondicional. Vegem com es pot expressar en el llenguatge ordinari. Hi ha diverses possibilitats.

a si, i només si, b,
a és condició necessària i suficient per a b,
b és condició necessària i suficient per a a.

Atès que $a \leftrightarrow b$ és lògicament equivalent a $(a \to b) \wedge (b \to a)$, tenim: "Si a, aleshores b" i "si b, aleshores a". Vegem-ne un exemple:

Exemple 4.6 (amb **bicondicional**) Amb n nombre enter:

$$n \text{ senar } \leftrightarrow n^3 \text{ senar}$$

"n és senar si, i només si, n^3 és senar".
"n^3 és senar si, i només si, n és senar".
"n és senar és condició necessària i suficient perquè n^3 sigui senar".
"n^3 és senar és condició necessària i suficient perquè n sigui senar".
"Una condició necessària i suficient perquè n sigui senar és que n^3 sigui senar".
"Una condició necessària i suficient perquè n^3 sigui senar és que n sigui senar".

També es pot formular com segueix:

"Per a $n \in \mathbb{Z}$, són equivalents:

a) n és senar
b) n^3 és senar"

A totes les expressions anteriors, podem substituir "n senar" per $2 \nmid n$, i "n^3 senar" per $2 \nmid n^3$, i en tindrem exemples addicionals. ■

4.2. Traducció: formalització o simbolització i desformalització

Entenem aquí la formalització com el procés de traduir enunciats en llenguatge natural a llenguatge de proposicions, de manera que un enunciat s'expressi finalment com a fórmula proposicional. La traducció també es pot considerar en sentit contrari, de la fórmula proposicional al llenguatge natural, un cop assignats "valors" a les lletres proposicionals.

El capítol següent es dedica al llenguatge de predicats. El llenguatge de predicats és un entorn més ric que el de proposicions, ja que disposem addicionalment de variables i quantificadors. Llavors tindrem ocasió de veure un bon nombre d'exemples i exercicis de simbolització, i inversament, de manera que aquí ens limitem a uns pocs exemples o exercicis.

4.2.1. Traducció de llenguatge natural a formal: formalització o simbolització

PROBLEMA 4.14

Expresseu els enunciats següents, donats en llenguatge natural, en forma de fórmula proposicional (formalització o simbolització):

a) "Flash Gordon és un personatge de còmic i Winston Churchill és un personatge històric".

b) "Ni plou ni fa sol".

c) "Plou, però fa sol".

d) "Alex Raymond és un dels millors dibuixants de còmics de tots els temps".

e) "Entren pardals a les aules, però no garces, ni cotorres, ni merles ni coloms".

f) "Si un ocell arriba a la finestra, és el moment que el savi reemprengui el seu camí".

Solució

a) $p \wedge q$, on $p :=$ "Flash Gordon és un personatge de còmic", $q :=$"Winston Churchill és un personatge històric".

b) $\neg p \wedge \neg q$, on $p :=$"plou", $q :=$"fa sol".

c) $p \wedge q$, on $p :=$"plou", $q :=$"fa sol".

d) p, on $p :=$"Alex Raymond és el millor dibuixant de còmics de tots els temps".

e) $p \wedge \neg g \wedge \neg t \wedge \neg m \wedge \neg c$ on $p :=$"entren pardals", $g :=$"entren garces", $t :=$"entren cotorres", $m :=$"entren merles", $c :=$"entren coloms". Observeu que el matís adversatiu "però" es perd en la formalització (i queda reduït a un simple "i").

f) $p \to q$, on $p :=$"un ocell arriba a la finestra", $q :=$"és el moment que el savi reemprengui el seu camí".

PROBLEMA 4.15

Expresseu formalment les afirmacions següents com a fórmules proposicionals, a partir de les proposicions més senzilles possible (simples, sense connectives):

a) *Plou i fa sol.*

b) Set de Nou *és molt intel·ligent, però molt maldestre per a les relacions humanes.*

c) *L'aigua està freda o està calenta.*

d) *L'home no ha arribat a la lluna.*

e) *En Joan ha anat al cinema o al teatre, però no a la piscina.*

f) *L'aigua no està ni gaire freda ni gaire calenta.*

g) *No sóc un nen.*

h) *Els selenites no existeixen.*

Solució

a) $p \wedge q$, si $p :=$"plou" i $q :=$ "fa sol".

b) La paraula "però" emfasitza una contraposició, un cert demèrit en el llenguatge natural, però, des del punt de vista lògic, té simplement un valor de "i", conjuntiu (es perden possibles matisos); per tant, si $p :=$ "*Set de Nou* és molt intel·ligent" i $q :=$ "*Set de Nou* és molt maldestre per a les relacions humanes ", aleshores és $p \wedge q$.

c) $p \vee q$, amb $p :=$ "l'aigua està freda" i $q :=$ "l'aigua està calenta".

d) $\neg q$, si $q :=$ "l'home ha arribat a la lluna" (observeu que la veracitat-falsedat és contextual temporal).

e) $(p \vee q) \wedge \neg w$, on $p :=$ "en Joan ha anat al cinema", $q :=$ "en Joan ha anat al teatre", $w :=$ "en Joan ha anat a la piscina".

f) Si $p :=$ "l'aigua està molt freda" i $q :=$ "l'aigua està molt calenta", és $(\neg p) \wedge (\neg q)$. Observeu que l'estructura lògica de la frase és més simple que l'enunciat del llenguatge natural; queda despullada de qualsevol redundància i estructures emfasitzants.

g) $\neg p$, si $p :=$ "sóc un nen".

h) La frase és negació de $p :=$ "els selenites existeixen". En realitat, hauríem de dir "no (els selenites existeixen)", és a dir, "no els selenites existeixen", però seria molt antinatural en el llenguatge natural. La resposta és $\neg p$.

PROBLEMA 4.16

Si p és " Plou*" i q és "*Fa sol*", escriviu una fórmula proposicional per a cada una de les afirmacions següents:*

a) *Plou i fa sol.*

b) *No plou i no fa sol.*

c) *Plou i no fa sol.*

d) *Ni plou ni fa sol.*

e) *No plou i fa sol.*

f) *Si plou, no fa sol.*

Solució

a) $p \wedge q$

b) $(\neg p) \wedge (\neg q)$

c) $p \wedge (\neg q)$

d) $(\neg p) \wedge (\neg q)$

e) $(\neg p) \wedge q$

f) $p \rightarrow \neg q$

4.2.2. Traducció de fórmula proposicional a llenguatge natural: desformalització

PROBLEMA 4.17

Indiquem:

$p :=$ *"La lisina és un aminoàcid essencial".*

$q :=$ *"La melatonina és una hormona".*

$r :=$ *'És de dia".*	$w :=$ *"En Joan va a la biblioteca".*
$s :=$ *"És de nit".*	$g :=$ *"Fa fred".*
$t :=$ *"En Joan va al teatre".*	$h :=$ *"Fa calor".*

Expresseu en llenguatge natural els enunciats següents donats en forma de fórmula proposicional (desformalització).

a) $p \wedge q$
b) $r \vee s$
c) $r \to \neg s$
d) $t \wedge \neg w$
e) $\neg g \wedge \neg h$

Solució

a) La lisina és un aminoàcid essencial i la melatonina és una hormona.
b) És de dia o és de nit.
c) Si és de dia, no és de nit.
d) En Joan va al teatre i no va a la biblioteca.
e) No fa fred ni calor (=no fa fred i no fa calor).

PROBLEMA 4.18

*Si p és "*Jugo a cartes*" i q és "*Descanso*", expresseu en llenguatge natural:*

a) $\neg p$
b) $p \wedge q$
c) $p \vee q$
d) $\neg p \wedge \neg q$
e) $p \to q$
f) $\neg p \to \neg q$
g) $\neg q \to \neg p$
h) $q \to \neg p$
i) $\neg p \vee \neg q$

Solució

a) No jugo a cartes.
b) Jugo a cartes i descanso.
c) Jugo a cartes o descanso.
d) Ni jugo a cartes ni descanso (o anàlegs).
e) Si jugo a cartes, descanso (és a dir, si jugo a cartes, llavors descanso).
f) Si no jugo a cartes, aleshores no descanso.
g) Si no descanso, aleshores no jugo a cartes.

h) No jugo a cartes si descanso.

i) O no jugo a cartes o no descanso.

4.3. El llenguatge: gramàtica

Els elements del llenguatge de proposicions són: l'alfabet (amb les connectives) i les fórmules (amb les regles de formació o de generació de fórmules, normalment noves fórmules a partir de fórmules preexistents).

4.3.1. L'alfabet i les fórmules

L'alfabet. És format per:

– les lletres proposicionals ($a, b, c, \ldots, p, q, r, \ldots, p_1, p_2, \ldots$), eventualment amb subíndexs (hi ha provisió infinita).

– les connectives: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.

– els parèntesis $($, $)$ (per a facilitar-ne la legibilitat humana, hi afegirem opcionalment espais en blanc, sense valor).

Les fórmules. Distingim entre les fórmules atòmiques o simples i les compostes.

Fórmules atòmiques o simples (són les lletres proposicionals): p, q, r. No tenen connectives.

Fórmules compostes. Són les que es formen a partir de les atòmiques per aplicació de les connectives lògiques: $(p \vee q) \rightarrow w$, per exemple.

4.3.2. Regles de formació de fórmules proposicionals

Descrivim a continuació les regles de generació de les fórmules proposicionals (en la versió que aquí considerem pel que fa a les connectives).

Regles de formació. Descriuen quines són les fórmules proposicionals ("ben formades", qualificatiu redundant ja que, si no ho són, ja no són fórmules). Les regles són:

R1 (regla 1): Les lletres proposicionals són fórmules (simples o atòmiques).

R2 (regla 2): Si α és una fórmula, també ho és $\neg\alpha$.

R3a: Si α i β són fórmules, també ho és $(\alpha \wedge \beta)$.

R3b: Si α i β són fórmules, també ho és $(\alpha \vee \beta)$.

R3c: Si α i β són fórmules, també ho és $(\alpha \rightarrow \beta)$.

R3d: Si α i β són fórmules, també ho és $(\alpha \leftrightarrow \beta)$.

R4 (regla 4): Qualsevol fórmula s'obté per l'aplicació de les regles anteriors un nombre **finit** de vegades.

Així, si A és una fórmula proposicional:

a) o bé és una lletra proposicional (àtom),
b) o bé és $\neg A_1$,
c) o bé és $A_1 \star A_2$, per a algunes fórmules proposicionals A_1, A_2, i per a alguna connectiva $\star$ d'entre $\wedge, \vee, \rightarrow, \leftrightarrow$.

4.3.3. Les subfórmules

Una **subfórmula** de la fórmula F és una subcadena de caràcters de F que és una fórmula. És a dir, és una fórmula que forma part de F. Intuïtivament, és una subcadena de caràcters que podem formar (i que podem llegir). És una subcadena que es pot obtenir per aplicació de les regles anteriors de formació de fórmules (és, per tant, una fórmula). És una de les fórmules que s'obtenen en el procés de generació de la fórmula en aplicació de les regles anteriors.

En podem donar una definició recursiva o inductiva: les subfórmules són les fórmules produïdes per les regles següents:

S1: Si F és una lletra proposicional, l'única subfórmula és F.

S2: Si $F = \neg G$, les subfórmules de F són F i les subfórmules de G.

- **S3a:** Si $F = (G \wedge H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.
- **S3b:** Si $F = (G \vee H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.
- **S3c:** Si $F = (G \rightarrow H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.
- **S3d:** Si $F = (G \leftrightarrow H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.

Alternativament, utilitzant notació de conjunts i fórmules conjuntistes, si indiquem per $S(F) = \{T | T \text{ és subfórmula de } F\}$:

S1: Si F és una lletra proposicional, $S(F) = \{F\}$.

S2: Si $F = \neg G$, és $S(F) = \{F\} \cup S(G)$.

- **S3a:** Si $F = (G \wedge H)$, aleshores les subfórmules de F són: $S(F) = \{F\} \cup S(G) \cup S(H)$.
- **S3b:** Si $F = (G \vee H)$, aleshores les subfórmules de F són: $S(F) = \{F\} \cup S(G) \cup S(H)$.
- **S3c:** Si $F = (G \rightarrow H)$, aleshores les subfórmules de F són: $S(F) = \{F\} \cup S(G) \cup S(H)$.
- **S3d:** Si $F = (G \leftrightarrow H)$, aleshores les subfórmules de F són: $S(F) = \{F\} \cup S(G) \cup S(H)$.

Exemple 4.7 Considereu la cadena de caràcters: $\neg p \vee (r \wedge s)$. És una fórmula proposicional? Per què?

Resposta: Sí, perquè es genera a partir de les fórmules atòmiques p, r, s aplicant les regles de formació de fórmules:

Denotem $F = \neg p \vee (r \wedge s)$.

p, r, s són fórmules, per la regla $R1$.

$(r \wedge s)$ és una fórmula per aplicació de la regla $R3a$ a les fórmules r i s, en un dels ordres. La denotem $\alpha = (r \wedge s)$.

$\neg p$, aplicant la regla $R2$ a la fórmula p. La denotem $\beta = \neg p$.

F es genera aplicant la regla $R3b$ a α i a β, en aquest ordre, de manera que $F = \alpha \vee \beta$.

Al mateix temps, es van generant les subfórmules de la fórmula:
p, r, s, $(r \wedge s)$, $\neg p$, $\neg p \vee (r \wedge s)$.

En aquest exemple, es podria anar generant la fórmula en ordres diferents, i això donaria lloc a diverses seqüències de generació i d'ordenació de les subfórmules. Vegem-ne algunes:

Seqüència 1 de generació de la fórmula i les subfórmules:
$p, \neg p, r, s, (r \wedge s), \neg p \vee (r \wedge s)$

Seqüència 2 de generació de la fórmula i les subfórmules:
$p, r, s, \neg p, (r \wedge s), \neg p \vee (r \wedge s)$

Seqüència 3 de generació de la fórmula i les subfórmules:
$p, r, s, (r \wedge s), \neg p, \neg p \vee (r \wedge s)$,

Seqüència 3 de generació de la fórmula i les subfórmules:
$s, r, p, (r \wedge s), \neg p, \neg p \vee (r \wedge s)$

Seqüència 4 de generació de la fórmula i les subfórmules:
$r, s, (r \wedge s), p, \neg p, \neg p \vee (r \wedge s)$

Seqüència 5 de generació de la fórmula i les subfórmules:
$r, p, \neg p, s, (r \wedge s), \neg p \vee (r \wedge s)$ ■

Vegem un exemple simple de generació d'una fórmula.

Exemple 4.8 Considerem la fórmula proposicional $F = \neg(p \vee q)$. Vegem com es pot generar aplicant les regles anteriors.

1. Per aplicació de R1, p és una fórmula.
2. Per aplicació de R1, q és una fórmula.
3. Per aplicació de R3b a les dues fórmules anteriors, $(p \vee q)$ és una fórmula.
4. Per aplicació de R2 a la fórmula anterior, $\neg(p \vee q)$ és una fórmula.

Més formalment:

1. Per aplicació de R1, $F_1 = p$ és una fórmula.
2. Per aplicació de R1, $G_1 = q$ és una fórmula.
3. Per aplicació de R3b, $H = (F_1 \vee G_1)$ és una fórmula.
4. Per aplicació de R2, $F = \neg H$ és una fórmula. ■

Exemple 4.9 Indiqueu si $)\neg(p\wedge)q\neg\neg))($ és una fórmula proposicional (ben formada).

No. Formalment, perquè no es pot generar amb cap de les regles de formació de fórmules proposicionals ben construïdes. Cap regla no produeix a l'inici de la cadena el caràcter ")". Intuïtivament, perquè no la podem llegir. Amb això ja és suficient per a donar una resposta negativa, però, a més, hi ha altres subcadenes que tampoc no es poden generar per cap regla, com per exemple: $\wedge)$, $)q$, $\neg)$, $)($. ■

PROBLEMA 4.19

Escriviu un mínim de sis cadenes de caràcters (del càlcul proposicional) que no siguin fórmules proposicionals ben formades.

Solució. Algunes possibilitats:

a) $()$
b) $)($
c) $($
d) $(\neg$
e) $)\rightarrow)$
f) $)\leftrightarrow($

PROBLEMA 4.20

Doneu exemples de cadenes de caràcters que no siguin fórmules proposicionals ben formades. Els caràcters poden ser: parèntesis, connectives lògiques i lletres proposicionals (fórmules o proposicions atòmiques). Expliqueu per què no són ben formades.

Solució

a) $(((($
b) $()()()$
c) $()\rightarrow()$
d) $((((()))))$
e) $\rightarrow\rightarrow a\wedge b$
f) $(a\rightarrow(b\wedge c)$
g) $\neg a\neg b\neg c$
h) $((a\wedge b\rightarrow(c\vee d$

No són correctes perquè no es poden formar amb les regles de generació de fórmules ben formades. No són correctes sintàcticament. Per exemple, en el cas de (e), cap regla no genera $\rightarrow\rightarrow$; en el cas (f), els parèntesis no estan equilibrats.

PROBLEMA 4.21

Considereu la fórmula proposicional $(p \vee q) \to (r \wedge \neg s)$. *Indiqueu una seqüència d'aplicacions de les regles de la gramàtica del llenguatge de proposicions que generin aquesta fórmula.*

Solució

P1 (Pas 1): p és fórmula per R1,

P2 (Pas 2): q és fórmula per R1,

P3 (Pas 3): r és fórmula per R1,

P4 (Pas 4): s és fórmula per R1,

P5 (Pas 5): $\neg s$ és fórmula per R2, aplicada al resultat de P4,

P6: $(p \vee q)$ és fórmula per aplicació al resultat de P1,P2 de la regla R3b,

P7: $(r \wedge \neg s)$ és fórmula per aplicació al resultat de P3,P5 de la regla R3a,

P8: $(p \vee q) \to (r \wedge \neg s)$ és fórmula per aplicació al resultat de P6,P7 de la regla R3c, en l'ordre indicat P6 $\to$ P7.

PROBLEMA 4.22

Considereu la seqüència d'aplicació de les regles de generació de fórmules proposicionals. Indiqueu quina fórmula final es genera.

P1: p és fórmula per R1.

P2: q és fórmula per R1.

P3: r és fórmula per R1.

P4: s és fórmula per R1.

P5: R2, aplicada al resultat de P4.

P6: R2, aplicada al resultat de P2.

P7: regla R3a aplicada al resultat de P1,P6, en aquest ordre.

P8: per aplicació de la regla R3a al resultat de P5,P1, en aquest ordre.

P9: per aplicació de la regla R3c al resultat de P3,P8, en aquest ordre.

P10: per aplicació de la regla R2 al resultat de P9.

P11: per aplicació de la regla R3c al resultat de P7,P10, en aquest ordre.

Solució. Vegem pas a pas quines *subfórmules* es van generant:

P1: p és fórmula per R1.

P2: q és fórmula per R1.

P3: r és fórmula per R1.

P4: s és fórmula per R1.

P5: $\neg s$ és fórmula per R2, aplicada al resultat de P4.

P6: $\neg q$ és fórmula per R2, aplicada al resultat de P2.

P7: $(p \wedge \neg q)$ és fórmula per aplicació de la regla R3a al resultat de P1,P6, en aquest ordre.

P8: $(\neg s \wedge p)$ és fórmula per aplicació de la regla R3a al resultat de P5,P1, en aquest ordre.

P9: $(r \to (\neg s \wedge p))$ és fórmula per aplicació de la regla R3c al resultat de P3,P8, en aquest ordre.

P10: $\neg(r \to (\neg s \wedge p))$ és fórmula per aplicació de la regla R2 al resultat de P9.

P11: $(p \wedge \neg q) \to \neg(r \to (\neg s \wedge p))$ és fórmula per aplicació de la regla R3c al resultat de P7,P10, en aquest ordre.

La fórmula generada és:

$$(p \wedge \neg q) \to \neg(r \to (\neg s \wedge p))$$

Llista de les subfórmules en l'ordre en què s'han generat:

$$p, q, r, s, \neg s, \neg q, (p \wedge \neg q), (\neg s \wedge p), (r \to (\neg s \wedge p)),$$
$$\neg(r \to (\neg s \wedge p)), (p \wedge \neg q) \to \neg(r \to (\neg s \wedge p)).$$

4.3.4. Parèntesis i regles de prioritat en el llenguatge de proposicions

La prioritat màxima la tenen els parèntesis. Amb els parèntesis podem anul·lar regles de prioritat i forçar una lectura o interpretació diferent de la fórmula.

Per al joc estàndard amb les connectives $\neg, \wedge \vee, \to, \leftrightarrow$ tenim:

símbol	noms	prioritat (1=max)
( )	parèntesis	1 (màxima)
$\neg$	negació NOT	2
$\wedge$	conjunció AND	3
$\vee$	disjunció no exclusiva OR	4
$\to$	condicional	5
$\leftrightarrow$	bicondicional	6

Les connectives s'associen per la dreta quan estan repetides (es llegeix d'esquerra a dreta):

$p \vee q \vee r$ significa $(p \vee (q \vee r))$ o $p \vee (q \vee r)$ (tot i que conceptualment no hi ha ambigüitat, per l'associativitat en aquest cas).

$p \wedge q \wedge r$ significa $(p \wedge (q \wedge r))$ o $p \wedge (q \wedge r)$

$p \to q \to r$ és $p \to (q \to r)$

El símbol $\neg$ s'aplica "al mínim possible", és a dir, a la cadena més curta a la dreta que sigui sintàcticament correcta. Així, $\neg p \vee q$ és $(\neg p) \vee q$ i no $\neg(p \vee q)$. Aquest comportament varia si hi ha parèntesis convenients, com a $\neg(p \vee q)$, que no és $(\neg p) \vee q$.

El criteri anterior s'aplica també a $\wedge, \vee$.

Un excés de parèntesis pot dificultar la lectura d'una fórmula (a part que no seria generat per la gramàtica). Per exemple, si escrivim:

$$((p \to q) \leftrightarrow ((\neg q) \to (\neg p))),$$

podem prescindir dels parèntesis exteriors de la fórmula final, encara que s'hagi generat per la gramàtica:

$$(p \to q) \leftrightarrow ((\neg q) \to (\neg p)).$$

La gramàtica genera $\neg\alpha$ i no $(\neg\alpha)$. Es poden suprimir, doncs, aquests parèntesis, llevat que interessi per algun motiu:

$$(p \to q) \leftrightarrow (\neg q \to \neg p).$$

No s'ha de confondre $\neg q \to \neg p$ amb $\neg(q \to \neg p)$. S'interpreta com $(\neg q) \to (\neg p)$.

Consell. *És millor no confiar que el lector coneix les regles de prioritat i escriure els parèntesis que calgui perquè la fórmula no sigui ambigua*. Vegem-ne un exemple:

Exemple 4.10 La fórmula $a \vee b \to c$ es pot interpretar, a manca de regles de prioritat, com

$(a \vee b) \to c$, o bé com

$a \vee (b \to c)$.

D'acord amb les regles, és $(a \vee b) \to c$.

Es recomana escriure d'entrada: $(a \vee b) \to c$. ■

PROBLEMA 4.23

Considereu la fórmula proposicional $(\neg p \vee \neg q) \to (\neg r \to s)$. *Indiqueu com la llegiu aplicant-hi les regles de prioritat*.

Solució

p
$a := \neg p$
q
$b := \neg q$
$c := a \vee b$
r
$d := \neg r$
s
$e := d \to s$
$c \to e$

La fórmula és $c \to e$, amb $e = d \to s$, amb $d = \neg r$. És $c = a \vee b$, amb $a = \neg p$, $b = \neg q$.

4.4. Anàlisi d'una fórmula proposicional

Entenem per anàlisi d'una fórmula proposicional l'obtenció de l'estructura de la fórmula, lligada a la seva generació segons les regles de la gramàtica. L'objectiu pot ser obtenir la taula de veritat o expressar-la en forma d'arbre. En concret, donada una fórmula, es tracta de:

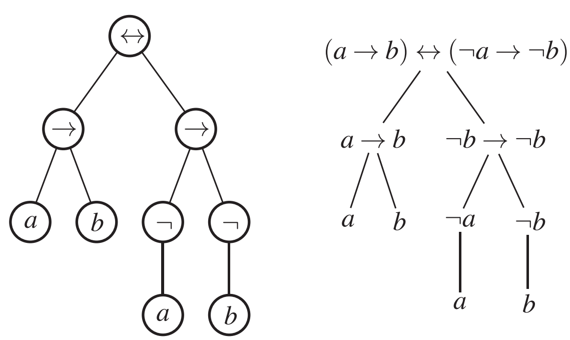
a) identificar-hi les variables proposicionals, atòmiques (les lletres),
b) identificar-hi la connectiva principal ("què és la fórmula?"),
c) escriure'n l'arbre,
d) obtenir-ne les subfórmules i identificar-ne les respectives connectives principals,
e) dir com es genera per les regles de la gramàtica,
f) obtenir la taula de la fórmula proposicional.

És útil expressar la fórmula en forma d'arbre.

Exemple 4.11 **Arbre** d'una fórmula.

Suposem que es demana l'arbre d'una fórmula proposicional, concretament

$(a \to b) \leftrightarrow (\neg a \to \neg b)$ ([BENA93]). Correspon a l'equivalència del contrarecíproc. Aquesta és una possible resposta:



Exemple 4.12 *Connectiva principal. Estructura de la fórmula.*

Quina és l'estructura de la fórmula següent?

$((\neg\neg\neg p \wedge \neg q) \to (\neg(\neg r \vee \neg s \vee t))) \to \neg p$

Resposta: un condicional:

$((\neg\neg\neg p \wedge \neg q) \to (\neg(\neg r \vee \neg s \vee t)))\to\neg p$

És $\alpha \to \beta$, on $\alpha := ((\neg\neg\neg p \wedge \neg q) \to (\neg(\neg r \vee \neg s \vee t)))$ i $\beta := \neg p$. ■

Exemple 4.13 *Equilibrament de parèntesis.*

Suposem que tenim una fórmula proposicional molt complicada, difícil de llegir, de la qual sospitem que els parèntesis no estan ben posats. Comptem els que obren i els que tanquen. Si el nombre dels que obren no coincideix amb el nombre dels que tanquen, podem concloure que la fórmula és incorrecta.

Per exemple, és correcta la fórmula:

$\neg((\neg((p \wedge \neg q) \vee r) \wedge s) \rightarrow (\neg r \rightarrow \neg((r \wedge s) \rightarrow p))))$?

Resposta: és incorrecta.

La fórmula concreta no és correcta perquè hi ha més parèntesis que tanquen“)” que parèntesis que obren“(”. ■

Contestem “què és la fórmula” a l’exercici següent:

PROBLEMA 4.24

Per a les fórmules següents, indiqueu quina és l’estructura bàsica, primària:

a) *un condicional*
b) *un bicondicional*
c) *una negació*
d) *una conjunció*
e) *una disjunció*

Identifiqueu-ne la connectiva principal.

a) $((A \wedge \neg B) \rightarrow C) \vee (D \wedge \neg A)$
b) $((A \wedge \neg B \wedge \neg C) \rightarrow D) \rightarrow (E \wedge \neg A)$
c) $A \rightarrow (B \vee C)$
d) $\neg(A \rightarrow (B \vee (C \rightarrow \neg D)))$
e) $(r \rightarrow s) \rightarrow t$
f) $(r \rightarrow s) \vee \neg(t \rightarrow \neg w)$
g) $(r \vee s) \rightarrow (t \wedge \neg(w \rightarrow \neg z))$
h) $\neg(a \leftrightarrow (b \rightarrow c))$
i) $(p \vee q) \rightarrow \neg(p \wedge \neg q)$
j) $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$

Solució

a) És una disjunció. Si $\alpha = ((A \wedge \neg B) \rightarrow C)$, $\beta = (D \wedge \neg A)$, és $\alpha \vee \beta$.

$$((A \wedge \neg B) \rightarrow C) \vee (D \wedge \neg A).$$

b) És un condicional. Si $\alpha = ((A \wedge \neg B \wedge \neg C) \to D)$, $\beta = (E \wedge \neg A)$, és $\alpha \to \beta$.

$$((A \wedge \neg B \wedge \neg C) \to D) \to (E \wedge \neg A).$$

c) Un condicional. És $A \to \beta$, on $\beta = (B \vee C)$.

$$A \to (B \vee C).$$

d) Una negació.

$\neg(A \to (B \vee (C \to \neg D)))$. Concretament,

$$\neg F, \text{ amb } F = (A \to (B \vee (C \to \neg D))).$$

e) $(r \to s) \to t$ és un condicional.

Condicional: $(r \to s) \to t$

f) $(r \to s) \vee \neg(t \to \neg w)$ és una disjunció.

Disjunció: $(r \to s) \vee \neg(t \to \neg w)$

g) $(r \vee s) \to (t \wedge \neg(w \to \neg z))$ (condicional).

h) $\neg (a \leftrightarrow (b \to c))$ (negació).

i) $(p \vee q) \to \neg(p \wedge \neg q)$ (condicional).

j) $(p \to q) \leftrightarrow (\neg q \to \neg p)$ (bicondicional).

PROBLEMA 4.25

Considereu la fórmula proposicional:

$$(((p \to q) \wedge \neg(r \to \neg s)) \to ((p \vee r) \to (\neg q \vee s)))$$

a) Estan (ben) equilibrats els parèntesis?
b) Indiqueu quines són les variables atòmiques o lletres proposicionals.
c) Identifiqueu les connectives i indiqueu-ne el nom.
d) Podem eliminar parèntesis?
e) Expliqueu com es genera la fórmula aplicant-hi les regles de generació.
f) Escriviu totes les subfórmules.

Solució

a) Sí, hi ha el mateix nombre de parèntesis que obren que parèntesis que tanquen (7).

b) p, q, r, s.

c) $\rightarrow$ (condicional), $\wedge$ (conjunció), $\neg$ (negació), $\vee$ (disjunció).

d) Alguns: $((p \rightarrow q) \wedge \neg(r \rightarrow \neg s)) \rightarrow ((p \vee r) \rightarrow (\neg q \vee s))$. Aplicant-hi les regles de prioritat, en podríem eliminar més, però pot augmentar el perill de confusió (per a la lectura humana):

$$(p \rightarrow q \wedge \neg(r \rightarrow \neg s)) \rightarrow (p \vee r \rightarrow \neg q \vee s) \text{ (no és recomanable).}$$

e) *i*) p és fórmula, per R1 (la denominem s1) (s1=p).
ii) q és fórmula, per R1 (la denominem s2) (s2=q).
iii) $(p \rightarrow q)$, per R3c aplicada a s1 i a s2 (la denominem s3) (s3=$p \rightarrow q$).
iv) r és fórmula, per R1 (la denominem s4).
v) s és fórmula, per R1 (la denominem s5).
vi) $\neg s$ és fórmula, per R2 aplicada a s5 (la denominem s6).
vii) $(r \rightarrow \neg s)$, per R3c aplicada a s5 i a s6 (la denominem s7).
viii) $\neg(r \rightarrow \neg s)$, per R2 aplicada a s7 (la denominem s8).
ix) $((p \rightarrow q) \wedge \neg(r \rightarrow \neg s))$, per R3a aplicada a s3 i a s8 (la denominem s9).
x) $(p \vee r)$, per R3b aplicada a s1 i a s4 (la denominem s10).
xi) $\neg q$, per R1 aplicada a s2 (la denominem s11).
xii) $(\neg q \vee s)$, per R3b aplicada a s11 i a s5 (la denominem s12).
xiii) $((p \vee r) \rightarrow (\neg q \vee s))$, per R3c aplicada a s10 i a s12 (la denominem s13).
xiv) $(((p \rightarrow q) \wedge \neg(r \rightarrow \neg s)) \rightarrow ((p \vee r) \rightarrow (\neg q \vee s)))$, per R3c aplicat a s9 i a s13 (se n'obté la fórmula final).

f) Les subfórmules van sortint en el procés de generació descrit anteriorment:

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

PROBLEMA 4.26

Considereu la fórmula proposicional $(p \wedge \neg q) \to \neg(q \vee p)$. *Indiqueu quines de les següents (cadenes de caràcters) en són subfórmules:*

a) $\neg$
b) $p \wedge \neg q$
c) $(p \wedge \neg q)$
d) $\neg q$
e) $\to \neg($
f) $q \vee p$
g) $(q \vee p)$
h) $(p \vee q)$
i) $(\neg q \wedge p)$
j) $(q \wedge \neg p)$
k) $\neg q) \to$
l) $p \wedge \neg q)$
m) $(p \wedge \neg$
n) $\to$
o) $) \to$
p) q
q) $(\quad)$

Solució

a) No.
b) S'admet.
c) Sí.
d) Sí.
e) No.
f) S'admet.
g) Sí.
h) No.
i) No.
j) No.
k) No.
l) No.
m) No.
n) No.
o) No.
p) Sí.
q) No.

Observació. Les fórmules $p \wedge \neg q$ o $q \vee p$ no ho serien estrictament, ja que hi falten parèntesis exteriors, però s'admeten per a determinats usos, com per exemple per al càlcul de la taula de veritat de la fórmula completa, on escrivim les anteriors, sense que calgui escriure estrictament $(p \wedge \neg q)$ o $(q \vee p)$, que és també correcte, òbviament.

PROBLEMA 4.27

Considereu diverses fórmules proposicionals.

a) $(p \to q)$
b) $\neg(p \wedge q) \equiv ((\neg p) \vee (\neg q))$
c) $((p \to q) \leftrightarrow ((\neg q) \to (\neg p)))$
d) $(\neg(\neg(\neg(p))))$
e) $(r \wedge (s \wedge t))$
f) $(p \to q) \equiv ((\neg q) \to (\neg p))$
g) $(((\neg p) \to q) \to (r \to (\neg s)))$
h) $((p \vee q) \leftrightarrow ((\neg q) \vee p))$
i) $(((\neg(\neg(\neg(p))) \wedge (\neg q)) \to (\neg(((\neg r) \vee (\neg s)) \vee t))) \to (\neg p))$

Elimineu parèntesis (des d'estadis intermedis d'eliminació fins al màxim possible).

Solució. Per a algunes, és possible que no es puguin eliminar els parèntesis exteriors, per exemple si ha de ser subfórmula d'una fórmula més complexa, com és el cas de $(p \to q)$, subfórmula de $(p \to q) \to t$.

a) $p \to q$
b) $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ o, fins i tot, $\neg(p \wedge q) \equiv \neg p \vee \neg q$
c) $(p \to q) \leftrightarrow (\neg q \to \neg p)$
d) $\neg\neg\neg p$
e) $r \wedge (s \wedge t)$
f) $(p \to q) \equiv (\neg q \to \neg p)$ o, fins i tot, $p \to q \equiv \neg q \to \neg p$
g) $(\neg p \to q) \to (r \to \neg s)$
h) $(p \vee q) \leftrightarrow (\neg q \vee p)$
i) $((\neg\neg\neg p \wedge \neg q) \to (\neg(\neg r \vee \neg s \vee t))) \to \neg p$

PROBLEMA 4.28

Indiqueu totes les subfórmules de

$$\neg((\neg((p \wedge \neg q) \vee r) \wedge s) \to (\neg r \to \neg((r \wedge s) \to p))).$$

Solució. *Analitzem l'estructura bàsica*. Llegim per l'esquerra els parèntesis que s'obren i es tanquen; fent un seguiment dels parèntesis, observeu-ne l'estructura bàsica (és la negació d'un condicional):

$F := \neg((\neg((p \wedge \neg q) \vee r) \wedge s) \to (\neg r \to \neg((r \wedge s) \to p)))$

$F := \neg(F_1)$ o F_1, on $F_1 := (\neg((p \wedge \neg q) \vee r) \wedge s) \to (\neg r \to \neg((r \wedge s) \to p))$

$F_1 := (F_2 \to F_3)$ o $F_2 \to F_3$, on $F_2 := (\neg((p \wedge \neg q) \vee r) \wedge s)$ i $F_3 := (\neg r \to \neg((r \wedge s) \to p))$

$F_2 := (F_4 \wedge s)$, on $F_4 := \neg((p \wedge \neg q) \vee r)$

$F_3 := (F_5 \to F_6)$, on $F_5 := \neg r$ i $F_6 := \neg((r \wedge s) \to p)$

$F_4 := \neg F_7$, $F_7 := (F_8 \vee r)$, $F_8 := (p \wedge F_9)$, $F_9 := \neg q$

$F_6 := \neg F_{10}$, $F_{10} := (F_{11} \to p)$, $F_{12} := (r \wedge s)$,

Subfórmules (totes expressades o desenvolupades en termes de p, q, r, s):

$p, q, r, s, F, F_1, \ldots, F_{12}$.

Per tant, la llista de subfórmules és:

p, q, r, s (les lletres proposicionals)

$\neg((\neg((p \wedge \neg q) \vee r) \wedge s) \to (\neg r \to \neg((r \wedge s) \to p)))$ (la total)

$((\neg((p \wedge \neg q) \vee r) \wedge s) \to (\neg r \to \neg((r \wedge s) \to p)))$

$(\neg((p \wedge \neg q) \vee r) \wedge s)$

$(\neg r \to \neg((r \wedge s) \to p))$

I ara, per a cadascuna de les dues últimes:

subfórmules de $(\neg((p \wedge \neg q) \vee r) \wedge s)$	subfórmules de $(\neg r \rightarrow \neg((r \wedge s) \rightarrow p))$
s	$\neg r$
$\neg((p \wedge \neg q) \vee r)$	r
$((p \wedge \neg q) \vee r)$	$\neg((r \wedge s) \rightarrow p)$
r	$((r \wedge s) \rightarrow p)$
$(p \wedge \neg q)$	p
p	$(r \wedge s)$
$\neg q$	r
q	s

4.5. Taules de veritat. La taula de veritat d'una fórmula proposicional

Interessa el valor de veritat (0,1) d'una fórmula a partir dels valors de veritat (0,1) de les lletres proposicionals. Recordem: 0=fals, 1=cert; també F=fals, V=cert. També T=cert (de *true*).

Se'n pot donar una descripció conceptual o expressar el seu comportament veritatiu a través d'una taula, la *taula de veritat* de la fórmula. Per exemple:

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

Però, normalment, no ho tindrem com a la taula anterior, sinó que l'haurem d'obtenir a partir de les *subfórmules*, de manera progressiva a la pràctica.

La taula de veritat d'una fórmula proposicional es pot obtenir de manera fàcil i sistematitzada com una taula, amb columnes intermèdies corresponents a subfórmules, on el càlcul es fa de manera progressiva, d'acord amb l'estructura de la fórmula i de la manera en què es generaria a partir de les lletres. En la resolució d'exercicis, s'ha de procedir d'aquesta manera.

Com obtenir la taula de veritat d'una fórmula proposicional?

Sortosament, el procés és força intuïtiu i no sol presentar problemes. En primer lloc, es tracta d'identificar les lletres proposicionals i considerar totes les possibilitats de valors de veritat (0,1) de les variables conjuntament.

Hem de considerar una taula amb tantes files com valors de veritat siguin possibles per al conjunt de les variables o lletres. En el cas de dues variables, seran $2 \times 2 = 4$ files. Per exemple, amb les variables p, q, resultaria la taula de l'esquerra; la consideració de tots els valors de veritat possibles dóna lloc a les columnes corresponents a p, q. En el cas d'una fórmula amb tres variables, serien $2 \times 2 \times 2 = 8$ files, d'on resultaria la taula de la dreta:

p	q	$\cdots$
0	0	$\cdots$
0	1	$\cdots$
1	0	$\cdots$
1	1	$\cdots$

r	s	t	$\cdots$
0	0	0	$\cdots$
0	0	1	$\cdots$
0	1	0	$\cdots$
1	0	0	$\cdots$
0	1	1	$\cdots$
1	0	1	$\cdots$
1	1	0	$\cdots$
1	1	1	$\cdots$

Posteriorment, s'han d'obtenir les subfórmules fins arribar a la fórmula completa. Es tracta d'obtenir les taules de veritat de les diverses subfórmules, de manera que per a cada una d'elles només s'hagi d'aplicar la taula d'una connectiva bàsica a les subfórmules anteriors; per a passar a la columna següent, es tracta d'aplicar una de les taules bàsiques, d'alguna de les connectives $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$. S'han d'obtenir en seqüència, com si s'estigués generant la fórmula en aplicació de les regles de la gramàtica. Aquest ordre és el mateix que farem servir per a la taula, tot i que pot no ser únic.

Es tracta d'identificar la connectiva principal de la fórmula. Aquesta connectiva produeix la fórmula a partir de subfórmules, a les quals s'aplica el mateix procediment.

Exemple 4.14 Vegem el cas de la fórmula proposicional $(p \rightarrow q) \leftrightarrow (\neg p \rightarrow \neg q)$:

Lletres proposicionals: p, q

Subfórmules: p, q, $p \rightarrow q$, $\neg p$, $\neg q$, $\neg p \rightarrow \neg q$, $(p \rightarrow q) \leftrightarrow (\neg p \rightarrow \neg q)$

O també: p, q, $\neg p$, $\neg q$, $p \rightarrow q$, $\neg p \rightarrow \neg q$, $(p \rightarrow q) \leftrightarrow (\neg p \rightarrow \neg q)$

O també: p, q, $\neg q$, $\neg p$, $p \rightarrow q$, $\neg p \rightarrow \neg q$, $(p \rightarrow q) \leftrightarrow (\neg p \rightarrow \neg q)$

Connectiva principal de la fórmula: $\leftrightarrow$

És un bicondicional, un "... si, i només si, ...".

Vegem com s'obté en aquest exemple.

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

Observeu que es pot procedir en un altre ordre (limitadament, depenent de la fórmula):

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg p \to \neg q$	$(p \to q) \leftrightarrow (\neg p \to \neg q)$
0	0	1	1	1	1	1
0	1	1	0	1	0	0
1	0	0	1	0	1	0
1	1	0	0	1	1	1

Vegem ara un exemple amb tres variables proposicionals:

Exemple 4.15 Vegem com obtenir la taula de veritat de $((r \vee s) \wedge (r \wedge t)) \to (r \wedge t)$.

Lletres proposicionals; r, s, t

Subfórmules; r, s, t, $(r \vee s)$, $(r \wedge t)$, $((r \vee s) \wedge (r \wedge t))$, $((r \vee s) \wedge (r \wedge t)) \to (r \wedge t)$

La fórmula és un condicional. La connectiva principal és: $\to$

r	s	t	$r \vee s$	$r \wedge t$	$(r \vee s) \wedge (r \wedge t)$	$((r \vee s) \wedge (r \wedge t)) \to (r \wedge t)$
0	0	0	0	0	0	1
0	0	1	0	0	0	1
0	1	0	1	0	0	1
1	0	0	1	0	0	1
0	1	1	1	0	0	1
1	0	1	1	1	1	1
1	1	0	1	0	0	1
1	1	1	1	1	1	1

En resum: per descomposició i anàlisi de les subfórmules constituents, es pot escriure la taula de veritat corresponent. En primer lloc, s'escriuren les columnes dels operands i s'omplen amb totes les possibilitats per als valors de veritat. Després, s'escriuen les columnes corresponents a les subfórmules més senzilles i es va progressant cap a subfórmules més complexes, fins arribar a la fórmula final.

Vegem uns quants exercicis d'obtenció de taules de veritat:

PROBLEMA 4.29

La connectiva NAND, corresponent a NOT(AND), es defineix com $\neg(p \wedge q)$ *i es denota per* $p|q$. *És a dir,* $(p|q) = p(NAND)q = \neg(p \wedge q)$. *Escriviu la seva taula de veritat.*

Solució. *Anàlisi de la fórmula*:

Lletres: p, q

Subfórmules: $p, q, (p \wedge q), \neg(p \wedge q)$

p	q	$p \wedge q$	$\neg(p \wedge q)$ (NAND, $\mid$)
0	0	0	**1**
0	1	0	**1**
1	0	0	**1**
1	1	1	**0**

PROBLEMA 4.30

La connectiva NOR, corresponent a NOT(OR), es defineix com $\neg(p \vee q)$ *i es denota per* $p \downarrow q$. *Per tant,* $(p \downarrow q) = p(NOR)q = \neg(p \vee q)$. *Obteniu la taula de veritat.*

Solució. *Anàlisi de la fórmula*:

Lletres: p, q

Subfórmules: $p, q, (p \vee q), \neg(p \vee q)$

p	q	$p \vee q$	$\neg(p \vee q)$ (NOR, $\downarrow$)
0	0	0	**1**
0	1	1	**0**
1	0	1	**0**
1	1	1	**0**

PROBLEMA 4.31

Obteniu la taula de veritat la fórmula proposicional $(\neg p \wedge q) \vee (p \wedge \neg q)$.

Solució. *Anàlisi de la fórmula*:

Lletres proposicionals (operands, si la considerem una nova connectiva): p, q

Subfórmules (fem una lectura "de dintre cap enfora", com si generéssim les subfórmules a partir de les lletres; s'apliquen les regles de generació (en realitat, és una anàlisi de fora cap endins)):

p, q
$\neg p$, $\neg q$
$(\neg p \wedge q)$, $(p \wedge \neg q)$
$(\neg p \wedge q) \vee (p \wedge \neg q)$

És una disjunció. Connectiva principal: $\vee$

La taula de veritat és:

p	q	$\neg p$	$\neg q$	$\neg p \wedge q$	$p \wedge \neg q$	$(\neg p \wedge q) \vee (p \wedge \neg q)$
0	0	1	1	0	0	**0**
0	1	1	0	1	0	**1**
1	0	0	1	0	1	**1**
1	1	0	0	0	0	**0**

PROBLEMA 4.32

Obteniu la taula de veritat de la fórmula proposicional: $(p \vee q) \wedge \neg(p \wedge q)$.

Solució. *Anàlisi de la fórmula*:

Lletres: p, q

Estructura i generació de la fórmula $G = (p \vee q) \wedge \neg(p \wedge q)$:

Fem una lectura "de fora cap endins", des de la fórmula completa fins a les lletres proposicionals.

La fórmula G és una conjunció, aplicada a les fórmules (subfórmules): $G_1 = (p \vee q)$, $G_2 = \neg(p \wedge q)$, de manera que $G = G_1 \wedge G_2$.

G_1 és una disjunció, de les subfórmules p, q (i aquí hem acabat).

G_2 és una negació, de la subfórmula $G_{21} = (p \wedge q)$; finalment, G_{21} és conjunció de les subfórmules p, q, i aquí hem acabat.

p	q	G_1	G_{21}	G_2	$(p \vee q) \wedge \neg(p \wedge q)$ $(= G)$
0	0	0	0	1	**0**
0	1	1	0	1	**1**
1	0	1	0	1	**1**
1	1	1	1	0	**0**

p	q	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
0	0	0	0	1	**0**
0	1	1	0	1	**1**
1	0	1	0	1	**1**
1	1	1	1	0	**0**

Observació. És la fórmula de la disjunció exclussiva.

Als problemes anteriors, tenim dues fórmules proposicionals, amb les mateixes lletres:

$$G = (\neg p \wedge q) \vee (p \wedge \neg q)$$

$$H = (p \vee q) \wedge \neg(p \wedge q)$$

Són fórmules *diferents*, ja que com a cadenes de caràcters no coincideixen, com es pot veure comparant per posicions. Ara bé, s'ha observat que, malgrat ser diferents, *tenen la mateixa taula de veritat*. Això significa que, des del punt de vista lògic exerceixen la mateixa funció, tenen la mateixa funcionalitat lògica. Podem substituir l'una per l'altra en una fórmula, a l'efecte de la funcionalitat lògica. Amb els mateixos "inputs (0,1)" per a les lletres, s'obté la mateixa sortida per a la fórmula.

Aquest és un concepte important, el de l'equivalència lògica entre fórmules proposicionals, que es tractarà a la secció següent i en seccions posteriors (4.6, 4.7):

4.6. Equivalències lògiques

Definició 4.4 *Donades dues fórmules proposicionals, en termes de les mateixes lletres proposicionals, es diu que són **lògicament equivalents** si les taules de veritat respectives coincideixen. La notació corresponent és $F \equiv G$, si F, G són les fórmules. És a dir, si, per a totes les possibles assignacions de valors veritatius a les lletres proposicionals, les fórmules tenen valors de veritat coincidents per a cada cas.*

Observació. Noteu que el símbol $\equiv$ no és cap connectiva, ni pertany al llenguatge de les fórmules proposicionals. És del llenguatge en què expressem propietats sobre les fórmules proposicionals. L'afirmació "les fórmules proposicionals F, G són (lògicament) equivalents" és una propietat que s'afirma sobre fórmules: no pertany al llenguatge de proposicions. L'expressió $F \equiv G$ no és una fórmula del llenguatge de proposicions.

No equivalència lògica. Dues fórmules proposicionals no són lògicament equivalents si les taules de veritat no coincideixen. El símbol corresponent és $\not\equiv$. Exemple: $F \not\equiv G$.

4.6.1. Demostració d'equivalències lògiques per taules de veritat

▷ ***Com es demostra que dues fórmules proposicionals són lògicament equivalents?*** Com a conseqüència de la definició, el **mètode bàsic** per a la demostració d'equivalència lògica és el càlcul de les taules de veritat respectives i la comprovació posterior que coincideixen. És el que fem en els exemples i exercicis següents. El mètode és totalment rutinari i mai no presenta cap dificultat.

Exemple 4.16 $p \vee p \equiv p \qquad p \wedge p \equiv p$.

És conceptualment obvi: demostrable per taules de veritat. ■

Malgrat la simplicitat d'aquestes equivalències, poden ser útils per a simplificacions en fórmules, substituint $p \vee p$ per una única p. També es pot aplicar a l'inrevés, si ens cal una repetició de la lletra p als efectes de manipulació en una fórmula: substituint p per $p \vee p$, introduïm una segona còpia de p per a propòsits de reagrupament en una manipulació per tal de resoldre un problema.

Exemple 4.17 Vegem les equivalències lògiques (o que les fórmules indicades són lògicament equivalents):

$$p \equiv (p \vee p)$$
$$p \equiv (p \wedge p)$$

Escrivim una taula conjunta per a veure que tenen les mateixes taules de veritat:

p	$p \vee p$	$p \wedge p$
0	**0**	**0**
1	**1**	**1**

Les dues fórmules de l'esquerra corresponen a la disjunció exclusiva:

Exemple 4.18 Demostreu les equivalències lògiques:

$$(\neg p \wedge q) \vee (p \wedge \neg q) \equiv (p \vee q) \wedge \neg(p \wedge q) \equiv \neg(p \leftrightarrow q).$$

Si denotem:

$$G = (\neg p \wedge q) \vee (p \wedge \neg q)$$
$$H = (p \vee q) \wedge \neg(p \wedge q),$$

ja hem demostrat a la secció anterior (4.5) que són equivalents ($G \equiv H$), per coincidència de taules de veritat. Ho resumim a la taula següent, on s'observa la coincidència de les columnes respectives:

p	q	$(\neg p \wedge q) \vee (p \wedge \neg q)$	$(p \vee q) \wedge \neg(p \wedge q)$	$p \leftrightarrow q$	$\neg(p \leftrightarrow q)$
0	0	**0**	**0**	1	**0**
0	1	**1**	**1**	0	**1**
1	0	**1**	**1**	0	**1**
1	1	**0**	**0**	1	**0**

Així, $G \equiv H \equiv \neg(p \leftrightarrow q)$, i són dos a dos equivalents. ■

Un exemple molt senzill és el de la doble negació:

Exemple 4.19 Demostració de l'equivalència lògica de la doble negació:

$$\neg\neg p \equiv p$$

Vegem que coincideixen les taules de veritat:

p	$\neg p$	$\neg\neg p$
0	1	0
1	0	1

Per tant, són lògicament equivalents. ■

Equivalències importants són la de la distributivitat: de la disjunció respecte de la conjunció i també de la conjunció respecte de la disjunció, és a dir:

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

(distributivitat de la disjunció $\vee$ respecte de la conjunció $\wedge$)

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

(distributivitat de la conjunció $\wedge$ respecte de la disjunció $\vee$)

Demostrem-ne una com a exercici, amb tres lletres proposicionals (distributivitat de la "i" respecte de la "o"); l'altra es demostra anàlogament:

PROBLEMA 4.33

Demostreu l'equivalència lògica: $r \wedge (s \vee t) \equiv (r \wedge s) \vee (r \wedge t)$

Solució. Comprovem que les taules de veritat coincideixen:

r	s	t	$s \vee t$	$r \wedge s$	$r \wedge t$	$r \wedge (s \vee t)$	$(r \wedge s) \vee (r \wedge t)$
0	0	0	0	0	0	**0**	**0**
0	0	1	1	0	0	**0**	**0**
0	1	0	1	0	0	**0**	**0**
1	0	0	0	0	0	**0**	**0**
0	1	1	1	0	0	**0**	**0**
1	0	1	1	0	1	**1**	**1**
1	1	0	1	1	0	**1**	**1**
1	1	1	1	1	1	**1**	**1**

Unes equivalències molt importants són les de De Morgan per a fórmules proposicionals:

Equivalències lògiques de De Morgan:

$\neg(p \vee q) \equiv (\neg p \wedge \neg q)$ (De Morgan)
(la negació d'una disjunció "és" una conjunció de negacions);

$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ (De Morgan)
(la negació d'una conjunció "és" una disjunció de negacions).

A la secció posterior 4.7, es veuen de manera més completa. Vegem aquí, només com a exemple de com provar l'equivalència lògica, la demostració d'una d'elles:

Exemple 4.20 Demostrem l'equivalència lògica: $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ (De Morgan). Comprovarem que les taules de veritat coincideixen:

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
0	0	1	1	0	1	1
0	1	1	0	0	1	1
1	0	0	1	0	1	1
1	1	0	0	1	0	0

■

Una de les aplicacions de lleis de De Morgan és per negar amb seguretat expressions complicades, i de forma automatitzada. Vegem-ne un exemple senzill:

Exemple 4.21 Obteniu negacions de:

"plou i fa sol"

"plou o fa sol"

Formalitzant, amb $p =$“plou”, $q =$“fa sol”, les frases són, respectivament:

$$p \wedge q \text{ (“plou i fa sol”)}$$
$$p \vee q \text{ (“plou o fa sol”)}$$

Aplicant les equivalències de De Morgan, resulta:

– la negació de “plou i fa sol” correspon a $\neg(p \wedge q) \equiv \neg p \vee \neg q$, és a dir, “no plou o no fa sol”.
– la negació de “plou o fa sol” correspon a $\neg(p \vee q) \equiv \neg p \wedge \neg q$, és a dir, “no plou i no fa sol”, que també podem reescriure com “ni plou ni fa sol”. ■

Vegem com podem expressar el bicondicional en termes del condicional i la negació. Es tracta de formular una equivalència lògica:

PROBLEMA 4.34

Demostreu l'equivalència que expressa el bicondicional en termes del condicional i la negació:

$$p \leftrightarrow q \equiv \neg((p \to q) \to \neg(q \to p))$$

Solució. Per a provar l'equivalència anterior, amb la qual expressem el bicondicional mitjançant el condicional i la negació:

$$p \leftrightarrow q \equiv \neg((p \to q) \to \neg(q \to p)),$$

vegem la igualtat de les taules de veritat respectives
(on $F = (p \to q) \to \neg(q \to p)$):

p	q	$p \to q$	$q \to p$	$\neg(q \to p)$	$(p \to q) \to \neg(q \to p)$	$\neg F$	$p \leftrightarrow q$
0	0	1	1	0	0	1	1
0	1	1	0	1	1	0	0
1	0	0	1	0	1	0	0
1	1	1	1	0	0	1	1

4.6.2. Demostració d'equivalències lògiques sense taules

▷ ***Es pot demostrar d'alguna altra manera, a part de per taules de veritat, que dues fórmules proposicionals són lògicament equivalents?*** Depenent del cas, és possible demostrar-ho utilitzant altres equivalències lògiques ja demostrades i disponibles (per això és interessant disposar d'una llista d'equivalències lògiques per tal de resoldre problemes de demostració d'equivalències). En demostrarem a la secció posterior 4.7. Moltes vegades s'han d'encadenar equivalències.

És immediat veure les propietats següents, a partir de la igualtat de les taules de veritat:

$F \equiv F$ (propietat reflexiva, reflexivitat)

Si $F \equiv G$, aleshores $G \equiv F$ (propietat simètrica, simetria)

Si $F \equiv G$ i $G \equiv H$, aleshores $F \equiv H$ (propietat transitiva, transitivitat)

També, i per taules, $\neg F \equiv \neg G$ si, i només si, $F \equiv G$.

Encadenant equivalències. Les propietats anteriors són útils moltes vegades en demostracions. En particular, generalitzant la tercera, en algunes demostracions es produeix un encadenament d'equivalències entre fórmules i podem deduir que la primera és lògicament equivalent a l'última (de fet, totes són equivalents amb totes, ja que totes les taules de veritat coincideixen) ($n \geq 2$):

De $F_1 \equiv F_2$, $F_2 \equiv F_3$, $\cdots$, $F_{n-1} \equiv F_n$, se'n deriva $F_1 \equiv F_n$.

Més informalment, $(F_1 \equiv F_2 \equiv F_3 \equiv \cdots \equiv F_{n-1} \equiv F_n) \Rightarrow F_1 \equiv F_n$.

Veurem molts exemples d'aplicació d'aquesta idea a la secció següent 4.7. A continuació un exemple simple, que és una variant argumental del resultat pel qual podem expressar "o" en termes de "no" i "i"; a l'apartat següent se'n mostra una altra variant argumental.

Exemple 4.22 (Encadenant equivalències)

$$p \vee q \overset{(1)}{\equiv} \neg\neg(p \vee q) \overset{(2)}{\equiv} \neg(\neg(p \vee q)) \overset{(2)}{\equiv} \neg(\neg p \wedge \neg q).$$

Explicació:

(1): per l'equivalència de doble negació

(2): per simple reescriptura de la fórmula

(3): una de les equivalències de De Morgan (aplicada a la subfórmula $\neg(p \vee q)$ i substitució a la fórmula). ■

Exemple 4.23 (Encadenant equivalències)

Expressió de la conjunció ("i", $\wedge$) en termes de la negació ("no", $\neg$) i la disjunció ("0", $\vee$).

$$p \wedge q \overset{(1)}{\equiv} \neg\neg(p \wedge q) \overset{(2)}{\equiv} \neg(\neg(p \wedge q)) \overset{(2)}{\equiv} \neg(\neg p \vee \neg q).$$

Explicació:

(1): per l'equivalència de doble negació

(2): per simple reescriptura de la fórmula

(3): una de les equivalències de De Morgan (aplicada a una subfórmula, $\neg(p \wedge q)$ i substitució a la fórmula). ■

Una altra possibilitat per a demostrar equivalències lògiques és obtenir *cadenes d'equivalències*:

$$F_1 \equiv F_2 \equiv F_3 \equiv \cdots \equiv F_{n-1} \equiv F_n$$

$$G_1 \equiv G_2 \equiv G_3 \equiv \cdots \equiv G_{m-1} \equiv G_m$$

Si $F_n \equiv G_m$, aleshores $F_1 \equiv G_1$ (tenen les mateixes taules de veritat). També es justifica per transitivitat o bé es refà l'esquema i es redueix a una única seqüència d'equivalències:

$$F_1 \equiv F_2 \equiv F_3 \equiv \cdots \equiv F_{n-1} \equiv F_n \equiv G_m \equiv G_{m-1} \equiv \cdots \equiv G_3 \equiv G_2 \equiv G_1$$

També es pot comprovar a través de les taules de veritat que

$$F \equiv G \text{ si, i només si, } \neg F \equiv \neg G.$$

Exemple 4.24 Com a exemple d'aplicació de l'afirmació anterior, obtenim un dels resultats anteriors, a partir d'una de les lleis de De Morgan:

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \Rightarrow \neg(\neg(p \vee q)) \equiv \neg(\neg p \wedge \neg q) \Rightarrow p \vee q \equiv \neg(\neg p \wedge \neg q). \blacksquare$$

Als dos exemples anteriors, s'han efectuat substitucions. També tenim que

$F \equiv G \Rightarrow \neg F \equiv \neg G$ no és més que un cas de substitució: F de $\neg F$ és substituïda per l'equivalent G per obtenir l'equivalència amb $\neg G$. Estudiem i formulem aquesta possibilitat d'efectuar substitucions:

▷ ***Substitució de subfórmules per fórmules equivalents***. Podem substituir una subfórmula per una fórmula equivalent i obtenir una nova fórmula equivalent a l'original? La resposta és afirmativa. Es precisa en el teorema següent.

Vegem un exemple addicional d'aquesta situació.

Teorema 4.1 *Sigui F una fórmula proposicional i sigui G una subfórmula de F. Sigui G' una fórmula proposicional lògicament equivalent a G, és a dir, $G \equiv G'$. Sigui F' el resultat de substituir G per G' a la fórmula F. Aleshores $F \equiv F'$. S'afirma per a una o més substitucions, a una o més ocurrències de G.*

Per tant, podem substituir per equivalències i obtenir una nova equivalència.

Aquest resultat s'utilitza gairebé de manera intuïtiva. És molt útil per a demostrar i obtenir noves equivalències lògiques i per a obtenir simplificacions o expressions alternatives a algunes fórmules (de fet, noves equivalències). Necessita demostració, que no fem aquí.

De fet, si analitzem què fem en un procés de substitució, podem veure que resulta de l'aplicació d'un nombre finit dels resultats següents, base de la substitució per fórmules equivalents:

(SUBS1) $F \equiv G \Rightarrow \neg F \equiv \neg G$
(SUBS2) $F \equiv G \Rightarrow F \vee H \equiv G \vee H$
(SUBS3) $F \equiv G \Rightarrow F \wedge H \equiv G \wedge H$
(SUBS4) $F \equiv G \Rightarrow F \to H \equiv G \to H$
(SUBS5) $F \equiv G \Rightarrow H \to F \equiv H \to G$
(SUBS6) $F \equiv G \Rightarrow F \wedge H \leftrightarrow G \wedge H$

Les afirmacions són certes: només cal raonar que les taules de veritat coincideixen.

No hi ha més casos, d'acord amb la gramàtica del llenguatge, que és la que diu com es generen les fórmules proposicionals.

Vegem-ne un exemple:

Exemple 4.25 Suposant que tenim l'equivalència $p \to q \equiv \neg p \vee q$ (vegeu llista a la secció 4.6.4), podem escriure la nova equivalència per substitució:

$$(p \wedge (p \to q)) \to q \equiv (p \wedge (\neg p \vee q)) \to q$$

O bé la nova es pot obtenir a partir de l'equivalència $p \to q \equiv \neg p \vee q$, aplicant les regles anteriors:

$p \to q \equiv \neg p \vee q$,
$(p \to q) \equiv (\neg p \vee q)$, d'on per (SUBS3)
$p \wedge (p \to q) \equiv p \wedge (\neg p \vee q)$
$(p \wedge (p \to q)) \equiv (p \wedge (\neg p \vee q))$, d'on per (SUBS4)
$(p \wedge (p \to q)) \to q \equiv (p \wedge (\neg p \vee q)) \to q$. ■

Vegem un exemple addicional d'aquesta situació:

Exemple 4.26 Expressió de la disjunció en termes de la negació i la conjunció.

En manipulacions de fórmules, moltes vegades substituïm p per $\neg\neg p$ si ens convé per a alguna deducció o, a l'inrevés, substituïm $\neg\neg p$ per p. Segons l'afirmació, obtenim equivalència amb la fórmula resultant. És el que passa quan escrivim

$$p \vee q \equiv (\neg\neg p \vee q)$$

Hem aplicat l'equivalència de la doble negació i la substitució.

Aquest pas pot formar part d'algun procés deductiu. Imaginem que es tracta de provar que podem expressar la disjunció en termes de negació i conjunció. Podem continuar l'argumentació:

$p \vee q \equiv$

$\equiv \neg\neg p \vee \neg\neg q$, per doble negació i substitució, dues vegades
$\equiv \neg(\neg p) \vee \neg(\neg q)$ (reescriptura)
$\equiv \neg(\neg p \wedge \neg q)$ (per una de les equivalències de De Morgan)

Així, hem aconseguit expressar "o" en funció de "no" i "i".

També hem demostrat una equivalència fent servir altres equivalències. Naturalment, també es pot demostrar comprovant que les taules de veritat són les mateixes. ■

4.6.3. No-equivalència lògica: com demostrar-la

Com demostrar la no-equivalència lògica?

▷ ***Quan dues fórmules proposicionals no són lògicament equivalents?*** Quan les taules de veritat no coincideixen. N'hi ha prou amb una fila per a la qual els valors de veritat de les fórmules són diferents (no cal que sigui per a totes les files).

Vegem un exemple interessant de no-equivalència. Està molt estesa la creença que la negació d'un condicional $p \to q$ és $\neg p \to \neg q$. És fals! Vegem que les fórmules són no equivalents lògicament, és a dir:

$\neg(p \to q) \not\equiv \neg p \to \neg q$:

PROBLEMA 4.35

Vegeu que $\neg(p \to q)$ i $\neg p \to \neg q$ no són lògicament equivalents.

Solució. Comprovem que les taules de veritat de la fórmula no coincideixen:

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg(p \to q)$	$\neg p \to \neg q$
0	0	1	1	1	0	1
0	1	1	0	1	0	0
1	0	0	1	0	1	1
1	1	0	0	1	0	1

Ens podem plantejar si $\neg(p \to q)$ serà (lògicament equivalent a) algun dels següents: $\neg q \to \neg p$, $\neg p \to q$, $p \to \neg q$, $q \to p$, $q \to \neg p$, $\neg q \to p$.

La resposta és negativa i es pot comprovar veient que les taules de veritat no coincideixen, anàlogament al problema anterior.

Això no ens diu quina és la fórmula correcta de negació d'un condicional. Avançant idees, és:

$\neg(p \to q) \equiv p \wedge \neg q$ (vegeu secció posterior 4.7 i subsecció 4.6.4)

Una altra manera d'abordar el problema, sense taules de veritat, consisteix a poder demostrar que són respectivament equivalents a d'altres fórmules per a les quals podem provar que no són equivalents.

$$F = F_1 \equiv F_2 \equiv F_3 \equiv \cdots \equiv F_{n-1} \equiv F_n$$
$$G = G_1 \equiv G_2 \equiv G_3 \equiv \cdots \equiv G_{m-1} \equiv G_m$$

Si $F_n \not\equiv G_m$, aleshores resulta $F_1 \not\equiv G_1$. En efecte, si fos $F_1 \equiv G_1$, aleshores, per transitivitat, hauria de ser $F_n \equiv G_m$.

4.6.4. Llista d'equivalències lògiques importants

Com hem vist, és útil disposar d'equivalències lògiques ja demostrades i disponibles, per a demostrar-ne de noves, moltes vegades mitjançant substitució de subfórmules. Segueix una llista; les demostracions es veuran a la secció posterior 4.7 (seran exercicis de demostració d'equivalències).

Donem una llista de les equivalències més importants. S'enuncien per a fórmules en termes de les lletres proposicionals.

S'indiquen les que són especialment importants per a l'estructura o esquema de demostracions.

a) $p \vee (p \wedge q) \equiv p$

b) $p \wedge (p \vee q) \equiv p$

c) $p \wedge p \equiv p$ (idempotència)

d) $p \vee p \equiv p$ (idempotència)

e) $\neg\neg p \equiv p$ (doble negació)

f) $p \vee q \equiv q \vee p$ (commutativitat de la disjunció)

g) $p \wedge q \equiv q \wedge p$ (commutativitat de la conjunció)

h) $p \vee (q \vee r) \equiv (p \vee q) \vee r$ (associativitat de la disjunció)

i) $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ (associativitat de la conjunció)

j) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ (distributivitat de $\vee$ respecte de $\wedge$)

k) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (distributivitat de $\wedge$ respecte de $\vee$)

l) $\neg(p \vee q) \equiv \neg p \wedge \neg q$ (De Morgan) (negació de la disjunció)
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ (De Morgan) (negació de la disjunció)

m) $p \rightarrow q \equiv \neg p \vee q$ (condicional en termes de negació i disjunció) [demostracions]

n) $\neg(p \rightarrow q) \equiv p \wedge \neg q$ (negació del condicional) [demostracions]

o) $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ [demostracions]
(bicondicional en termes de condicional i conjunció)

p) $(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$ (casos, “o” a l'antecedent) [demostracions]

q) $p \rightarrow q \equiv (\neg q \rightarrow \neg p)$ (equivalència del contrarecíproc) [demostracions]

r) $p \rightarrow (q \vee r) \equiv (p \wedge \neg q) \rightarrow r \equiv (p \wedge \neg r) \rightarrow q$ (“o” en el conseqüent) [demostracions]

s) $p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r \equiv q \rightarrow (p \rightarrow r)$ [demostracions]

Per a fórmules proposicionals qualssevol (F, G, H), es poden derivar de les anteriors. Es poden obtenir per substitució de les lletres proposicionals per fórmules proposicionals.

a) $F \vee (F \wedge G) \equiv F$

b) $F \wedge (F \vee G) \equiv F$

c) $F \wedge F \equiv F$

d) $F \vee F \equiv F$

e) $\neg\neg F \equiv F$ (doble negació)

f) $F \vee G \equiv G \vee F$ (commutativitat)

g) $F \wedge G \equiv G \wedge F$ (commutativitat)

h) $F \vee (G \vee H) \equiv (F \vee G) \vee H$ (associativitat)

i) $F \wedge (G \wedge H) \equiv (F \wedge G) \wedge H$ (associativitat)

j) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ (distributivitat de $\vee$ respecte de $\wedge$)

k) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ (distributivitat de $\wedge$ respecte de $\vee$)

l) $\neg(F \vee G) \equiv \neg F \wedge \neg G$ (De Morgan)

$\neg(F \wedge G) \equiv \neg F \vee \neg G$ (De Morgan)

m) $F \rightarrow G \equiv \neg F \vee G$ (condicional en termes de negació i disjunció)

n) $\neg(F \rightarrow G) \equiv F \wedge \neg G$ (negació del condicional)

o) $F \leftrightarrow G \equiv (F \rightarrow G) \wedge (G \rightarrow F)$
(bicondicional en termes de condicional i conjunció)

p) $(F \vee G) \rightarrow H \equiv (F \rightarrow H) \wedge (G \rightarrow H)$ (casos)

q) $F \rightarrow G \equiv (\neg G \rightarrow \neg F)$ (contrarecíproc)

r) $F \rightarrow (G \vee H) \equiv (F \wedge \neg G) \rightarrow H \equiv (F \wedge \neg H) \rightarrow G$

s) $F \rightarrow (G \rightarrow H) \equiv (F \wedge G) \rightarrow H \equiv G \rightarrow (F \rightarrow H)$

4.7. Demostració de les equivalències lògiques importants

4.7.1. Llista d'equivalències

Repetim per a referència la llista de les equivalències més importants. S'enuncien per a fórmules en termes de les lletres proposicionals. S'indiquen les que ja s'han demostrat com a exemple i exercici a la secció anterior "equivalències lògiques" (4.6).

a) $p \vee (p \wedge q) \equiv p$

b) $p \wedge (p \vee q) \equiv p$

c) $p \wedge p \equiv p$ (idempotència)

d) $p \vee p \equiv p$ (idempotència)

e) $\neg\neg p \equiv p$ (doble negació) [ja demostrada anteriorment]

f) $p \vee q \equiv q \vee p$ (commutativitat de la disjunció)

g) $p \wedge q \equiv q \wedge p$ (commutativitat de la conjunció)

h) $p \vee (q \vee r) \equiv (p \vee q) \vee r$ (associativitat de la disjunció)

i) $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ (associativitat de la conjunció)

j) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
(distributivitat de $\vee$ respecte de $\wedge$) [ja demostrada anteriorment]

k) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (distributivitat de $\wedge$ respecte de $\vee$)

l) $p \rightarrow q \equiv \neg p \vee q$ (condicional en termes de negació i disjunció)

m) $\neg(p \rightarrow q) \equiv p \wedge \neg q$ (negació del condicional)

n) $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
(bicondicional en termes de condicional i conjunció)

o) $(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$ (casos)

p) $p \rightarrow q \equiv (\neg q \rightarrow \neg p)$ (equivalència del contrarecíproc)

q) $\neg(p \vee q) \equiv \neg p \wedge \neg q$ (De Morgan)
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ (De Morgan) [ja demostrat anteriorment]

r) $p \rightarrow (q \vee r) \equiv (p \wedge \neg q) \rightarrow r \equiv (p \wedge \neg r) \rightarrow q$

s) $p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r \equiv q \rightarrow (p \rightarrow r)$

A part del mètode de comprovació d'igualtat de taules de veritat, hi ha altres mètodes de demostració d'equivalències lògiques (vegeu seccions anteriors del capítol dedicades a aquesta qüestió):

- Utilitzar equivalències lògiques ja demostrades, que es poden substituir a les fórmules.
- Es prova $F \equiv H$ i $G \equiv H$ per a alguna fórmula proposicional H convenient i es conclou $F \equiv G$ per transitivitat.
- Una barreja de les idees anteriors.

En veurem exemples a continuació.

4.7.2. Demostracions d'equivalències lògiques i exemples d'ús

► 1. *Demostració de l'equivalència lògica de la doble negació (demostrada anteriorment)*:

$$\neg\neg p \equiv p \tag{4.1}$$

Vegem que coincideixen les taules de veritat:

p	$\neg p$	$\neg\neg p$
0	1	0
1	0	1

Per tant, són lògicament equivalents.

► 2. *Demostració de les equivalències lògiques de De Morgan (també lleis de De Morgan)*:

$$\neg(p \vee q) \equiv (\neg p \wedge \neg q) \tag{4.2}$$
$$\neg(p \wedge q) \equiv (\neg p \vee \neg q) \tag{4.3}$$

Demostració de la primera: $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

Per taules de veritat (són equivalents perquè les taules de veritat coincideixen):

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

Demostració de la segona: $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$.

Mètode 1. La segona es pot demostrar de la mateixa manera que la primera, veient que les taules de veritat coincideixen (s'ha vist anteriorment com a exemple, en la secció anterior 4.6).

Mètode 2. En comptes de fer-ho així, vegem que es pot demostrar la segona (4.3) a partir de la primera (4.2), que se suposa demostrada, com és el cas:

$\neg(p \wedge q) \equiv$

$\equiv \neg(\neg\neg p \wedge \neg\neg q)$ per (4.1)
(equivalència de la doble negació i substitució dues vegades).

$\equiv \neg\neg(\neg p \vee \neg q)$ per (4.2).

$\equiv \neg p \vee \neg q$, per (4.1) (equivalència de la doble negació). ■

Mètode 3. L'argumentació es pot reformular segons diverses variants. Per exemple:

$$p \wedge q \overset{(\alpha)}{\equiv} \neg\neg p \wedge \neg\neg q \overset{(\beta)}{\equiv} \neg(\neg p \vee \neg q)$$

α : per l'equivalència de doble negació (4.1).

β: per l'equivalència de De Morgan (4.2).

A partir del que s'ha obtingut, aplicant $F \equiv G \Rightarrow \neg F \equiv \neg G$, podem escriure:

$p \wedge q \equiv \neg(\neg p \vee \neg q)$, d'on, aplicant $F \equiv G \Rightarrow \neg F \equiv \neg G$,

$\neg(p \wedge q) \equiv \neg(\neg(\neg p \vee \neg q))$, d'on, per reescriptura,

$\neg(p \wedge q) \equiv \neg\neg(\neg p \vee \neg q))$, d'on, per l'equivalència de doble negació,

$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$ ■

Observació. El resultat $F \equiv G \Rightarrow \neg F \equiv \neg G$ no s'ha demostrat, però és molt intuïtiu i fàcil de provar, per exemple per taules de veritat.

Observació. També es pot demostrar la primera a partir de la segona, que se suposa demostrada, per exemple, per taules de veritat. En efecte, vegem-ho com a exemple:

Exemple 4.27 Provem $\neg(p \wedge q) \equiv \neg p \vee \neg q \Rightarrow \neg(p \vee q) \equiv \neg p \wedge \neg q$

$$\begin{aligned}
&\neg(p \vee q) \equiv \\
&\equiv \neg(\neg\neg p \vee \neg\neg q) && \text{(per doble negació)}, \\
&\equiv \neg(\neg(\neg p \wedge \neg q)) && \text{(per De Morgan (segona))}, \\
&\equiv \neg\neg(\neg p \wedge \neg q)) && \text{(per reescriptura)}, \\
&\equiv \neg p \wedge \neg q && \text{(per doble negació)}. \ ■
\end{aligned}$$

Un exemple d'ús d'alguna de les equivalències de De Morgan:

Exemple 4.28 Com negar "fa fred i fa vent"?

Siguin $H =$ "fa fred", $J =$ "fa vent". En aplicació de l'equivalència de De Morgan de negació de la conjunció $(H \wedge J)$, la negació és "no fa fred o no fa vent" $(\neg H \vee \neg J)$. ■

► 3. *Demostració de l'equivalència lògica que expressa el condicional en termes de* $\neg$ *i* $\vee$:

$$p \rightarrow q \equiv \neg p \vee q \tag{4.4}$$

Vegem rutinàriament que les taules de veritat coincideixen i, per tant, són equivalents lògicament:

p	q	$\neg p$	$p \to q$	$\neg p \vee q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

És important per a expressar la disjunció en termes del condicional:

$A \vee B \equiv \neg A \to B \equiv \neg B \to A$. En efecte, $A \vee B \equiv \neg(\neg A) \vee B \equiv \neg A \to B$ i també $A \vee B \equiv B \vee A \equiv \neg(\neg B) \vee A \equiv \neg B \to A$.

Vegem-ne un exemple:

Exemple 4.29 Són equivalents:

"El cotxe és blau o vermell" (és a dir, "el cotxe és blau o el cotxe és vermell"), $(B \vee V)$,
"Si el cotxe no és blau, aleshores és vermell" $(\neg B \to V)$,
"Si el cotxe no és vermell, aleshores és blau" $(\neg V \to B)$,

amb $B =$"el cotxe és blau", $V =$"el cotxe és vermell" ■

► 4. *Demostració de l'equivalència lògica de negació del condicional en termes de* $\neg$ *i* $\wedge$:

$$\neg(p \to q) \equiv p \wedge \neg q \tag{4.5}$$

És una equivalència molt important. Val la pena fixar-s'hi especialment, ja que la negació del condicional es fa erròniament en moltes ocasions. Se'n han mostrat alguns dels errors en un exercici anterior.

Mètode 1. Comprovant que les taules de veritat coincideixen.

p	q	$\neg q$	$p \to q$	$\neg(p \to q)$	$p \wedge \neg q$
0	0	1	1	0	0
0	1	0	1	0	0
1	0	1	0	1	1
1	1	0	1	0	0

Per tant, són equivalents.

Mètode 2. Fent servir equivalències lògiques ja demostrades, per exemple qualsevol de les anteriors que ens convingui.

$$\neg(p \to q) \overset{(4.4)}{\equiv} \neg(\neg p \vee q) \overset{(4.2)}{\equiv} \neg\neg p \wedge \neg q \overset{(4.1)}{\equiv} p \wedge \neg q$$

Una situació en la qual és convenient negar correctament un condicional és en el mètode de demostració per reducció a l'absurd (vegeu capítol posterior): si l'afirmació que s'ha de demostrar té la forma d'un condicional, el mètode comença amb la negació del condicional.

► 5. *Demostració de l'equivalència lògica del contrarecíproc*:

$$p \to q \equiv \neg q \to \neg p \tag{4.6}$$

És una equivalència molt important per a demostracions (pel contrarecíproc).

Mètode 1. Comprovant que les taules de veritat coincideixen. És rutina.

p	q	$\neg q$	$\neg p$	$p \to q$	$\neg q \to \neg p$
0	0	1	1	1	1
0	1	0	1	1	1
1	0	1	0	0	0
1	1	0	0	1	1

Les taules coincideixen: per tant, són equivalents.

Mètode 2. Fent servir equivalències lògiques ja demostrades, per exemple qualsevol de les anteriors que ens convingui.

$$\begin{aligned}
&\neg q \to \neg p \equiv \\
&\equiv \neg\neg q \vee \neg p \text{ (per (4.4))}, \\
&\equiv q \vee \neg p \text{ (per (4.1), doble negació)}, \\
&\equiv \neg p \vee q \text{ (per commutativitat de } \vee\text{)}, \\
&\equiv p \to q \text{ (per (4.4))}.
\end{aligned}$$

Vegem-ne un exemple en el llenguatge ordinari:

Exemple 4.30 Considerant $L =$"En Joan està lliure", $T =$"En Joan estudia a la tarda", l'enunciat:

"Si en Joan està lliure, aleshores estudia a la tarda" ($L \to T$)

equival a

"Si en Joan no estudia a la tarda, aleshores no està lliure" ($\neg T \to \neg L$),

d'acord amb l'equivalència. ■

Exemple 4.31 Per a nombres enters:

"Si un nombre és parell, aleshores el seu quadrat és parell"

Contrarecíproc o proposició contrarecíproca de l'anterior:

"Si el quadrat d'un nombre no és parell, aleshores el nombre no és parell". ■

► 6. *Demostració de l'equivalència lògica que expressa el bicondicional en termes de* $\wedge$ *i* $\rightarrow$ *(condicional), que anomenarem* equivalència del bicondicional:

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p) \tag{4.7}$$

Comprovem que les taules de veritat coincideixen, amb la qual cosa resulten equivalents.

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$
0	0	1	1	1	1
0	1	1	0	0	0
1	0	0	0	0	0
1	1	1	1	1	1

► 7. *Demostració de l'equivalència*:

$$(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r) \tag{4.8}$$

Mètode 1. Comprovant que les taules de veritat coincideixen.

p	q	r	$p \vee q$	$p \rightarrow r$	$q \rightarrow r$	$(p \vee q) \rightarrow r$	$(p \rightarrow r) \wedge (q \rightarrow r)$
0	0	0	0	1	1	1	1
0	0	1	0	1	1	1	1
0	1	0	1	1	0	0	0
1	0	0	1	0	1	0	0
0	1	1	1	1	1	1	1
1	0	1	1	1	1	1	1
1	1	0	1	0	0	0	0
1	1	1	1	1	1	1	1

De la igualtat de les taules deriva l'equivalència lògica anterior.

Mètode 2. Fent servir equivalències lògiques ja demostrades, per exemple qualsevol de les anteriors que ens convingui.

$$\begin{aligned}
&(p \vee q) \rightarrow r \equiv \\
&\overset{(4.4)}{\equiv} \neg(p \vee q) \vee r \\
&\overset{(4.2)}{\equiv} (\neg p \wedge \neg q) \vee r \text{ (per De Morgan)}, \\
&\equiv (\neg p \vee r) \wedge (\neg q \vee r) \text{, per la distributivitat de } \vee \text{ respecte de } \wedge, \\
&\overset{(4.5)}{\equiv} (p \rightarrow r) \wedge (q \rightarrow r).
\end{aligned}$$

És important per a demostracions de condicionals amb una disjunció a l'antecedent.

► 8. *Demostració de les equivalències lògiques següents*:

$$p \to (r \vee s) \equiv (p \wedge \neg r) \to s \tag{4.9}$$
$$p \to (r \vee s) \equiv (p \wedge \neg s) \to r \tag{4.10}$$

És important per a demostracions de condicionals amb una disjunció al conseqüent.

Mètode 1. Comprovant que les taules de veritat coincideixen. És rutinari.

Mètode 2. Fent servir equivalències lògiques ja demostrades, per exemple qualsevol de les anteriors que ens convingui.

Vegem la primera.

$$\begin{aligned}
& p \to (r \vee s) \\
& \overset{(4.4)}{\equiv} \neg p \vee (r \vee s) \\
& (\neg p \vee r) \vee s, \text{ per associativitat de } \vee, \\
& \overset{(4.1)}{\equiv} (\neg p \vee \neg\neg r) \vee s, \text{ per doble negació,} \\
& \overset{(4.3)}{\equiv} \neg(p \wedge \neg r) \vee s \text{ (per De Morgan),} \\
& \overset{(4.4)}{\equiv} (p \wedge \neg r) \to s \\
& (p \wedge \neg r) \to s
\end{aligned}$$

Vegem-ne uns primers exemples il·lustratius:

Exemple 4.32 L'afirmació:

"Si en Joan ha comprat un cotxe, aleshores és vermell o gris" ($C \to (V \vee G)$)

equival a

"Si en Joan ha comprat un cotxe i no és vermell, aleshores és gris ($(C \wedge \neg V) \to G$)"

que equival a

"Si en Joan ha comprat un cotxe i no és gris, aleshores és vermell ($(C \wedge \neg G) \to V$)",

amb

$C =$ "en Joan ha comprat un cotxe"
$V =$ "en Joan ha comprat un cotxe vermell"
$G =$ "en Joan ha comprat un cotxe gris". ■

Exemple 4.33 Un altre exemple (llenguatge de predicats): per a x, y nombres reals, són equivalents:

$$\begin{aligned}
& xy = 0 \to (x = 0 \vee y = 0) \\
& (xy = 0 \wedge x \neq 0) \to y = 0 \\
& (xy = 0 \wedge y \neq 0) \to z = 0. \ \blacksquare
\end{aligned}$$

Vegem uns exemples d'ús d'aquesta equivalència, que ens permet substituir un esquema demostratiu per un altre.

Exemple 4.34 (utilitza variables, llenguatge de predicats) Considereu l'enunciat:

"Sigui n múltiple de 5. Demostreu que o bé n no és múltiple de 3 o bé n és múltiple de 15".

Formalment, l'enunciat és, per a n nombre enter:

$$5|n \to (3 \nmid n \vee 15|n).$$

És més clar demostrar:

$$(5|n \wedge \neg(3 \nmid n)) \to 15|n), \text{ que és}$$

$$(5|n \wedge 3|n) \to 15|n), \text{ que ja és obvi. } \blacksquare$$

Exemple 4.35 Vegem la utilitat per a demostracions. Vegem al mateix temps diverses formulacions d'un mateix enunciat.

"Si el producte de dos nombres enters és parell, aleshores almenys un dels dos és parell".

Introduint variables (llenguatge de predicats), "si ab és parell, aleshores a és parell o b és parell". Això equival a "si el producte de dos nombres enters és parell i un d'ells no és parell, aleshores ho és l'altre".

Siguin a, b nombres reals (fixos). Vegem que "si $2|ab$, aleshores a o b són parells", és a dir,

$$2|ab \to (2|a \vee 2|b).$$

És equivalent a $(2|ab \wedge 2 \nmid a) \to 2|b$, és a dir,

"si ab és parell i a no és parell, aleshores b és parell".

Aquesta última formulació és útil per a la demostració del resultat:

Si ab és parell, és $ab = 2k$ per a un k enter convenient. Si a no és parell, és senar, i és $a = 2q+1$, per a un cert q enter. Aleshores: $2k = ab = (2q+1)b = 2qb+b$, d'on $b = 2k-2qb = 2(k-2qb) = 2k'$, amb $k' = k-2qb$, de manera que b és parell, com s'havia de veure. $\blacksquare$

La demostració de la segona equivalència és similar a la primera:

$$\begin{aligned} & p \to (r \vee s) \\ \overset{(4.4)}{\equiv} \; & \neg p \vee (r \vee s) \end{aligned}$$

$(\neg p \vee s) \vee r$, per commutativitats i associativitat de $\vee$,

$\overset{(4.1)}{\equiv} (\neg p \vee \neg\neg s) \vee r$, per doble negació,

$\overset{(4.3)}{\equiv} \neg(p \wedge \neg s) \vee r$ (per De Morgan),

$\overset{(4.4)}{\equiv} (p \wedge \neg s) \rightarrow r$

$(p \wedge \neg s) \rightarrow r$

► 9. *Demostració de l'equivalència lògica*:

$$p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r \tag{4.11}$$

Mètode 1. Comprovant rutinàriament que les taules de veritat coincideixen.

Mètode 2. Fent servir equivalències lògiques ja demostrades, per exemple qualsevol de les anteriors que ens convingui.

Vegem el segon mètode.

$p \rightarrow (q \rightarrow r) \equiv$

$\equiv \neg p \vee (q \rightarrow r)$, per 4.4,

$\equiv \neg p \vee (\neg q \vee r)$, per 4.4,

$\equiv (\neg p \vee \neg q) \vee r$, per associativitat de $\vee$,

$\equiv \neg(p \wedge q) \vee r$, per 4.2,

$\equiv (p \wedge q) \rightarrow r$, per 4.4.

Vegem un exemple d'ús d'aquesta estructura lògica:

Exemple 4.36 Són equivalents:

"Si estem en forma, aleshores si el llac és prop d'aquí, aleshores anirem al llac".

"Si estem en forma, (aleshores) si el llac és prop d'aquí, (aleshores) anirem al llac".

"Si el llac és prop d'aquí, si estem en forma, anirem al llac".

"Si estem en forma i el llac és prop d'aquí, anirem al llac".

Corresponen a les fórmules (amb les lletres, de significat obvi):

$F \rightarrow (P \rightarrow L)$

$P \rightarrow (F \rightarrow L)$

$(F \wedge P) \rightarrow L$ ■

Vegem un exemple de la primera equivalència, on podem substituir un esquema demostratiu per un altre que ens resulti més abordable.

Exemple 4.37 (fem servir variables, llenguatge de predicats)

Suposem que s'ha de demostrar: "Sigui n un múltiple de 3. Proveu que, si n és un múltiple de 5, aleshores n és múltiple de 15". Veiem que s'ha de demostrar que és cert:

$$3|n \to (5|n \to 15|n)$$

També es pot enunciar: "Si un nombre és múltiple de 3, (aleshores) si és múltiple de 5, (aleshores) és múltiple de 15".

És equivalent demostrar:

$$(3|n \wedge 5|n) \to 15|n$$

Seria equivalent a provar:

$$5|n \to (3|n \to 15|n) \blacksquare$$

Exemple 4.38 (fem servir variables, llenguatge de predicats)
Són equivalents:

"La suma de dos nombres enters parells és parell"

"Si a és parell, aleshores, si b és parell, $a+b$ és parell".

"Si b és parell, aleshores, si a és parell, $a+b$ és parell".

"Si a és parell i b són parells, aleshores $a+b$ és parell".

"$2|a \to (2|b \to 2|a+b)$"

"$2|b \to (2|a \to 2|a+b)$"

"$(2|a \wedge 2|b) \to 2|a+b)$" $\blacksquare$

▹ ***Variant metodològica per a demostracions***. Una variant d'interès pràctic per a la demostració d'una equivalència lògica fent servir altres equivalències. La idea és encadenar equivalències per a les dues fórmules fins a arribar a sengles fórmules que siguin iguals o equivalents (si són iguals, són equivalents).

$$F \equiv F_1 \equiv \cdots \equiv F_{n-1} \equiv F_n$$
$$G \equiv G_1 \equiv \cdots \equiv G_{m-1} \equiv G_m$$

Si $F_n \equiv G_m$, aleshores $F \equiv G$. En efecte:

$$F \equiv F_1 \equiv \cdots \equiv F_{n-1} \equiv F_n \equiv G_m \equiv G_{m-1} \equiv \cdots \equiv G_2 \equiv G_1 \equiv G$$

Exemple 4.39 (un exemple d'ús de l'anterior a la demostració d'una equivalència, la que segueix):

$$p \to (q \to r) \equiv (p \wedge q) \to r$$

$p \to (q \to r) \equiv$
$\equiv \neg p \vee (q \to r)$ per l'equivalència del condicional $(a \to b \equiv \neg a \vee b)$,
$\equiv \neg p \vee (\neg q \vee r)$ per l'equivalència del condicional $(a \to b \equiv \neg a \vee b)$.

Per altra banda:

$(p \wedge q) \to r \equiv$
$\equiv \neg(p \wedge q) \vee r$ per l'equivalència del condicional $(a \to b \equiv \neg a \vee b)$,
$\equiv (\neg p \vee \neg q) \vee r$ per una de les equivalències de De Morgan,
$\equiv \neg p \vee (\neg q \vee r)$ per associativitat de $\vee$.

Les dues últimes són iguals, d'on l'equivalència $p \to (q \to r) \equiv (p \wedge q) \to r$, pel que s'ha dit abans. ■

4.7.3. Generalitzacions d'algunes equivalències lògiques a més operands

▷ Equivalències de De Morgan per a més de dos operands:

Equivalències de De Morgan per a tres operands (els enunciats ja incorporen les associativitats):

$$\neg(p \wedge q \wedge r) \equiv \neg p \vee \neg q \vee \neg r$$
$$\neg(p \vee q \vee r) \equiv \neg p \wedge \neg q \wedge \neg r$$

Per a quatre operands, anàlogament es compleix:

$$\neg(p \wedge q \wedge r \wedge s) \equiv \neg p \vee \neg q \vee \neg r \vee \neg s$$
$$\neg(p \vee q \vee r \vee s) \equiv \neg p \wedge \neg q \wedge \neg r \wedge \neg s$$

Exemple 4.40 Demostrem les equivalències de De Morgan per a tres operands.

Per exemple, per a la primera (anàlogament per a la segona), es tracta d'utilitzar la llei de De Morgan per a dos operands:

$\neg(p \wedge q \wedge r) \equiv$
$\equiv \neg(p \wedge (q \wedge r))$ per associativitat de $\wedge$, l'expressem com a conjunció de dues fórmules
$\equiv \neg p \vee \neg(q \wedge r)$ per De Morgan per a dos operands
$\equiv \neg p \vee (\neg q \vee \neg r)$ per De Morgan per a dos operands
$\equiv \neg p \vee \neg q \vee \neg r$ per associativitat de $\vee$ ■

Per a n operands, la conjunció i la disjunció es poden definir:

– recursivament a partir de la definició per a dos operands i per l'associativitat: per exemple, per a "i", $n \geq 3$, $p_1 \wedge \cdots \wedge p_n = p_1 \wedge (p_2 \wedge \cdots \wedge p_n)$.
– conceptualment: per exemple, per a "i", $p_1 \wedge \cdots \wedge p_n$ és cert si, i només si, tots els p_i són certs.

La generalització a n operands és certa; la demostració rigorosa es pot fer per inducció.

$$\neg(p_1 \wedge \cdots \wedge p_n) \equiv \neg p_1 \vee \cdots \vee \neg p_n$$
$$\neg(p_1 \vee \cdots \vee p_n) \equiv \neg p_1 \wedge \cdots \wedge \neg p_n$$

▷ Quina equivalència seria l'anàleg de 4.9, és a dir, de $p \to (q \vee r \vee s) \equiv$ per a tres operands al conseqüent?

Vegem un exemple del llenguatge natural:

Exemple 4.41 Són equivalents, entre d'altres variants:

"Si plou, ens quedarem a casa, o anirem al cinema o anirem al teatre".

"Si plou i no anem al cinema ni al teatre, aleshores ens quedarem a casa".

"Si plou i no anem al cinema, aleshores anirem al teatre o ens quedarem a casa". ■

Responem la qüestió al problema següent.

PROBLEMA 4.36

Deduïu per equivalències lògiques l'equivalència següent: $p \to (q \vee r \vee s) \equiv (p \wedge \neg q \wedge \neg r) \to s$. *Proposeu variants.*

Solució. La idea principal és fer servir l'equivalència lògica del mateix tipus però per a tres operands al conseqüent.

$p \to (q \vee r \vee s) \equiv$
$\equiv p \to ((q \vee r) \vee s)$, per associativitat de la disjunció,
$\equiv (p \wedge \neg(q \vee r)) \to s$, per l'equivalència del mateix tipus,
$\equiv (p \wedge (\neg q \wedge \neg r)) \to s$, per una de les equivalències de De Morgan,
$\equiv (p \wedge \neg q \wedge \neg r)) \to s$, per associativitat de $\wedge$.

Variants: Per commutativitat i associativitat aplicades a la fórmula inicial, resulta:

$$p \to (q \vee r \vee s) \equiv (p \wedge \neg q \wedge \neg s)) \to r$$
$$p \to (q \vee r \vee s) \equiv (p \wedge \neg r \wedge \neg s)) \to q$$

Amb altres associacions:

$$\begin{aligned}
&p \to (q \vee r \vee s) \equiv \\
&\equiv p \to (q \vee (r \vee s)) \\
&\equiv (p \wedge \neg q) \to (r \vee s)), \text{ per l'equivalència del mateix tipus,} \\
&\equiv (p \wedge \neg r) \to (q \vee s)) \\
&\equiv (p \wedge \neg s) \to (r \vee q))
\end{aligned}$$

▷ Quina equivalència seria l'anàleg de $(p \vee q) \to t$ (base de les demostracions per casos) per a més operands a l'antecedent?

Per exemple, per a tres operands a l'antecedent,

$$(r \vee s \vee t) \to w \equiv (r \to w) \wedge (s \to w) \wedge (t \to w),$$

(anàlogament per a 4 o n, però aleshores s'hauria de demostrar per inducció o acceptar una justificació menys formal). Ho demostrem en un exercici posterior.

Exemple 4.42 (Del llenguatge natural). Són equivalents (a) i (b):

a) "Si plou, (aleshores) ens quedarem a casa; (i) si neva, ens quedarem a casa i si fa vent, ens quedarem a casa"

$$\text{“}(P \to C) \wedge (N \to C) \wedge (V \to C)\text{”.}$$

b) "Si plou o neva o fa vent, ens quedarem a casa"

$$\text{“}(P \vee N \vee V) \to C\text{”.}$$

■

Es pot demostrar l'equivalència anterior amb taules de veritat o per deducció amb equivalències lògiques, com veiem a l'exercici següent:

PROBLEMA 4.37

Deduïu l'equivalència lògica següent utilitzant equivalències lògiques:

$$(r \vee s \vee t) \to w \equiv (r \to w) \wedge (s \to w) \wedge (t \to w)$$

Solució

$$\begin{aligned}
&(r \vee s \vee t) \to w \equiv \\
&\equiv \neg(r \vee s \vee t) \vee w, \text{ per l'equivalència } \alpha \to \beta \equiv \neg\alpha \vee \beta, \\
&\equiv (\neg r \wedge \neg s \wedge \neg t) \vee w, \text{ per una de les equivalències de De Morgan per a tres operands,} \\
&\equiv (\neg r \vee w) \wedge (\neg s \vee w) \wedge (\neg t \vee w), \text{ per distributivitat de } \vee \text{ respecte de } \wedge, \\
&\equiv (r \to w) \wedge (s \to w) \wedge (t \to w), \text{ per l'equivalència } \alpha \to \beta \equiv \neg\alpha \vee \beta.
\end{aligned}$$

▷ Quina equivalència seria l'anàleg de $(p \wedge q) \to r \equiv p \to (q \to r)$ per a les fórmules amb conjunció de més de dos operands a l'antecedent?

Com seria, per exemple, per a:

$$(p \wedge q \wedge t) \to r \equiv ?\ (3 \text{ operands})$$
$$(p \wedge q \wedge t \wedge w) \to r \equiv ?\ (4 \text{ operands})$$

En el cas de tres operands a l'antecedent, és:

$$(p \wedge q \wedge t) \to r \equiv p \to (q \to (t \to r)).$$

En veurem la demostració a l'exercici següent.

Exemple 4.43

Exemple 1. Vegem un exemple del llenguatge natural:

"Si el llac és prop d'aquí, (aleshores) si en trobem el camí, (aleshores) si és de dia, (aleshores) anirem al llac".

"Si el llac és prop d'aquí, (i) en trobem el camí i és de dia, (aleshores) anirem al llac". ■

Exemple 2. Vegem també un exemple amb fórmules matemàtiques:

$$3|n \to (5|n \to (7|n \to 3 \cdot 5 \cdot 7|n)),$$
$$(3|n \wedge 5|n \wedge 7|n) \to 3 \cdot 5 \cdot 7|n \ ■$$

Es pot demostrar l'equivalència anterior per taules de veritat o per deducció amb altres equivalències lògiques disponibles.

PROBLEMA 4.38

Deduïu amb equivalències lògiques l'equivalència:

$$(p \wedge q \wedge t) \to r \equiv p \to (q \to (t \to r))$$

Formuleu-ne variants.

Solució

$(p \wedge q \wedge t) \to r \equiv$

$\equiv (p \wedge (q \wedge t)) \to r$, per associativitat de la conjunció,

$\equiv (p \to ((q \wedge t) \to r)$, per l'equivalència $(A \wedge B) \to C \equiv (A \to (B \to C))$, amb $A = p$, $B = (q \wedge t) =$, $C = r$,

$\equiv (p \to (q \to (t \to r))$, per una segona aplicació de l'equivalència $(A \wedge B) \to C \equiv (A \to (B \to C))$, amb $A = q$, $B = t$, $C = r$.

Per commutativitat i associativitat en diversos passos de la deducció anterior, agrupant a $p \wedge q \wedge t$, es pot agrupar diferentment i en resulten diverses variants:

$$(p \wedge q \wedge t) \to r \equiv p \to (t \to (q \to r))$$
$$(p \wedge q \wedge t) \to r \equiv p \to (q \to (t \to r))$$
$$(p \wedge q \wedge t) \to r \equiv q \to (p \to (t \to r))$$
$$(p \wedge q \wedge t) \to r \equiv q \to (t \to p \to r))$$
$$(p \wedge q \wedge t) \to r \equiv t \to (q \to p \to r))$$
$$(p \wedge q \wedge t) \to r \equiv t \to (p \to q \to r))$$

$(p \wedge q \wedge t) \to r \equiv p \to ((t \wedge q) \to r))$ (i altres de tipus similar).

4.7.4. Exercicis diversos i exemples d'aplicació d'equivalències lògiques

▷ El resultat següent és útil en algunes demostracions d'equivalències (bicondicional):

PROBLEMA 4.39

Demostreu l'equivalència lògica $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$.

Solució

Mètode 1. Un mètode rutinari consisteix a provar que les taules de veritat coincideixen. És el que hauríem de seguir si no disposéssim d'equivalències lògiques a punt per a utilitzar.

Mètode 2. Un segon mètode consisteix a demostrar el resultat utilitzant altres equivalències ja demostrades (vegeu llista):

$\neg p \leftrightarrow \neg q \equiv (\neg p \to \neg q) \wedge (\neg q \to \neg p)$, per l'equivalència que expressa el bicondicional en termes de la conjunció.

Podem seguir dues variants argumentals:

Variant 1: Observant que, per l'equivalència del contrarecíproc, ja tenim

$\neg p \to \neg q \equiv q \to p$ i $\neg q \to \neg p \equiv p \to q$.

Substituint a l'última fórmula, en resulta:

$(\neg p \to \neg q) \wedge (\neg q \to \neg p) \equiv (q \to p) \wedge (p \to q)$, que, per l'equivalència de la commutativitat de $\wedge$, és lògicament equivalent a $(p \to q) \wedge (q \to p)$, lògicament equivalent a $p \leftrightarrow q$.

Variant 2: $\neg p \leftrightarrow \neg q \equiv (\neg p \to \neg q) \wedge (\neg q \to \neg p) \equiv$, per l'equivalència que expressa el bicondicional en termes de la conjunció,

$\equiv (\neg(\neg q) \to \neg(\neg p)) \wedge (\neg(\neg p) \to \neg(\neg q))$, per l'equivalència del contrarecíproc,

$\equiv (q \to p) \wedge (p \to q)$, per l'equivalència de la doble negació,

$\equiv (p \to q) \wedge (q \to p)$, per commutativitat,

$\equiv p \leftrightarrow q$, per l'equivalència del bicondicional.

▷ *Quines equivalències es fan servir en els exercicis següents?*:

Exemple 4.44 Equivalència lògica de la negació del bicondicional:

Vegem-ne una obtenció detallada, indicant quina equivalència lògica es fa servir a cada pas per a demostrar:

$$\neg(A \leftrightarrow B) \equiv ((A \wedge \neg B) \vee (\neg A \wedge B))$$

Es pot obtenir per equivalències:

$\neg(A \leftrightarrow B) \equiv$
$\equiv \neg((A \to B) \wedge (B \to A))$, per l'equivalència del bicondicional,
$\equiv (\neg(A \to B) \vee \neg(B \to A))$, per una de les lleis de De Morgan (negació de la "i"),
$\equiv ((A \wedge \neg B) \vee (B \wedge \neg A))$, per l'equivalència de negació del condicional. ■

Els exercicis següents s'han de resoldre de manera similar.

PROBLEMA 4.40

Considereu la seqüència següent d'esquivalències lògiques. S'hi apliquen equivalències lògiques i substitució. Indiqueu quines.

$$\begin{aligned}
&((p \to q) \wedge (q \to r)) \to (p \to r) \equiv \\
&\equiv \neg[(p \to q) \wedge (q \to r)] \vee (p \to r) \ (\textit{per ...}) \\
&\equiv [\neg(p \to q) \vee \neg(q \to r)] \vee (p \to r) \ (\textit{per ...}) \\
&\equiv [(p \wedge \neg q) \vee (q \wedge \neg r)] \vee (p \to r) \ (\textit{per ...}) \\
&\equiv [(p \wedge \neg q) \vee (q \wedge \neg r)] \vee (\neg p \vee r) \ (\textit{per ...}) \\
&\equiv (p \wedge \neg q) \vee (q \wedge \neg r) \vee \neg p \vee r \ (\textit{per ...})
\end{aligned}$$

Solució. S'hi apliquen equivalències lògiques i substitució:

$((p \to q) \wedge (q \to r)) \to (p \to r) \equiv$

$\equiv \neg[(p \to q) \wedge (q \to r)] \vee (p \to r)$ (per l'equivalència $a \to b \equiv \neg a \vee b$),

$\equiv [\neg(p \to q) \vee \neg(q \to r)] \vee (p \to r)$ (per una de les equivalències de De Morgan: $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$),

$\equiv [(p \wedge \neg q) \vee (q \wedge \neg r)] \vee (p \to r)$ (per l'equivalència de negació del condicional: $\neg(a \to b) \equiv a \wedge \neg b$),

$\equiv [(p \wedge \neg q) \vee (q \wedge \neg r)] \vee (\neg p \vee r)$ (per l'equivalència del condicional com a disjunció: $p \to r \equiv \neg p \vee r$),

$\equiv (p \wedge \neg q) \vee (q \wedge \neg r) \vee \neg p \vee r$ (per l'equivalència d'associativitat de la disjunció $\vee$),

on $\alpha = (p \to q)$, $\beta = (q \to r)$.

PROBLEMA 4.41

A partir de la fórmula proposicional $(p \to q) \to ((q \to r) \to (p \to r))$, *s'escriu la seqüència d'equivalències lògiques:*

Justifiqueu cada pas indicant quina equivalència s'hi fa servir.

$$(p \to q) \to ((q \to r) \to (p \to r)) \equiv \tag{1}$$
$$\equiv (\neg p \vee q) \to ((q \to r) \to (p \to r)) \tag{2}$$
$$\equiv \neg(\neg p \vee q) \vee [(q \to r) \to (p \to r)] \tag{3}$$
$$\equiv (\neg\neg p \wedge \neg q) \vee [(q \to r) \to (p \to r)] \tag{4}$$
$$\equiv (p \wedge \neg q) \vee [(q \to r) \to (p \to r)] \tag{5}$$
$$\equiv (p \wedge \neg q) \vee [\neg(q \to r) \vee (p \to r)] \tag{6}$$
$$\equiv (p \wedge \neg q) \vee [\neg(q \to r) \vee (\neg p \vee r)] \tag{7}$$
$$\equiv (p \wedge \neg q) \vee [(q \wedge \neg r) \vee (\neg p \vee r)] \tag{8}$$
$$\equiv (p \wedge \neg q) \vee (q \wedge \neg r) \vee (\neg p \vee r)] \tag{9}$$

Solució

Pas de (1) a (2): per l'equivalència $\alpha \to \beta \equiv \neg\alpha \vee \beta$.
Pas de (2) a (3): per l'equivalència $\alpha \to \beta \equiv \neg\alpha \vee \beta$.
Pas de (3) a (4): per una de les equivalències de De Morgan.
Pas de (4) a (5): per l'equivalència de doble negació.
Pas de (5) a (6): per l'equivalència $\alpha \to \beta \equiv \neg\alpha \vee \beta$.
Pas de (6) a (7): per l'equivalència $\alpha \to \beta \equiv \neg\alpha \vee \beta$.
Pas de (7) a (8): per l'equivalència de negació del condicional.
Pas de (8) a (9): com a conseqüència de l'equivalència d'associativitat de la disjunció.

PROBLEMA 4.42

Demostrarem l'equivalència següent de tres maneres diferents. Indiqueu què s'aplica a cada pas.

$$p \leftrightarrow q \equiv \neg((p \to q) \to \neg(q \to p))$$

Demostració 1:

$$\neg((p \to q) \to \neg(q \to p)) \equiv$$
$$\equiv (p \to q) \wedge \neg\neg(q \to p),$$
$$\equiv (p \to q) \wedge (q \to p),$$
$$\equiv p \leftrightarrow q.$$

Demostració 2:

$$\begin{aligned}&\neg((p \to q) \to \neg(q \to p)) \equiv\\ &\equiv \neg(\neg(p \to q) \vee \neg(q \to p)),\\ &\equiv (\neg\neg(p \to q) \wedge \neg\neg(q \to p)),\\ &\equiv (p \to q) \wedge (q \to p)\\ &\equiv p \leftrightarrow q.\end{aligned}$$

Demostració 3:

$$\begin{aligned}&p \leftrightarrow q \equiv\\ &\equiv \neg\neg(p \leftrightarrow q),\\ &\equiv \neg\neg((p \to q) \wedge (q \to p)),\\ &\equiv \neg[\neg((p \to q) \wedge (q \to p))],\\ &\equiv \neg[\neg(p \to q) \vee \neg(q \to p)],\\ &\equiv \neg[(p \to q) \to \neg(q \to p)].\end{aligned}$$

Solució. Per a demostrar $p \leftrightarrow q \equiv \neg((p \to q) \to \neg(q \to p))$, s'utilitza substitució i diverses equivalències lògiques (disponibles de la llista).

Demostració 1:

$\neg((p \to q) \to \neg(q \to p)) \equiv$
$\equiv (p \to q) \wedge \neg\neg(q \to p)$, per negació del condicional
$\equiv (p \to q) \wedge (q \to p)$, per doble negació
$\equiv p \leftrightarrow q$, per l'equivalència del bicondicional.

Demostració 2:

$\neg((p \to q) \to \neg(q \to p)) \equiv$
$\equiv \neg(\neg(p \to q) \vee \neg(q \to p))$, per l'expressió del condicional amb negació i disjunció
$\equiv (\neg\neg(p \to q) \wedge neg\neg(q \to p))$, per una equivalència de De Morgan
$\equiv (p \to q) \wedge (q \to p)$, per doble negació
$\equiv p \leftrightarrow q$, per equivalència del bicondicional.

Demostració 3:

$p \leftrightarrow q \equiv$
$\equiv \neg\neg(p \leftrightarrow q)$, per l'equivalència de doble negació
$\equiv \neg\neg((p \to q) \wedge (q \to p))$, per l'equivalència del bicondicional
$\equiv \neg[\neg((p \to q) \wedge (q \to p))]$ (reescriptura)
$\equiv \neg[\neg(p \to q) \vee \neg(q \to p)]$, per una equivalència de De Morgan
$\equiv \neg[(p \to q) \to \neg(q \to p)]$,
per l'equivalència que expressa el condicional amb negació i disjunció.

PROBLEMA 4.43

Sigui $(p \wedge \neg q) \rightarrow \neg(q \vee p)$ una fórmula proposicional. Indiqueu quines de les fórmules proposicionals següents són lògicament equivalents a la donada. En cas afirmatiu, justifiqueu-ho sense taules de veritat.

a) $(p \wedge \neg q) \rightarrow \neg(p \vee q)$
c) $(\neg q \wedge p) \rightarrow \neg(p \vee q)$
e) $(p \wedge \neg q) \rightarrow (\neg q \wedge \neg p)$
b) $(\neg q \wedge p) \rightarrow \neg(q \vee p)$
d) $\neg(p \wedge \neg q) \vee \neg(q \vee p)$
f) $\neg(\neg p \vee q) \rightarrow \neg(q \vee p)$

Solució. Totes són lògicament equivalents a l'original. Per tant, són mútuament lògicament equivalents, per substitucions de subfórmules per d'altres de lògicament equivalents. Concretament:

a) Equivalència amb subfórmula, commutativitat de la disjunció: $p \vee q \equiv q \vee p$.
b) Equivalència amb subfórmula, commutativitat de la conjunció: $p \wedge \neg q \equiv \neg q \wedge p$.
c) Equivalència amb subfórmula, commutativitat de la conjunció i de la disjunció.
d) equivalència del condicional en termes de negació i disjunció.
e) De Morgan.
f) De Morgan i doble negació.

PROBLEMA 4.44

Considereu les fórmules següents. Agrupeu-les per equivalència lògica (per exemple: 1-5, 2-4-9).

1) $(A \rightarrow B) \wedge (A \rightarrow C)$
2) $A \rightarrow (B \rightarrow C)$
3) $A \rightarrow (B \vee C)$
4) $A \vee B$
5) $(A \wedge \neg C) \rightarrow B$
6) $\neg A \rightarrow B$
7) $(A \rightarrow C) \wedge (B \rightarrow C)$
8) $(A \vee B) \rightarrow C$
9) $A \rightarrow (B \wedge C)$
10) $(A \wedge \neg B) \rightarrow C$
11) $\neg(A \rightarrow B)$
12) $(A \wedge B) \rightarrow C$
13) $(A \rightarrow B)$
14) $\neg(A \vee B)$
15) $A \wedge \neg B$
16) $\neg A \vee \neg B$
17) A
18) $\neg A \wedge \neg B$
19) $\neg B \rightarrow A$
20) $\neg\neg A$
21) $B \vee A$
22) $\neg(A \wedge B)$
23) $\neg B \rightarrow \neg A$
24) $(A \vee B) \wedge (A \vee C)$
25) $A \wedge B$
26) $A \wedge (B \wedge C)$
27) $B \wedge A$
28) $(A \wedge B) \wedge C$
29) $A \vee (B \vee C)$
30) $(A \wedge B) \vee (A \wedge C)$
31) $A \vee (B \wedge C)$
32) $(A \vee B) \vee C$
33) $A \wedge (B \vee C)$

Solució

a) **2–12**
b) **3–10–5**
c) **4–6–19–21**
d) **7–8**
e) **9–1**
f) **11–15**
g) **13–23**
h) **14–18**
i) **22–16**
j) **17–20**
k) **25–27**
l) **26–28**
m) **29–32**
n) **33–30**
o) **31–24**

PROBLEMA 4.45

Completeu la deducció següent explicant en què es basa cada pas. Se suposa que p,q,r,t són lletres proposicionals.

$$\begin{aligned}
\neg(p \to (\neg(q\wedge r)\vee t)) &\equiv p\wedge\neg(\neg(q\wedge r)\vee t) && \textit{[per ...]}\\
&\equiv p\wedge(\neg\neg(q\wedge r)\wedge\neg t) && \textit{[per ...]}\\
&\equiv p\wedge((q\wedge r)\wedge\neg t) && \textit{[per ...]}\\
&\equiv p\wedge q\wedge r\wedge\neg t && \textit{[per ...]}
\end{aligned}$$

Solució. Repetim la seqüència anterior justificant cada pas:

$$\begin{aligned}
\neg(p \to (\neg(q\wedge r)\vee t)) &\equiv p\wedge\neg(\neg(q\wedge r)\vee t)\\
&\quad \text{[per } \neg(a\to b)\equiv a\wedge\neg b\text{]}\\
&\equiv p\wedge(\neg\neg(q\wedge r)\wedge\neg t)\\
&\quad \text{[per De Morgan, } \neg(a\vee b)\equiv\neg a\wedge\neg b\text{]}\\
&\equiv p\wedge((q\wedge r)\wedge\neg t)\\
&\quad \text{[per equivalència de doble negació } \neg\neg a\equiv a\text{]}\\
&\equiv p\wedge q\wedge r\wedge\neg t\\
&\quad \text{[per associativitat de la conjunció]}
\end{aligned}$$

▷ ***Negar fórmules complicades***

La negació d'una fórmula F és simplement $\neg F$ (però normalment això no resulta interessant o convenient). En diverses situacions, estem interessats en altres fórmules que siguin equivalents lògicament a $\neg F$ (potser, per exemple, en alguna demostració per reducció a l'absurd o per a demostrar pel contrarecíproc).

Es poden obtenir a partir de $\neg F$ aplicant successivament equivalències lògiques. Totes les fórmules que es van obtenint són lògicament equivalents a $\neg F$ i podem dir que són "negacions de F" (equivalents a la negació de F).

Exemple 4.45 Sigui $F = p \to (\neg(q\wedge r)\vee t)$.

Anem a obtenir una seqüència de fórmules lògicament equivalents a la negació de F. Escrivim diverses fórmules equivalents a la negació de $p\to(\neg(q\wedge r)\vee t)$.

Si hem de negar $p\to(\neg(q\wedge r)\vee t)$, escriurem una seqüència de fórmules lògicament equivalents, totes equivalents a la negació, i pararem quan ens interessi, és a dir, quan la fórmula obtinguda tingui la forma que ens convingui. Per exemple:

$$\begin{aligned}
&\neg(p\to(\neg(q\wedge r)\vee t))\\
&p\wedge\neg(\neg(q\wedge r)\vee t)\\
&p\wedge(\neg\neg(q\wedge r)\wedge\neg t)\\
&p\wedge((q\wedge r)\wedge\neg t)\\
&p\wedge q\wedge r\wedge\neg t
\end{aligned}$$

(després es justifica cada pas)

Qualsevol de les escrites "és" negació de l'original (és a dir, és lògicament equivalent a la negació).

Refem la seqüència anterior justificant cada pas (s'efectuen diverses substitucions):

$$\begin{aligned}
\neg(p \to (\neg(q \wedge r) \vee t)) &\equiv p \wedge \neg(\neg(q \wedge r) \vee t) && [\text{per l'equivalència } \neg(a \to b) \equiv a \wedge \neg b\,] \\
&\equiv p \wedge (\neg\neg(q \wedge r) \wedge \neg t) && [\text{per una equivalència de De Morgan}] \\
&\equiv p \wedge ((q \wedge r) \wedge \neg t) \\
& && [\text{per l'equivalència de doble negació } \neg\neg a \equiv a\,] \\
&\equiv p \wedge q \wedge r \wedge \neg t && [\text{per associativitat de la conjunció}] \;\blacksquare
\end{aligned}$$

PROBLEMA 4.46

Negueu:

a) Plou i fa sol.

b) No sóc un vell.

c) L'home no ha arribat a Mart.

d) Fa calor i hi ha molta humitat.

e) $5 > 3$

f) Sóc astronauta, però no sóc militar.

Solució

a) Sense formalització, en un primer nivell, la negació seria "no (plou i fa sol)", que equival, en un segon nivell, a "no plou o no fa sol", o a d'altres frases equivalents, com ara "o bé no plou o bé no fa sol" o "o no plou o no fa sol". Si p és "plou", q és "fa sol", formalment $\neg(p \wedge q)$, negació de $p \wedge q$. Desenvolupant i aplicant una de les equivalències de De Morgan, la negació equival a $\neg p \vee \neg q$, és a dir, "no plou o no fa sol".

b) "No (no sóc un vell)", és a dir, "Sóc un vell". Formalment, $\neg(\neg p)$, si p és "Sóc un vell".

c) L'home ha arribat a Mart.

d) La proposició és $c \wedge h$, amb $c :=$ "fa calor", $h :=$ "hi ha molta humitat". La negació és $\neg(c \wedge h) \equiv \neg c \vee \neg h$ (De Morgan), "no fa calor o no hi ha molta humitat".

e) $\neg(5 > 3)$, és a dir, $5 \not> 3$, és a dir, $5 \leq 3$.

f) Si $a :=$ "sóc astronauta", $m :=$ "sóc militar", la proposició que es vol negar és $a \wedge \neg m$. Formalment, aplicant una de les equivalències de De Morgan, és $\neg(a \wedge \neg m) \equiv (\neg a \vee (\neg\neg m)) \equiv (\neg a \vee m)$. Per tant, "no sóc astronauta o sóc militar".

PROBLEMA 4.47

Considereu la fórmula proposicional: $\neg p \to (r \to \neg s)$. *Escriviu diverses fórmules equivalents a la negació de l'anterior. Arribeu a una fórmula amb només conjuncions i negacions.*

Solució

$\neg(\neg p \rightarrow (r \rightarrow \neg s))$, [simple negació de la fórmula original] que equival a
$\neg p \wedge \neg(r \rightarrow \neg s))$, [per negació del condicional] que equival a
$\neg p \wedge (r \wedge \neg\neg s)$, [per negació del condicional] que equival a
$\neg p \wedge (r \wedge s)$, [per doble negació] que equival a
$\neg p \wedge r \wedge s$ [per associativitat].

PROBLEMA 4.48

Identifiqueu entre les fórmules següents la negació del condicional $p \rightarrow q$.

a) $\neg p \wedge \neg q$
b) $\neg p \vee \neg q$
c) $\neg(p \vee q)$
d) $p \wedge \neg q$
e) $\neg p \vee q$
f) $\neg p \wedge q$
g) $\neg q \rightarrow \neg p$
h) $p \rightarrow \neg q$
i) $\neg p \rightarrow \neg q$
j) $\neg p \rightarrow q$

Solució. $p \wedge \neg q$

▷ *No haver de fer servir la disjunció:*

1. **Disjunció en termes del condicional**. Si hem de demostrar una disjunció $A \vee B$, pot no resultar còmode. Pot resultar confús o incòmode perquè no tenim per on començar; en un condicional, això no passa. L'equivalència $A \rightarrow B \equiv \neg A \vee B$ és útil per a expressar la conjunció en termes del condicional, cosa que ens resulta més còmode, sobretot per a demostracions.

Podem escriure:

$$\begin{aligned}
&A \vee B \equiv \\
&(\neg\neg A) \vee B \text{ (doble negació)}, \\
&\equiv \neg(\neg A) \vee B \text{ (reescriptura)}, \\
&\equiv (\neg A \rightarrow B), \text{ (s'aplica } \neg\alpha \vee \beta \equiv \alpha \rightarrow \beta, \text{ amb } \alpha = \neg A),
\end{aligned}$$

i així expressem una disjunció com a condicional. I també $A \vee B \equiv \neg B \rightarrow A$ (s'obté anàlogament, o com a contrarecíproc de $\neg A \vee B$). Pot ser interessant com a tècnica demostrativa.

Exemples 4.46

Exemple 1. Si n és un nombre enter, suposem que hem de demostrar la disjunció "n és parell o n és senar". Tot i que es pot demostrar directament considerant el residu de la divisió entera per 2, podem demostrar equivalentment qualsevol dels enunciats:

"Si n no és parell, aleshores és senar"
"Si n no és senar, aleshores és parell". ■

Exemple 2. També s'observa aquest ús en el llenguatge ordinari, no només en enunciats per a demostrar: són equivalents:

"plou o fa sol"
"si no plou, fa sol"
"si no fa sol, plou". ■

També pot ser interessant per a obtenir el condicional a llenguatges de programació on no està disponible. O per a obtenir una porta lògica, o un circuit, que realitzi el condicional, utilitzant altres components o altres portes lògiques. Amb un circuit que implementi $\neg A \vee B$ (una porta OR i una NOT), està implementant el condicional $A \to B$.

2. S'aplica la mateixa idea quan tenim disjuncions, o bé a l'antecedent, o bé al conseqüent d'un condicional (abans se n'han vist alguns exemples):

$$p \to (r \vee s) \equiv (p \wedge \neg r) \to s \text{ (“o” al conseqüent)}$$
$$p \to (r \vee s) \equiv (p \wedge \neg s) \to r$$
$$(p \vee q) \to r \equiv (p \to r) \wedge (q \to r) \text{ (“o” a l'antecedent)}$$

PROBLEMA 4.49

Demostreu que no són lògicament equivalents:

$$a \to (b \to c)$$
$$(a \to b) \to c$$

Solució. Dues fórmules proposicionals són lògicament equivalents si, i només si, tenen la mateixa taula de veritat. Comprovem que les taules de veritat no coincideixen:

a	b	c	$b \to c$	$a \to (b \to c)$	$a \to b$	$(a \to b) \to c$
0	0	0	1	1	1	0
0	0	1	1	1	1	1
0	1	0	0	1	1	0
1	0	0	1	1	0	1
0	1	1	1	1	1	1
1	0	1	1	1	0	1
1	1	0	0	0	1	0
1	1	1	1	1	1	1

Per tant, no són lògicament equivalents.

PROBLEMA 4.50

A partir d'una fórmula proposicional, escriviu les fórmules que es produeixen com a conseqüència d'aplicar les equivalències lògiques que s'indiquen.

$a \to (b \to c) \equiv$
$\equiv \cdots$ *[per $\alpha \to \beta \equiv \neg\alpha \vee \beta$ aplicat al condicional de l'esquerra]*
$\equiv \cdots$ *[per $\alpha \to \beta \equiv \neg\alpha \vee \beta$]*
$\equiv \cdots$ *[per associativitat de $\vee$]*
$\equiv \cdots$ *[per De Morgan]*
$\equiv \cdots$ *[per $\alpha \to \beta \equiv \neg\alpha \vee \beta$]*

Solució

$a \to (b \to c) \equiv$
$\equiv \neg a \vee (b \to c)$ [per $\alpha \to \beta \equiv \neg\alpha \vee \beta$ aplicat al condicional de l'esquerra],
$\equiv \neg a \vee (\neg b \vee c)$ [per $\alpha \to \beta \equiv \neg\alpha \vee \beta$],
$\equiv (\neg a \vee \neg b) \vee c$ [per associativitat de $\vee$],
$\equiv \neg(a \wedge b) \vee c$ [per De Morgan],
$\equiv (a \wedge b) \to c$ [per $\alpha \to \beta \equiv \neg\alpha \vee \beta$].

PROBLEMA 4.51

A partir d'una fórmula proposicional, escriviu les fórmules que es produeixen com a conseqüència d'aplicar les equivalències lògiques que s'indiquen.

$(a \to b) \to c \equiv$
$\equiv$? *[per $\alpha \to \beta \equiv \neg\alpha \vee \beta$ aplicat al condicional de la dreta]*
$\equiv$? *[per negació del condicional]*
$\equiv$? *[per De Morgan a l'operand de l'esquerra de la disjunció]*
$\equiv$? *[per $\alpha \to \beta \equiv \neg\alpha \vee \beta, \beta = c$]*

Solució

$(a \to b) \to c \equiv$
$\equiv \neg(a \to b) \vee c$ [per $\alpha \to \beta \equiv \neg\alpha \vee \beta$ aplicat al condicional de la dreta],
$\equiv (a \wedge \neg b) \vee c$ [per negació del condicional],
$\equiv \neg(\neg a \vee b) \vee c$ [per De Morgan a l'operand de l'esquerra de la disjunció],
$\equiv (\neg a \vee b) \to c$ [per $\alpha \to \beta \equiv \neg\alpha \vee \beta, \beta = c$].

PROBLEMA 4.52

Escriviu les fórmules proposicionals següents utilitzant només les connectives $\neg, \vee$:

a) $p \wedge (r \vee \neg s)$

b) $(p \wedge \neg q) \wedge \neg r$

Es tracta de reescriure les fórmules i obtenir-ne d'equivalents utilitzant equivalències lògiques.

Solució. Podem utilitzar l'equivalència $A \wedge B \equiv \neg(\neg A \vee \neg B)$, que es pot obtenir a partir de l'equivalència lògica de De Morgan: $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$. En efecte, amb una primera negació i després per l'equivalència de doble negació,

$$\begin{gathered}\neg(A \wedge B) \equiv (\neg A \vee \neg B)\\ \Downarrow \\ \neg\neg(A \wedge B) \equiv \neg(\neg A \vee \neg B)\\ \Downarrow \\ (A \wedge B) \equiv \neg(\neg A \vee \neg B)\end{gathered}$$

a) $p \wedge (r \vee \neg s)$. Apliquem l'equivalència anterior per a $A = p$, $B = (r \vee \neg s)$ (ja expressat en els termes que es demanen). Aleshores, resulta la fórmula equivalent:

$$\begin{array}{l} p \wedge (r \vee \neg s)\\ \neg(\neg p \vee \neg(r \vee \neg s)) \end{array}$$

b) $(p \wedge \neg q) \wedge \neg r$. Haurem d'aplicar dues vegades l'equivalència. Primerament, amb $A = (p \wedge \neg q)$, $B = \neg r$:

$$\begin{array}{l} (p \wedge \neg q) \wedge \neg r\\ \neg(\neg(p \wedge \neg q) \vee \neg(\neg r))\\ \neg(\neg(p \wedge \neg q) \vee r) \text{ (ara podríem aplicar simplement De Morgan a } \neg(p \wedge \neg q)) \end{array}$$

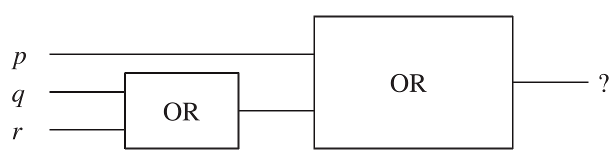
Ara, amb $A = p$, $B = \neg q$:

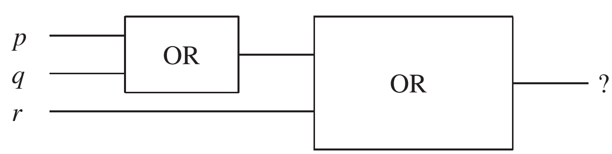
$$\begin{array}{l} \neg(\neg\neg(\neg p \vee \neg\neg q) \vee r)\\ \neg((\neg p \vee q) \vee r)\\ \neg(\neg p \vee q \vee r) \end{array}$$

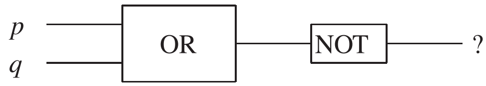
▷ *Circuits*

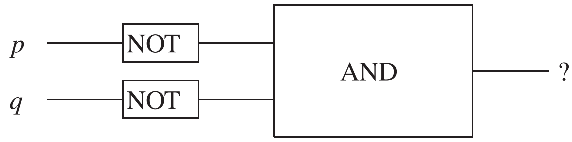
PROBLEMA 4.53

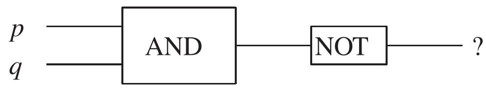
Indiqueu una fórmula lògica que correspongui a aquests "circuits" lògics, on NOT correspon a "no", ¬; AND correspon a "i", ∧; OR correspon a "o", ∨. Quina n'és la sortida?

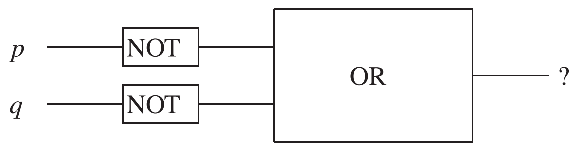




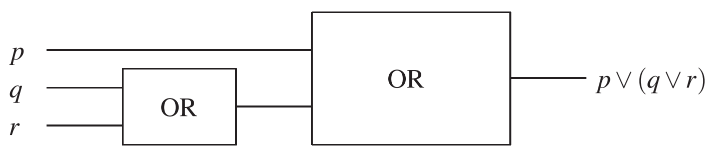

p
q
OR
NOT
?

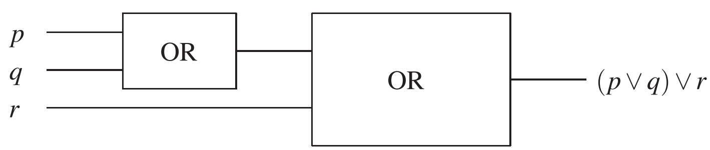

p
q
NOT
NOT
AND
?

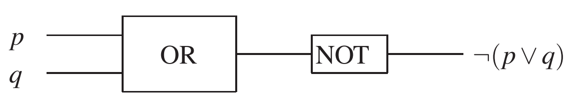

p
q
AND
NOT
?

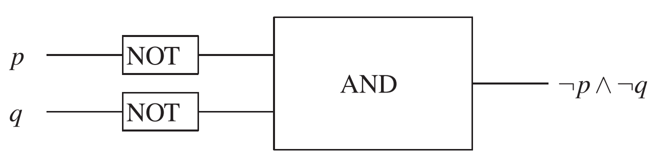

p
q
NOT
NOT
OR
?

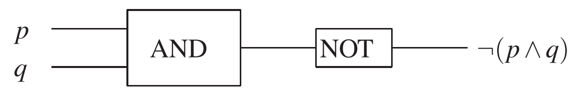
Solució

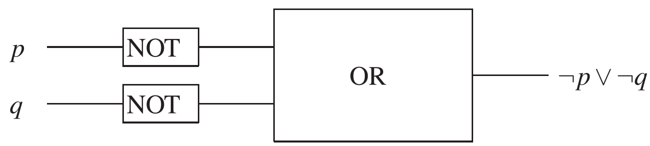

p
q
r
OR
OR
$p \vee (q \vee r)$


p
q
r
OR
OR
$(p \vee q) \vee r$


p
q
OR
NOT
$\neg(p \vee q)$


p
q
NOT
NOT
AND
$\neg p \wedge \neg q$





▷ *Fórmules amb menys connectives*

PROBLEMA 4.54

Estudieu:

a) Tota fórmula proposicional amb $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ *es pot reescriure amb només* $\neg, \wedge$*? Com?*

b) Tota fórmula proposicional amb $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ *es pot reescriure amb* $\neg, \vee$*? Com?*

Solució

a) Sí. Utilitzem les equivalències lògiques:

$p \vee q \equiv (\neg\neg p \vee \neg\neg q) \equiv \neg(\neg p \wedge \neg q)$, per De Morgan i doble negació.

$p \rightarrow q \equiv (\neg p \vee q) \equiv (\neg p \vee \neg\neg q) \equiv \neg(p \wedge \neg q)$

$(p \leftrightarrow q) \equiv (p \rightarrow q) \wedge (q \rightarrow p) \equiv \neg(p \wedge \neg q) \wedge \neg(q \wedge \neg p)$, utilitzant l'equivalència anterior.

b) Sí, fent servir diverses equivalències lògiques:

$p \wedge q \equiv (\neg\neg p \wedge \neg\neg q) \equiv \neg(\neg p \vee \neg q)$, per De Morgan i doble negació.

$p \rightarrow q \equiv (\neg p \vee q)$ (equivalència del condicional, v. llista d'equivalències, 4.6.4).

$(p \leftrightarrow q) \equiv (p \rightarrow q) \wedge (q \rightarrow p) \equiv ((\neg p \vee q) \wedge (\neg q \vee p)) \equiv \neg(\neg(\neg p \vee q) \vee \neg(\neg q \vee p))$, per les anteriors.

4.8. Tautologies i contradiccions

4.8.1. Ni "sempre veritat" ni "sempre falsa"

S'observa que hi ha fórmules proposicionals que prenen diferents valors veritatius, cert o fals, depenent dels valors veritatius de les lletres proposicionals. Això es pot veure, per exemple, si considerem la fórmula $\neg(p \vee q)$:

p	q	$p \vee q$	$\neg(p \vee q)$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

Si considerem totes les possibilitats, als dos extrems possibles hi haurien les fórmules proposicionals "sempre certes" i les que són "sempre falses", és a dir, per a tots els valors de veritat possibles de les lletres proposicionals. Són les tautologies i les contradiccions, respectivament.

La fórmula anterior s'expressa mitjançant les lletres proposicionals p,q. És $F = \neg(p \vee q)$; de forma genèrica, $F = F(p,q)$.

4.8.2. Tautologies

Definició 4.5 *SUna fórmula proposicional F que s'expressa en termes de lletres proposicionals ($F = F(p_1,\cdots,p_n)$) és una **tautologia** si, per a tots els valors de veritat possibles de les lletres proposicionals, és a dir, (0-1), la fórmula té valor de veritat* 1 *(cert). Dit d'una altra manera, a la taula de veritat de F, la columna de F està formada per uns (veritat).*

▷ ***Com se sap si una fórmula proposicional és una tautologia?***

La manera més simple és comprovant si la seva taula de veritat és tota de valors "1" (o "V" o "T"). En cas afirmatiu, és tautologia.

▷ ***Com es pot demostrar que una fórmula proposicional és una tautologia?***

Completant el que s'ha dit abans:

– **Mètode 1.** Per taules de veritat, comprovant que la columna de la fórmula és de uns, és a dir, que el seu valor veritatiu és 1 per a qualsevol valor veritatiu de les lletres.

– **Mètode 2.** Veient que no existeix cap valor de veritat de les lletres que faci falsa la fórmula. Se suposa la fórmula falsa per alguns valors de veritat de les lletres i es dedueix que no és possible (o perquè no poden existir o per contradicció). D'alguna manera, és una variant de l'anterior (deductiva, sense el càlcul complet de tota la taula).

– **Mètode 3.** Per equivalències lògiques; necessitarem les equivalències especials del final de la secció.

  L'afirmació "F és una tautologia" és una afirmació sobre una fórmula del llenguatge de proposicions. N'està fora. No forma part del llenguatge de proposicions.

Exemples bàsics de tautologies

Exemple 4.47 El més bàsic dels exemples és: $p \vee \neg p$.

Vegem que la fórmula anterior és una tautologia, comprovant que la taula de veritat de la fórmula és 1 per a tots els valors de veritat de p:

p	$\neg p$	$p \vee \neg p$
0	1	1
1	0	1

Comentari. Aquesta tautologia s'anomena "principi del terç exclòs" ("*law of the excluded middle*"), d'interès a la lògica clàssica. Tradueix la idea que, per a un enunciat, no hi ha cap posició o possibilitat intermèdia entre ser cert o ser fals (lògica binària).■

També $\alpha \vee \neg \alpha$ és una tautologia, on α és una fórmula proposicional. Es pot raonar directament analitzant els valors de veritat que se n'obtenen o considerar que és una substitució (final secció).

Exemple 4.48 Són també tautologies bàsiques:

$$p \to p$$

$$(p \wedge q) \to p$$
$$(p \wedge q) \to q$$

$$p \to (p \vee q)$$
$$q \to (p \vee q)$$

$$(p \wedge q) \to (p \vee q)$$

En demostrem algunes comprovant rutinàriament que les taules de veritat respectives coincideixen:

p	q	$p \wedge q$	$(p \wedge q) \to p$	$p \vee q$	$p \to (p \vee q)$	$(p \wedge q) \to (p \vee q)$
0	0	0	1	0	1	1
0	1	0	1	1	1	1
1	0	0	1	1	1	1
1	1	1	1	1	1	1

Observeu que són "tres taules de veritat en una".

Quins casos particulars obtenim quan $q = p$?■

▷ ***Quan la fórmula proposicional*** $F = F(p_1, \cdots, p_n)$ ***no és una tautologia?***

Quan, per a **algun** valor de veritat de les lletres, la fórmula és falsa. És a dir, existeix alguna combinació de valors de veritat de les lletres que fa la fórmula falsa. No cal que sigui per a tot valor veritatiu de les lletres.

Per exemple, $\neg p \wedge \neg q$ no és una tautologia:

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	0

Ens podem preguntar si algunes fórmules similars a l'exemple anterior, com ara indicarem, són tautologies o no:

$$\begin{array}{lll} p \rightarrow (p \wedge q) & p \rightarrow (p \wedge q) & \\ (p \vee q) \rightarrow p & (p \vee q) \rightarrow p & (p \vee q) \rightarrow (p \wedge q) \end{array}$$

Concretem-ho en un exercici:

PROBLEMA 4.55

Estudieu si són tautologies les fórmules següents:

$$\begin{array}{l} p \rightarrow (p \wedge q) \\ q \rightarrow (p \wedge q) \\ (p \vee q) \rightarrow p \\ (p \vee q) \rightarrow q \\ (p \vee q) \rightarrow (p \wedge q) \end{array}$$

Solució. Per similitud, només hem de veure si ho són

$$p \rightarrow (p \wedge q),\ (p \vee q) \rightarrow p \text{ i } (p \vee q) \rightarrow (p \wedge q).$$

Obtenim una taula de veritat conjunta per a estudiar la qüestió:

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow (p \wedge q)$	$(p \vee q) \rightarrow p$	$(p \vee q) \rightarrow (p \wedge q)$
0	0	0	0	0	1	1
0	1	0	1	1	0	0
1	0	0	1	0	1	0
1	1	1	1	1	1	1

Les columnes de les fórmules contenen zeros, raó per la qual no són tautologies.

4.8.3. El símbol $\mathbb{T}$

Amb aquest símbol, indiquem qualsevol tautologia, és a dir, qualsevol fórmula amb tots els valors de veritat 1. La fórmula ja no s'especifica: pot representar, per exemple, $p \vee \neg p$ o qualsevol altra tautologia. Per a operar juntament amb altres fórmules, la podem suposar del mateix nombre d'operands que la fórmula corresponent. Vegem que $p \vee \mathbb{T}$ és una tautologia:

p	$\mathbb{T}$	$p \vee \mathbb{T}$
0	1	1
1	1	1

p	1	$p \vee 1$
0	1	1
1	1	1

Podria ser també amb qualsevol altra fórmula F de n operands (lletres proposicionals): $F(p_1, \cdots, p_n)$. Tenim que $F \vee \mathbb{T}$ és una tautologia: la disjunció amb qualsevol tautologia és tautologia.

p_1	p_2	$\cdots$	p_n	$F(p_1, \cdots, p_n)$	$\mathbb{T}$	$F(p_1, \cdots, p_n) \vee \mathbb{T}$
0	0	$\cdots$	0	X	1	1
0	0	$\cdots$	1	X	1	1
$\cdots$	$\cdots$	$\cdots$	$\cdots$	X	1	1
1	1	$\cdots$	1	X	1	1

És $X = 0$ o $X = 1$.

Quina és la taula de veritat de $p \wedge \mathbb{T}$? De $F \wedge \mathbb{T}$? La de p i F, respectivament. Es veu escrivint la taula. Notació alternativa amb 1 o 0: $p \vee 1 \equiv 1$ (i altres similars).

4.8.4. Tautologies i equivalències lògiques

Les equivalències lògiques són una bona font de tautologies, ja que:

Teorema 4.2 *$\alpha \equiv \beta$ si, i només si, $\alpha \leftrightarrow \beta$ és una tautologia.*

Demostració. Hem de veure que α i β tenen la mateixa taula de veritat si, i només si, la taula de veritat de $\alpha \leftrightarrow \beta$ està formada tota per 1, que és obvi.

Exemple 4.49 Segueixen diverses tautologies. El lector comprovarà que ho són veient que la taula de veritat de la fórmula és de uns o identificant de quina equivalència deriva:

$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$ (derivat d'una de les equivalències de De Morgan),

$p \wedge (q \wedge r) \leftrightarrow (p \wedge q) \wedge r$ (derivat de l'equivalència d'associativitat de $\wedge$),

$p \wedge (r \vee s) \leftrightarrow (p \wedge r) \vee (p \wedge s)$ (derivat de l'equivalència de distributivitat de $\wedge$ respecte de $\vee$). ■

La llista anterior és ampliable expressant com a tautologies les equivalències de la llista de la secció 4.6.4.

PROBLEMA 4.56

Escriviu les equivalències lògiques com a tautologies:

a) $\neg\neg p \equiv p$

b) $(p \wedge q) \equiv (q \wedge p)$

c) $(p \vee q) \equiv (q \vee p)$

d) $(p \wedge (q \wedge r)) \equiv (p \wedge (q \wedge r))$

e) $(p \vee (q \vee r)) \equiv (p \vee (q \vee r))$

f) $(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$

g) $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$

h) $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$

i) $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$

j) $(p \to q) \equiv (\neg q \to \neg p)$

Solució

a) $\neg\neg p \leftrightarrow p$ (és tautologia)

b) $(p \wedge q) \leftrightarrow (q \wedge p)$

c) $(p \vee q) \leftrightarrow (q \vee p)$

d) $(p \wedge (q \wedge r)) \leftrightarrow (p \wedge (q \wedge r))$

e) $(p \vee (q \vee r)) \leftrightarrow (p \vee (q \vee r))$

f) $(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$

g) $(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$

h) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$

i) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$

j) $(p \to q) \leftrightarrow (\neg q \to \neg p)$

4.8.5. Contradiccions

Definició 4.6 *Una fórmula proposicional F que s'expressa en termes de lletres proposicionals ($F = F(p_1, \cdots, p_n)$) és una* ***contradicció*** *si, per a tots els valors de veritat possibles de les lletres proposicionals (0-1), la fórmula té valor de veritat* 0 *(fals). Dit d'una altra manera, a la taula de veritat de F, la columna de F està formada per zeros (fals).*

Com se sap si una fórmula és una contradicció?

La manera més simple és comprovant si la seva taula de veritat és tota de valors "0" (o "F"), fals.

Exemples de contradicció

Exemple 4.50 El més bàsic: $p \wedge \neg p$.

En efecte, vegem que la taula de veritat de la fórmula és tota de zeros:

p	$\neg p$	$p \wedge \neg p$
0	1	0
1	0	0

■

També és una contradicció $\alpha \wedge \neg\alpha$, on α és una fórmula proposicional.

És fàcil obtenir contradiccions: F és una contradicció si, i només si, $\neg F$ és una tautologia. Per tant, és suficient estudiar les tautologies: les contradiccions s'obtenen per negació.

També es poden obtenir tautologies per negació de contradiccions. Per exemple,

$$\neg(p \wedge \neg p)$$

és una tautologia.

L'afirmació "F és una contradicció" no forma part del llenguatge de proposicions.

4.8.6. El símbol $\mathbb{F}$

Amb aquest símbol, indiquem qualsevol contradicció, és a dir, qualsevol fórmula amb tots els valors de veritat 0. La fórmula ja no s'especifica: pot representar, per exemple, $p \wedge \neg p$ o alguna altra contradicció. Per a operar juntament amb altres fórmules, la podem suposar del mateix nombre d'operands que la fórmula corresponent. Vegem que $p \wedge \mathbb{F}$ és una contradicció:

p	$\mathbb{F}$	$p \wedge \mathbb{F}$
0	0	0
1	0	0

p	0	$p \wedge 0$
0	0	0
1	0	0

Podria ser també amb qualsevol altra fórmula G de n operands (lletres proposicionals): $G(p_1, \cdots, p_n)$. Tenim que $G \wedge \mathbb{F}$ és una contradicció: conjunció amb qualsevol contradicció és contradicció.

p_1	p_2	$\cdots$	p_n	$G(p_1, \cdots, p_n)$	$\mathbb{F}$	$G(p_1, \cdots, p_n) \wedge \mathbb{F}$
0	0	$\cdots$	0	X	0	0
0	0	$\cdots$	1	X	0	0
$\cdots$	$\cdots$	$\cdots$	$\cdots$	X	0	0
1	1	$\cdots$	1	X	0	0

És $X = 0$ o $X = 1$.

Quina és la taula de veritat de $p \vee \mathbb{F}$? De $G \vee \mathbb{F}$? La de p i G, respectivament. Es veu escrivint la taula. Notació alternativa amb 1 o 0: $p \vee 1 \equiv 1$ (i altres similars).

4.8.7. Equivalències especials amb $\mathbb{T}$ i $\mathbb{F}$

Completem algunes equivalències (cal afegir les commutacions corresponents):

$(p \vee \mathbb{T}) \equiv \mathbb{T}$ (on $\mathbb{T}$ indica qualsevol fórmula proposicional que és tautologia)
$(p \wedge \mathbb{T}) \equiv p$ (on $\mathbb{T}$ indica qualsevol tautologia)
$(p \vee \mathbb{F}) \equiv p$ (on $\mathbb{F}$ indica qualsevol contradicció)
$(p \wedge \mathbb{F}) \equiv \mathbb{F}$ (on $\mathbb{F}$ indica qualsevol contradicció)

$$\mathbb{T} \wedge \mathbb{T} \equiv \mathbb{T}$$
$$\mathbb{F} \wedge \mathbb{F} \equiv \mathbb{F}$$
$$\mathbb{T} \wedge \mathbb{F} \equiv \mathbb{F}$$
$$\mathbb{T} \vee \mathbb{T} \equiv \mathbb{T}$$
$$\mathbb{F} \vee \mathbb{F} \equiv \mathbb{F}$$
$$\mathbb{T} \vee \mathbb{F} \equiv \mathbb{T}$$

També són possibles altres notacions, escrivint “1” en comptes de $\mathbb{T}$ i “0” en comptes de $\mathbb{F}$. Exemple: $p \vee 1 \equiv 1$ o $1 \wedge 0 \equiv 0$.

La llista es pot generalitzar amb afirmacions del tipus (només és un exemple possible): $\mathbb{F} \vee \alpha \equiv \alpha$, on hem substituït una lletra proposicional per una fórmula (i altres).

També es poden considerar altres connectives.

Malgrat l’aparent trivialitat, poden ser útils en demostracions de tautologies o d’equivalències fent servir equivalències, moltes vegades per a obtenir simplificacions en una fórmula.

També per fer aparèixer lletres que no eren a la fórmula, cosa que pot ser útil per a certes manipulacions:

$p \wedge \mathbb{T} \equiv$
$\equiv p \wedge (q \vee \neg q)$ (per substitució)
$\equiv (p \wedge q) \vee (p \wedge \neg q)$ (per distributivitat de $\wedge$ respecte de $\vee$).

Amb similitud amb l’argumentació per a conjunts (on A, B són conjunts, subconjunts de Ω):

$$A = A \cap \Omega = A \cap (B \cup B^c) = (A \cap B) \cup (A \cap B^c) = (A \cap B) \cup (A - B).$$

Correspondria, si bé amb fórmules de predicat:

$$x \in A \Leftrightarrow (x \in A \wedge (x \in B \vee x \notin B)) \Leftrightarrow \cdots$$

Vegem un exemple d’ús de les tautologies amb $\mathbb{T}$ i $\mathbb{F}$:

Exemple 4.51 Proveu que $(p \wedge (p \to q)) \to q$ és una tautologia.

Es pot demostrar per dos mètodes:

Mètode 1. Per taules de veritat. Vegem que, per a tot valor veritatiu dels operands p, q, el valor veritatiu de la fórmula és 1.

p	q	$p \to q$	$p \wedge (p \to q)$	$(p \wedge (p \to q)) \to q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

Mètode 2. Utilitzant equivalències lògiques (vegeu llista 4.6.4).

Les fórmules següents són lògicament equivalents; es realitzen substitucions per equivalències sense que calgui indicar-ho en tots els casos:

$$
\begin{aligned}
&(p \wedge (p \to q)) \to q \equiv \\
&\equiv (p \wedge (\neg p \vee q)) \to q \text{ (per } p \to q \equiv \neg p \vee q \text{ i substitució)} \\
&\equiv ((p \wedge \neg p) \vee (p \wedge q)) \to q \text{ (per distributivitat de } \wedge \text{ respecte de } \vee\text{)} \\
&\equiv (\mathbb{F} \vee (p \wedge q)) \to q \text{ (per } p \wedge \neg p \equiv \mathbb{F}\text{)} \\
&\equiv (p \wedge q)) \to q \text{ (per } \mathbb{F} \vee \alpha \equiv \alpha\text{)} \\
&\equiv \neg(p \wedge q)) \vee q \text{ (per } \alpha \to \beta \equiv \neg\alpha \vee \beta\text{)} \\
&\equiv (\neg p \vee \neg q) \vee q \text{ (per una de les equivalències de De Morgan)} \\
&\equiv \neg p \vee (\neg q \vee q) \text{ (per associativitat de } \vee\text{)} \\
&\equiv \neg p \vee \mathbb{T} \text{ (per commutativitat de } \vee \text{ i } \neg\alpha \vee \alpha \equiv \mathbb{T}\text{)} \\
&\equiv \mathbb{T} \text{ (tot uns) (per } \alpha \vee \mathbb{T} \equiv \mathbb{T}\text{)}
\end{aligned}
$$

Com a conseqüència, o repetint l'argumentació, o per substitució,

$$(A \wedge (A \to B)) \to B \text{ és una tautologia. } \blacksquare$$

4.8.8. La substitució de lletres per fórmules en una tautologia dóna una nova tautologia

Donem sense demostració un resultat interessant.

Afirma que "la substitució en una tautologia produeix una tautologia".

Teorema. *Sigui S una tautologia i suposem-la expressada en termes de les lletres proposicionals* $p_1, \cdots, p_n$. *Siguin* $F_1, \cdots, F_n$ *fórmules proposicionals. Sigui W la fórmula proposicional que s'obté substituint, respectivament,* p_1 *per* F_1, ..., p_n *per* F_n. *Aleshores, W és una tautologia.*

Per això, abans hem dit que, havent demostrat unes tautologies per a fórmules en termes de lletres de proposició, les podíem estendre a fórmules més generals:

Són tautologies:

$\alpha \vee \neg\alpha$, on α és una fórmula proposicional.

$(A \wedge (A \to B)) \to B$, on A, B són fórmules proposicionals.

PROBLEMA 4.57

Estudieu si la fórmula següent és tautologia: $((p \to q) \to p) \to p$

Solució. Es pot demostrar que són tautologies comprovant que la columna de la taula de veritat de la fórmula està formada tota per uns. Si alguna no és tautologia, aleshores en alguna fila hi ha un 0 a la columna de la fórmula:

$$((p \to q) \to p) \to p.$$

Mètode 1. Utilitzem el procediment de la taula de veritat:

p	q	$p \to q$	$(p \to q) \to p$	$((p \to q) \to p) \to p$
0	0	1	0	1
0	1	1	0	1
1	0	0	1	1
1	1	1	1	1

Per tant, és tautologia.

Mètode 2. Si ha de ser tautologia, vegem si podem demostrar que no existeixen valors de veritat $v(p)$, $v(q)$, (0,1), per als quals el valor de veritat de la fórmula és 0 ($v(((p \to q) \to p) \to p) = 0$).

Si ha de ser $v(((p \to q) \to p) \to p) = 0$, tenint en compte que és el condicional $((p \to q) \to p) \to p$, l'única possibilitat és que sigui $v(((p \to q) \to p)) = 1$ i $v(p) = 0$. Però, aleshores, tenim $v(((0 \to q) \to 0)) = 1$. I, aleshores, ha de ser $v((0 \to q)) = 0$. Però això és impossible, ja que per a cap valor de veritat de q no es compleix el requeriment anterior: $v((0 \to 0)) = 1$, $v((0 \to 1)) = 1$.

Per tant, és tautologia.

Mètode 3. També es pot veure per un segon mètode, per equivalències lògiques (de les llistes de disponibles); escrivim una seqüència d'equivalències lògiques $((p \to q) \to p) \to p \equiv \cdots \equiv \mathbb{T}$:

$$((p \to q) \to p) \to p \equiv$$
$$\equiv ((\neg p \vee q) \to p) \to p \text{ (per } r \to s \equiv \neg r \vee s \text{ i substitució).}$$
$$\equiv (\neg(\neg p \vee q) \vee p) \to p \text{ (per } r \to s \equiv \neg r \vee s \text{ i substitució).}$$
$$\equiv (\neg\neg(\neg p \vee q) \vee p) \vee p \text{ (per } r \to s \equiv \neg r \vee s \text{ i substitució).}$$
$$\equiv ((\neg p \vee q) \vee p) \vee p \text{ (per doble negació i substitució).}$$

Ara podem fer servir $p \vee p \equiv p$ i substituir, amb l'aplicació prèvia de l'associativitat de $\vee$, o bé utilitzant repetidament associativitat i commutativitat,

$$\equiv (\neg p \vee p) \vee q \vee p$$
$$\equiv \mathbb{T} \vee (q \vee p)$$
$$\equiv \mathbb{T}, \text{ per } \mathbb{T} \vee \alpha \equiv \mathbb{T}, \text{ amb } \alpha = (q \vee p).$$

En aquest últim pas s'hauria pogut aplicar la propietat associativa de $\vee$ i escriure:

$$\equiv (\mathbb{T} \vee q) \vee p \equiv \mathbb{T} \vee p \equiv \mathbb{T}.$$

Per tant, és tautologia.

Observeu que hauríem pogut començar d'altres maneres, cosa que donaria lloc a diverses variants argumentals. Utilitzem $r \to s \equiv \neg r \vee s$. El lector pot continuar l'argumentació.

Primera variant:

$$((p \to q) \to p) \to p \equiv (\neg(p \to q) \vee p) \to p$$

Segona variant:

$$((p \to q) \to p) \to p \equiv \neg((p \to q) \to p)) \vee p$$

PROBLEMA 4.58

Estudieu si la fórmula següent és tautologia:

$$(p \to q) \to ((q \to r) \to (p \to r))$$

Solució. Es pot demostrar que són tautologies comprovant que la columna de la taula de veritat de la fórmula està formada tota per uns. Si alguna no és tautologia, aleshores en alguna fila hi ha un 0 a la columna de la fórmula.

$$((p \to q) \wedge (q \to r)) \to (p \to r).$$

Es pot resoldre per taules de veritat.

Mètode 1. Per taules de veritat. Cal veure que la columna corresponent a la fórmula és de uns.

Per tal de fer la taula més practicable, denotem

$\alpha = p \to q$, $\beta = q \to r$, $\gamma = p \to r$, i aleshores la fórmula és: $W = (\alpha \wedge \beta) \to \gamma$.

p	q	r	$p \to q\ (\alpha)$	$q \to r\ (\beta)$	$p \to r\ (\gamma)$	$\alpha \wedge \beta$	$(\alpha \wedge \beta) \to \gamma (W)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	1	0	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
1	0	1	0	1	1	0	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

Efectivament, és una tautologia.

Mètode 2. Suposant que per a algun valor de veritat de les lletres el valor de veritat de la fórmula és 0 i veient que no és possible.

Hem d'analitzar l'estructura de subfórmules de la fórmula, hem d'assignar valors de veritat a les subfórmules i a les lletres deductivament, aplicant les taules de veritat bàsiques, és a dir, de les connectives, fins arribar a una contradicció:

$$((p \to q) \land (q \to r)) \to (p \to r) \text{ (és un condicional).}$$

$$((p \to q) \land (q \to r)) \overset{0}{\to} (p \to r).$$

$$((p \to q) \overset{1}{\land} (q \to r)) \overset{0}{\to} (p \overset{0}{\to} r).$$

$$((p \overset{1}{\to} q) \overset{1}{\land} (q \overset{1}{\to} r)) \overset{0}{\to} (\overset{1}{p} \overset{0}{\to} \overset{0}{r}).$$

$$((\overset{1}{p} \overset{1}{\to} q) \overset{1}{\land} (q \overset{1}{\to} \overset{0}{r})) \overset{0}{\to} (\overset{1}{p} \overset{0}{\to} \overset{0}{r}).$$

$$((\overset{1}{p} \overset{1}{\to} \overset{\boxed{1}}{q}) \overset{1}{\land} (\overset{\boxed{0}}{q} \overset{1}{\to} \overset{0}{r})) \overset{0}{\to} (\overset{1}{p} \overset{0}{\to} \overset{0}{r}).$$

Per a obtenir un valor 0 per a la fórmula, tindríem una assignació contradictòria de valors de veritat per a la lletra q (es dedueixen valors veritatius incompatibles). Aquest valor per a la fórmula no es pot presentar i, per tant, és tautologia.

PROBLEMA 4.59

Estudieu si la fórmula següent és tautologia:

$$(p \to q) \to ((q \to r) \to (p \to r)).$$

Solució. Es pot demostrar que és tautologia comprovant que la columna de la taula de veritat de la fórmula està formada tota per uns. Si no és tautologia, aleshores en alguna fila hi ha un 0 a la columna de la fórmula.

Mètode 1. Podem procedir per taules de veritat.

$$(p \to q) \to ((q \to r) \to (p \to r)).$$

$\alpha = p \to q$, $\beta = q \to r$, $\gamma = p \to r$, i aleshores la fórmula és: $W = (\alpha \land \beta) \to \gamma$.

p	q	r	$p \to q$ (α)	$q \to r$ (β)	$p \to r$ (γ)	$\beta \to \gamma$	$\alpha \to (\beta \to \gamma)$ (W)
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	1	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	1	0	0	1	1
1	1	1	1	1	1	1	1

Per tant, és una tautologia.

Mètode 2. Vegem que no existeix cap assignació de 0,1 a les lletres que produeixi un valor 0 per a la fórmula. Suposem que sí i arribem a una contradicció.

$$(p \to q) \to ((q \to r) \to (p \to r)) \text{ (és un condicional).}$$

$$(p \to q) \xrightarrow{\mathbf{0}} ((q \to r) \to (p \to r)).$$

$$(p \xrightarrow{1} q) \xrightarrow{\mathbf{0}} ((q \to r) \xrightarrow{0} (p \to r)).$$

$$(p \xrightarrow{1} q) \xrightarrow{\mathbf{0}} ((q \xrightarrow{1} r) \xrightarrow{0} (p \xrightarrow{0} r)).$$

$$(p \xrightarrow{1} q) \xrightarrow{\mathbf{0}} ((q \xrightarrow{1} r) \xrightarrow{0} (\overset{1}{p} \xrightarrow{0} \overset{0}{r})).$$

$$(\overset{1}{p} \xrightarrow{1} q) \xrightarrow{\mathbf{0}} ((q \xrightarrow{1} \overset{0}{r}) \xrightarrow{0} (\overset{1}{p} \xrightarrow{0} \overset{0}{r})).$$

$$(\overset{1}{p} \xrightarrow{1} \overset{\boxed{1}}{q}) \xrightarrow{\mathbf{0}} ((\overset{\boxed{0}}{q} \xrightarrow{1} \overset{0}{r}) \xrightarrow{0} (\overset{1}{p} \xrightarrow{0} \overset{0}{r})).$$

Deduïm una assignació incompatible de valors de veritat per a q. Per tant, és tautologia.

4.9. Entreteniment

PROBLEMA 4.60

Siguin p,q proposicions atòmiques (lletres proposicionals). Completeu la taula de veritat:

p	q	$\neg q$	$p \wedge (\neg q)$
1			*0*
			1
0		*0*	*0*
		1	*0*

Solució

Pas 1:

p	q	$\neg q$	$p \wedge (\neg q)$
1		**0**	0
1		**1**	1
0	**1**	0	0
0		1	0

Pas 2:

p	q	$\neg q$	$p \wedge (\neg q)$
1	**1**	0	0
1	**0**	1	1
0	1	0	0
0	**0**	1	0

PROBLEMA 4.61

Siguin p, q lletres proposicionals. Completeu la taula de veritat:

p	q	$\neg p$	$\neg p \vee q$
	1	*1*	
1			*1*
			0
	0		*1*

Solució

Pas 1:

p	q	$\neg p$	$\neg p \vee q$
0	1	1	
1		**0**	1
	0	**0**	0
	0	**1**	1

Pas 2:

p	q	$\neg p$	$\neg p \vee q$
0	1	1	**1**
1	**1**	0	1
1	0	0	0
0	0	1	1

PROBLEMA 4.62

Siguin p, q, r lletres proposicionals. Completeu la taula de veritat:

p	q	r	$\neg q$	$p \wedge r$	$(p \wedge r) \vee \neg q$
1		*0*			*1*
			0		*1*
0	*0*	*0*			
0		*0*			*0*
1					*0*
	1	*1*		*0*	
	0			*1*	
0		*1*	*1*		

Solució

Pas 1:

p	q	r	$\neg q$	$p \wedge r$	$(p \wedge r) \vee \neg q$
1		0		**0**	1
	1		0	**1**	1
0	0	0	**1**	**0**	
0		0		**0**	0
1			**0**	**0**	0
0	1	1	**0**	0	
1	0	**1**	**1**	1	
0	**0**	1	1	**0**	**1**

Pas 2:

p	q	r	$\neg q$	$p \wedge r$	$(p \wedge r) \vee \neg q$
1		0	**1**	0	1
1	1	**1**	0	1	1
0	0	0	1	0	**1**
0		0	**0**	0	0
1	**1**	**0**	0	0	0
0	1	1	0	0	**0**
1	0	1	1	1	**1**
0	0	1	1	0	1

Pas 3:

p	q	r	$\neg q$	$p \wedge r$	$(p \wedge r) \vee \neg q$
1	**0**	0	1	0	1
1	1	1	0	1	1
0	0	0	1	0	1
0	**1**	0	0	0	0
1	1	0	0	0	0
0	1	1	0	0	0
1	0	1	1	1	1
0	0	1	1	0	1

→ 5

Lògica de predicats. Llenguatge de predicats

$$\forall x \exists y \forall z ((P(x,y,z) \rightarrow (\neg R(x,z) \rightarrow \exists w (\neg S(w))))$$

En aquest capítol, estem interessats en les fórmules de predicat que puguin correspondre a enunciats. En cas que siguin certs, no en farem cap demostració, i tampoc no aportarem cap contraexemple en cas que siguin falsos, llevat que es demani explícitament; estem essencialment interessats en la simbolització i la formalització.

5.1. Insuficiència del llenguatge de proposicions

El llenguatge de proposicions presenta diverses insuficiències. Per exemple:

a) Les frases són vistes com un tot, sense considerar cap estructura interna possible.

b) No disposem de variables.

c) No podem expressar generalitzacions amb elements del llenguatge ordinari del tipus "per a tot", "cada", "qualsevol". En realitat, no hi ha cap impediment a afirmar "tots els homes són mortals", però, des del punt de vista del llenguatge, s'ha de considerar la frase sencera com un tot (p), sense cap estructura per a expressar "tots ...".

Exemple 5.1 Com a proposicions, les frases següents són vistes *com un tot*, sense parts separades, indivisible, sense estructura manifesta:

"El gat dorm" "En Joan estudia" "L'alumne estudia" "$5 > 0$" ■

Això ens treu capacitat analítica i manipulativa, i finalment expressiva. Hem d'entrar en l'estructura de la fórmula i distingir-ne els components per tal de poder tractar-los separadament, si cal.

Sense variables. El fet de no disposar de variables, i no considerar l'estructura interna de la frase, fa que, si ara volem expressar que també "el gos dorm", hem de fer una frase separada, completament independent de la donada anteriorment ("el gat dorm").

No podem fer servir *un mateix patró* per a les dues, patró del qual es generarien “el gat dorm” i “el gos dorm”. No podem aprofitar la mateixa estructura, cosa que resulta ineficient. Anàlogament, si volem afirmar que la Maria també estudia, hem de construir una frase independent: “La Maria estudia”. En llenguatge de proposicions, no hi ha relació entre les afirmacions $5 > 0$, $6 > 0$, $-1 > 0$.

També podem escriure:

“3 és senar $\rightarrow 3^2$ és senar”,

“5 és senar $\rightarrow 5^2$ és senar”, ...

però no anirem molt lluny amb afirmacions similars. Volem poder dir que aquesta propietat és vàlida per a $5, 7, \cdots$ i, de fet, per a un nombre enter n arbitrari senar (però fix) i, finalment, per a **tot** n enter.

Voldríem poder escriure D(el gos), D(el gat), i produir, respectivament, “el gos dorm”, “el gat dorm” (“x dorm”, $D(x)$).

Exemple 5.2 El llenguatge de proposicions no ens permet expressar frases com les següents (algunes de les següents diuen el mateix, són equivalents, en el sentit que tenen el mateix significat); totes són vistes com un tot:

“Si n és un nombre enter senar, aleshores n^2 és senar” (falten variables en el llenguatge),

“Si n és un nombre enter senar qualsevol, aleshores n^2 és senar” (falten variables i poder expressar ‘qualsevol’ en el llenguatge),

“Per tot nombre enter senar parell, el quadrat també és parell” (falten variables i poder expressar ‘qualsevol’ en el llenguatge),

“Els quadrats dels nombres enters senars són senars” (falten variables i quantificadors en el llenguatge). ■

Exemple 5.3 Considereu:

“Josep té els ulls blaus” “Maria té els ulls blaus” “En Joan té els ulls blaus”

Observeu que, en llenguatge de proposicions, els exemples anteriors són proposicions p, q, r no relacionades:

p=“Josep té els ulls blaus” (és un tot, simplement un opac p, sense estructura interna que hàgim posat de manifest)

q=“Maria té els ulls blaus”

r=“en Joan té els ulls blaus”

Com expressar aquestes afirmacions a partir d’un mateix patró? ■

Exemple 5.4 Com expressar en el llenguatge de proposicions l'argumentació clàssica?:

"Tots els homes són mortals"

"Sòcrates és un home"

"Sòcrates és mortal"

El llenguatge no és prou fi per a això. Simplement seria:

$p =$ "Tots els homes són mortals"

$q =$ "Sòcrates és un home"

$r =$ "Sòcrates és mortal"

És a dir:

p

q

r ■

No anirem gaire lluny només amb les proposicions. Amb les fórmules proposicionals i, en general, amb el llenguatge o càlcul de proposicions, no es pot anar gaire lluny. Necessitem una generalització i incorporar-hi nous elements. Cal considerar un llenguatge que no presenti aquests problemes o insuficiències: **el llenguatge de predicats**.

5.2. Variables i predicats

Per tal d'augmentar la capacitat expressiva (i la potència del llenguatge) hem d'introduir:

- els predicats
- les variables
- les connectives (les mateixes que en el llenguatge de proposicions)
- els quantificadors (universal i existencial)
- les fórmules de predicats, amb les regles de formació de fórmules "ben formades".

Vegeu una fórmula de predicats típica:

$$\forall x \exists y \forall z (P(x,y,z) \rightarrow (\neg R(x,z) \rightarrow \exists w(\neg S(w))))$$

Descripció dels components de la fórmula:

Variables: x, y, z, w (lletres)

Quantificadors: $\forall$ (universal, "per a tot"), $\exists$ (existencial, "existeix")

Predicats: P, R, S (lletres), lletres de predicat

Connectives: $\rightarrow, \neg$.

Estructura subjecte-predicat d'una frase

Volem expressar a partir d'un mateix patró:

"Josep té els ulls blaus"

"Maria té els ulls blaus"

"En Joan té els ulls blaus"

o bé:

"Josep estudia"

"Maria estudia"

"Joan estudia"

En primer lloc, i des del punt de vista lingüístic i gramatical en el llenguatge ordinari, analitzem les frases anteriors i descomponem el tot en parts: *subjecte* i *predicat*. Posem de manifest una estructura interna. Així:

Subjecte: Maria

Predicat: té els ulls blaus

$$\underbrace{\text{Maria}}_{\textit{subjecte}}\underbrace{\text{té els ulls blaus}}_{\textit{predicat}}$$

Hem de generalitzar per la banda de les propietats o accions (predicats) i també per la banda del subjecte (variables).

5.2.1. Predicats

Què és un predicat (nivell gramatical)? És allò que es diu o afirma (es "predica") d'un subjecte:

- accions (per exemple, estudia, resol problemes, programa, estudia C++, dissenya un videojoc, fa un gràfic 3D per ordinador, va a la biblioteca, sap dibuixar).
- propietats (per exemple, tenir els ulls blaus, ser parell, ser no negatiu, ser mortal, ser més gran que 1, tenir el quadrat més gran que 2, ser enter).

Podem incrementar el nivell d'abstracció, formalització i simbolització, i assignar símbols als predicats, cosa que correspondria a una descripció conceptual, sense fórmules, si fos el cas. Aquestes són les **lletres de predicat**. Per exemple:

Exemple 5.5

$D =$"saber dibuixar" $\quad R =$"dormir"

$E =$"ser enter" $\quad H =$"ser home"

$S =$"ser senar" $\quad M =$"ser mortal"

$B =$"tenir els ulls blaus" $\quad G =$"ser més gran que 1" ■

$T =$"estudiar"

Alguns es poden formular mitjançant fórmules, sobretot els que tenen relació amb les matemàtiques. Per exemple:

“ser senar” és “no ser divisible per 2” (per exemple, $2 \nmid 5$)

“ser més gran que 1” (per exemple, $5 > 1$)

En alguns casos, hi pot haver **funcions** involucrades, com “ser de quadrat més gran que 5” (amb la funció $f(x) = x^2$, $3^2 > 5$, el quadrat de 3 és més gran que 5).

5.2.2. Variables

A què s’apliquen els predicats? A subjectes (constants i variables).

Podem aplicar els predicats a “**constants**”, com per exemple: “Sòcrates és mortal”, “23 és enter”, “42 és senar” (una afirmació falsa), “63 és senar”. I podem adoptar una notació funcional per a les constants. Així:

$M(s)$ si s representa “Sòcrates” o directament $M(\text{Sòcrates})$, per a expressar “Sòcrates és mortal”.

$B(\text{Maria})$

$G(4)$ (“4 és més gran que 1” o, en fórmula, $4 > 1$).

Però també volem poder-ho aplicar a “variables” i poder dir “x té els ulls blaus” i, com a cas particular per a $x =$Maria, generar “Maria té els ulls blaus”.

Variables i universal. Volem poder afirmar propietats per a variables. Per exemple

Exemple 5.6

“x és positiu” o, equivalentment, $x > 0$.

“x és un home”

“x estudia”

“x dorm”

“x és de quadrat més gran que 5”, o bé $x^2 > 5$, o bé “el quadrat de x és més gran que 5”.
■

La manera de formalitzar això és introduint un *domini de variables*, *l’universal*. Aquestes variables són objectes que pertanyen a un conjunt U, que anomenem l’**universal** o **univers de discurs** per a aquestes variables. També es diu que és el **domini** de les variables. Què pot ser l“universal”? L’universal és el que convé per a cada situació. És el lloc on varien les variables, valgui la redundància. És un conjunt no buit on poden prendre valors les variables d’un predicat. També es denota per Ω. Per exemple, si estem enunciant una propietat per als nombres reals, aleshores $\Omega = \mathbb{R}$; si és una propietat sobre els enters, $\Omega = \mathbb{Z}$.

Versió funcional amb variables. Hem presentat una versió conceptual: “B”, tenir els ulls blaus. Expressem funcionalment “x té els ulls blaus” amb variables com a $B(x)$, és a dir:

$$B(x) = \text{“}x \text{ té els ulls blaus”} \text{ (expressió funcional amb variables).}$$

Per al cas particular que $m =$ Maria, aleshores és $B(m)$. En els exemples anteriors, i adoptant una sintaxi funcional, podem expressar “Maria té els ulls blaus” com $B(Maria)$ i, anàlogament, per a tots els altres: $B(Joan)$, $B(Josep)$. També en serien exemples $T(Josep)$, $T(Maria)$, $T(Joan)$ si $T(x) =$ “x estudia”.

Visió dels predicats com a “generadors” de proposicions

Podem considerar un predicat com una afirmació que es formula en termes d’una o més variables. $P(x)$ mai no serà una ordre o una exclamació. Per a un valor concret de la variable (si depèn només d’una variable), s’obté una proposició. És a dir, si $u_0 \in U$, aleshores $P(u_0)$ és una proposició.

Si considerem $x \in \mathbb{R}$ i és $P(x) = (x > 0)$, resulta que “$(x > 0)$” no és una proposició, ja que no li podem atribuir cap valor de veritat o falsedat. Però, si donem valor a x, és a dir, fem que varïi en el seu domini ($x \in \mathbb{R}$), aleshores es genera una proposició per a cada valor de x concret:

$P(-1)$ és “$-1 > 0$”, que és una proposició (falsa)
$P(0)$ és “$0 > 0$”, que és una proposició (falsa)
$P(2)$ és “$2 > 0$”, que és una proposició (certa)

D’alguna manera, $P(x)$ es pot considerar com una “proposició” parametritzada. Per a cada “paràmetre” o valor x_0 concret , $P(x_0)$ és una proposició.

Exemple 5.7 En el cas de $U = \{-1, 0, 2, 5\}$, $P(x) = (x > 4)$ “genera” les proposicions:

$$(-1 > 4) \qquad (0 > 4) \qquad (2 > 4) \qquad (5 > 4) \ \blacksquare$$

Exemple 5.8 En el cas de $\Omega = \{1, 2, 3\}$, $Q(x) = (x < 0)$ “genera” les proposicions:

$$Q(1) = (1 < 0) \qquad Q(2) = (2 < 0) \qquad Q(3) = (3 < 0) \ \blacksquare$$

5.3. Extensió del llenguatge de proposicions: llenguatge de predicats

Presentem una versió **informal** del llenguatge de predicats; més endavant el descrivim amb precisió.

Ara ja veiem com hem ampliat o generalitzat el llenguatge de proposicions, amb variables i predicats:

La proposició “Maria té els ulls blaus” no és més que un cas particular de la família de frases “x té els ulls blaus”, de manera que, si considerem el predicat $B(x) =$ “x té els ulls blaus”, es pot obtenir la proposició com a $B(Maria)$.

Però falten més coses. D'entrada, cal poder compondre predicats per tal d'obtenir predicats nous mitjançant connectives, com veiem seguidament: podem obtenir la proposició composta "15 és múltiple de 3 i 15 és múltiple de 5" com a $T(15) \wedge C(15)$, amb els predicats $T =$ "ser múltiple de 3" i $C =$ "ser múltiple de 5" (versió conceptual). També en versió funcional, $T(n) =$ "n és múltiple de 3", $C(n) =$ "n és múltiple de 5", o bé $T(n) = (3|n), C(n) = (5|n)$.

5.3.1. Connectives amb predicats

De manera paral·lela amb el càlcul o el llenguatge de proposicions, volem poder efectuar un "càlcul" amb predicats, és a dir, obtenir o formular predicats nous a partir de predicats existents. Així, per a n nombre enter, a partir de

"n és múltiple de 3"

"n és múltiple de 5"

volem poder formar "n és múltiple de 3 i n és múltiple de 5", és a dir, equivalentment, "n és múltiple de 3 $\wedge$ n és múltiple de 5", o bé $3|n \wedge 5|n$. Hem utilitzat les connectives per a formar una nova fórmula de predicats. Les variables poden ser diferents: $2|a \wedge 2 \nmid b$, i fins i tot poden ser de tipus diferents.

Quines connectives tenim? Les mateixes que les del llenguatge de proposicions:

$\neg$	no	negació
$\vee$	o	disjunció (o no exclusiu)
$\wedge$	i	conjunció
$\rightarrow$	condicional	si ..., aleshores ... (i altres: condició necessària, condició suficient, només si)
$\leftrightarrow$	bicondicional	... si, i només si, ... (i altres variants, com: condició necessària i suficient)

Tenen el mateix significat que per a fórmules proposicionals. Exemples addicionals:

Exemple 5.9

$2|n \wedge 2 \nmid m$

$2|n \rightarrow 2|n^5$

$3|n^7 \rightarrow 3|n^2$

$5|n^3 \rightarrow 5|n$ ■

Existeix la taula de veritat d'una fórmula de predicats? **No existeix la "taula de veritat"** d'una fórmula en funció de les variables (no lògiques en general), que poden prendre infinits valors, dels dominis.

Ara bé, res no impedeix descriure tabularment el comportament veritatiu d'una connectiva amb predicats per a unes variables fixades, tot i que puguin ser arbitràries, que poden pertànyer a dominis finits o infinits.

Quin és el comportament veritatiu quan utilitzem les connectives amb predicats? Essencialment, el mateix que en el cas de les proposicions, **fixades les variables**. Podem pensar-ho així:

Podem dir que a $A \wedge B$ hem substituït $A = (3|n)$ i $B = (5|n)$, per a n fix (tot i que n arbitrària). Per a un n **fix**, s'obté una proposició concreta, que serà certa o falsa, el que sigui, i, per tant, se li pot aplicar la taula de veritat de la conjunció.

Fixat $x = a$, $P(x) \wedge Q(x)$ és cert si, i només si, $P(x)$ i $Q(x)$ són certs. Per a cada n serà el que correspongui, la fila que correspongui a la taula de la conjunció. Per exemple, per a $x = 3$, $P(3) \wedge Q(3)$ és cert, si, i només si, $P(3)$ i $Q(3)$ són certs.

També pot ser $P(x) \vee Q(y)$ o es poden considerar altres fórmules, com per exemple

$P(x) \vee \neg Q(y)$.

Fixat x, i per a aquest x,

$P(x)$	$Q(x)$	$P(x) \wedge Q(x)$
0	0	0
0	1	0
1	0	0
1	1	1

En el cas anterior de divisibilitat, (**fixat** n) vegeu les diverses possibilitats:

Fixat n,

$3\|n$	$5\|n$	$3\|n \wedge 5\|n$
0	0	0
0	1	0
1	0	0
1	1	1

En concret (no és una taula de veritat; és només la descripció de diversos casos),

Fixat n,

n	$3\|n$	$5\|n$	$3\|n \wedge 5\|n$
$n = 17$	0	0	0
$n = 20$	0	1	0
$n = 18$	1	0	0
$n = 30$	1	1	1

Versió conceptual. Per tant, podem aplicar connectives per tal d'obtenir predicats i fórmules de predicats més complexes:

Considerem fixades (tot i que arbitràries) les variables que hi apareixen. Limitarem aquí l'exposició a predicats d'una variable, però això no és obligatori; una descripció general complicaria les fórmules innecessàriament:

1. $\neg P(x)$ és cert si, i només si, $P(x)$ és fals.
2. $P(x) \wedge Q(y)$ és cert si, i només si, $P(x)$ i $Q(y)$ són certs.

3. $P(x) \vee Q(y)$ és cert si, i només si, algun dels $P(x)$ i $Q(y)$ és cert (o tots dos).
4. $P(x) \to Q(y)$ és fals si, i només si, $P(x)$ és cert i $Q(y)$ és fals.
5. $P(x) \leftrightarrow Q(y)$ és cert si, i només si, ambdós tenen els mateixos valors de veracitat (ambdós certs, ambdós falsos).

Exemple 5.10 Vegem i analitzem una fórmula de predicats on s'utilitzen connectives:

$$(P(x,y) \wedge Q(x,t)) \to \neg(R(x) \to \neg S(z,t))$$

Descripció de la fórmula:

Variables: x, y, z, t (lletres)

Predicats (2–aris): P, Q, S (lletres)

Predicats (1–aris): R (lletres)

Connectives: $\wedge, \to, \neg$

Connectiva principal: $\to$ (esquerra)

$(P(x,y) \wedge Q(x,t)) \longrightarrow \neg(R(x) \to \neg S(z,t))$

Què "és" la fórmula?: Un condicional.

No quantificada (sense quantificadors). ■

Equivalències. Per tant, es poden estendre les "taules de veritat" (sempre amb les variables fixades) i també, a partir de les equivalències per a proposicions, derivem les corresponents per a fórmules de predicat (sempre amb les variables fixades).

Així:

1. De l'equivalència de De Morgan $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$, per substitució, i **fixades les variables**, podem escriure que són equivalents

$$\neg(P(x) \vee Q(y)) \equiv (\neg P(x) \wedge \neg Q(y)).$$

2. O estendre l'equivalència lògica del contrarecíproc, que ens permet afirmar que són equivalents (sempre amb les variables **fixades**), per exemple:

$$P(x) \to Q(x) \text{ i } \neg Q(x) \to \neg P(x)$$

3. $\neg\neg P(x)$ i $P(x)$ són equivalents.
4. $\neg(P(x) \to Q(x))$ i $P(x) \wedge \neg Q(x)$ són equivalents
5. $P(x) \to Q(x)$ i $\neg P(x) \vee Q(x)$ són equivalents.

Exemples 5.11 Per a enters,

Exemple 1. $2 \nmid n \to 2 \nmid n^7$ equival a $\neg(2 \nmid n^7) \to \neg(2 \nmid n)$, que equival a $2|n^7 \to 2|n$. ■

Exemple 2. $2|ab \to (2|a \vee 2|b)$, que equival a $\neg(2|a \vee 2|b) \to \neg(2|ab)$ (pel contrarecíproc), que equival a $(2 \nmid a \wedge 2 \nmid b) \to 2 \nmid ab$ (per De Morgan). ■

Exemple 5.12 Escrivim diverses negacions equivalents de la fórmula

$$F = (P(x,y) \wedge Q(x,t)) \rightarrow \neg(R(x) \rightarrow \neg S(z,t)).$$

$\neg F \equiv$ (la connectiva principal és el condicional de l'esquerra de la fórmula),

$\equiv (P(x,y) \wedge Q(x,t)) \wedge \neg\neg(R(x) \rightarrow \neg S(z,t))$ (per equivalència de negació del condicional),

$\equiv (P(x,y) \wedge Q(x,t)) \wedge (R(x) \rightarrow \neg S(z,t))$ (per equivalència de doble negació). ■

5.3.2. Quantificadors

Fins aquí hem parlat de predicats i variables (a més del conjunt universal). Falta poder quantificar i poder formalitzar, finalment en una fórmula, les expressions "per a tot", "cada", "qualsevol", "qualssevol" i diversos equivalents, com a les expressions següents:

"**Per a tot** nombre enter n senar, n^2 és senar".

"Si n és un nombre enter senar **qualsevol**, aleshores n^2 és senar."

"El quadrat de **tot** nombre real és no negatiu".

"**Tots** els homes són mortals" o "tot home és mortal" o "els homes són mortals (quantificador amagat)".

"Per a x,y nombres reals **qualssevol**, $(x+y)^2 = x^2 + 2xy + y^2$".

I també altres expressions:

"**Existeixen** nombres reals positius"

"No **existeixen** solucions reals de l'equació $x^2 + 1 = 0$"

"**Existeix** alguna solució real de $x^2 = 3$"

"**Hi ha** algun alumne a la classe"

Són quantificadors:

$\exists$	existeix	quantificador existencial
$\forall$	per a tot	quantificador universal

$\forall x P(x)$ ***Quantificador universal***. Si P és un predicat amb univers de discurs Ω, aleshores la fórmula quantificada bàsica és $\forall x P(x)$. Vegeu l'ús del símbol $\forall$ ("per a tot"). Es llegeix "per a tot x, $P(x)$". Que $\forall x P(x)$ sigui una fórmula certa vol dir que "per a tot $x \in \Omega$, $P(x)$ és una proposició certa".

Vegem com podem formalitzar, en termes d'una fórmula de predicats, alguns dels enunciats anteriors. Les formalitzacions poden variar segons si s'incorporen els universals a la fórmula:

Exemples 5.13

Exemple 1. “Tot enter positiu és primer” (fals)
$\forall n(n \text{ és primer})$ (se sobreentén $\Omega = \mathbb{Z}$).
$\forall n(n \in \mathbb{Z} \to n \text{ és primer})$ $(\Omega = \mathbb{Z})$. ■

Exemple 2. “El quadrat de tot nombre real és no negatiu” (cert)
Es podria llegir de diverses maneres:

“per a tot x que sigui real, és $x^2 \geq 0$”
“per a tot x, si x és real, aleshores $x^2 \geq 0$”
“per a tot nombre real x, és $x^2 \geq 0$”
“per a cada nombre real x, és $x^2 \geq 0$”
“per a nombres reals x qualssevol, és $x^2 \geq 0$”
“si x és un nombre real qualsevol, aleshores és $x^2 \geq 0$”
(i altres variants equivalents).

O també, amb una altra estructura de frase:

“Sigui x un nombre real qualsevol. Aleshores, és $x^2 \geq 0$” (i variants).

Possibles formalitzacions:

$\forall x(x^2 \geq 0)$, amb $\Omega = \mathbb{R}$
$\forall x(x \in \mathbb{R} \to x^2 \geq 0)$ $(\Omega = \mathbb{R})$. ■

Exemple 3. Per a tot nombre enter n senar, n^2 és senar”. Es pot formalitzar com:

$$\forall n(2 \nmid n \to 2 \nmid n^2), \text{ amb } \Omega = \mathbb{Z}. \ ■$$

Exemple 4. Amb **més** d’un quantificador:

$$\forall a \forall b((2 \nmid a) \wedge (2 \nmid b) \to 2 \nmid ab) \text{ (amb } \Omega = \mathbb{Z}). \ ■$$

Exemple 5. Amb **més** d’un quantificador:

$\forall x \forall y((x+y)^2 = x^2 + 2xy + y^2)$ (amb $\Omega = \mathbb{R}$).
$\forall x \forall y((x \in \mathbb{R} \wedge x \in \mathbb{R}) \to (x+y)^2 = x^2 + 2xy + y^2)$. ■

Generalització per quantificació universal. Considerem l’enunciat (per a enters):

“si a i b són parells, aleshores $a+b$ és parell”, que podem formalitzar com $(2|a \wedge 2|b) \to 2|(a+b)$.

La propietat s’enuncia per a a, b fixats, tot i que arbitraris. No conté cap quantificador. Però es pot *generalitzar* immediatament l’enunciat, quantificant-lo (quantificació universal):

$\forall a \forall b((2|a \wedge 2|b) \to 2|(a+b))$.

Exemples 5.14

Exemple 1. Si n és un nombre enter, aleshores $3 \nmid n \leftrightarrow 3 \nmid n^4$. Atès que n és arbitrari, podem generalitzar: $\forall n(3 \nmid n \leftrightarrow 3 \nmid n^4)$, amb $\Omega = \mathbb{Z}$. ■

Exemple 2. Si n és un nombre enter, aleshores $5|n \leftrightarrow 5|n^{12}$. Atès que n és arbitrari, podem generalitzar: $\forall n(5|n \leftrightarrow 5|n^{12})$, amb $\Omega = \mathbb{Z}$. ■

$\exists xP(x)$ ***Quantificació existencial***. Es forma amb el símbol $\exists$ ("existeix"). La fórmula més bàsica és $\exists xP(x)$, si $P(x)$ és un predicat amb univers de discurs Ω. Que $\exists xP(x)$ és certa significa que existeix un $x \in \Omega$ tal que la proposició $P(x)$ és certa.

Exemples 5.15

Exemple 1. "Existeix arrel quadrada de 2 en els racionals" (fals)

$\exists x(x^2 = 2)$ $(\Omega = \mathbb{Q})$ (fals)
$\exists x(x \in \mathbb{Q} \wedge x^2 = 2)$. ■

Exemple 2. "Existeix arrel quadrada de 2 en els reals" (cert)

$\exists x(x^2 = 2)$ $(\Omega = \mathbb{R})$ (cert)
$\exists x(x \in \mathbb{R} \wedge x^2 = 2)$. ■

Exemple 3. "Existeixen nombres naturals múltiples de 4" (cert)

"Algun nombre natural és múltiple de 4"
"Hi ha nombres naturals múltiples de 4"
"$4|n$ per a algun nombre natural n"
"Per a algun nombre natural m, $4|m$"
$\exists x(4|x)$ $(\Omega = \mathbb{N})$
$\exists x(x \in \mathbb{N} \wedge 4|x)$ $(\Omega = \mathbb{N})$ ■

Més d'un quantificador (existencial i/0 universal). Vegem-ne alguns exemples:

Exemples 5.16

Exemple 1. $\forall x \forall y P(x,y)$. ■

Exemple 2. $\forall x \forall y((x+y)(x-y) = x^2 - y^2)$ $(\Omega = \mathbb{R})$.

Com es llegeix? "Per a tot x i per a tot y ..." o bé "Per a qualssevol nombres reals x, y, $(x+y)(x-y) = x^2 - y^2$". ■

Exemple 3. $\exists x \forall y(y + x = y)$ $(\Omega = \mathbb{R})$

Com es llegeix? "Existeix un x *tal que*, per a tot y ..." (existència d'element neutre per a la suma). ■

Exemple 4. $\forall x \exists x' (x + x' = 0)$ (existència d'element oposat). Es llegeix: "Per a tot x, existeix un x' tal que $x + x' = 0$". ■

$\forall x \forall y (2 \nmid xy \rightarrow (2 \nmid x \wedge 2 \nmid y))$ $(\Omega = \mathbb{Z})$. ■

Atenció: En molts textos, de vegades s'escriu amb sintaxi més relaxada; i així, per exemple, trobem diverses variants, acceptades, però ja fora de la gramàtica del llenguatge:

$(x+y)(x-y) = x^2 - y^2$, per a tot real x, y
$(x+y)(x-y) = x^2 - y^2$, $\forall x$, $\forall y$
$(x+y)(x-y) = x^2 - y^2$, $\forall x, y$
$(x+y)(x-y) = x^2 - y^2$, $\forall x \in \mathbb{R}$, $\forall y \in \mathbb{R}$
$(x+y)(x-y) = x^2 - y^2$, $\forall x, y \in \mathbb{R}$.

Idea de la negació de les fórmules quantificades bàsiques. Tot i que se sistematitzarà en una secció posterior, esmentem ara breument la qüestió.

Considerem l'exemple:

"No existeixen nombres naturals negatius"

Seria, literalment, $\neg \exists x (x \in \mathbb{N} \wedge x < 0)$.

Certament, equival a dir que, "per a tot nombre natural x, és $x \geq 0$".

L'estructura de negació d'un quantificador existencial és, en un cas senzill, $\neg \exists x P(x) \equiv \forall x \neg P(x)$.

A l'exemple anterior, com podem arribar de forma automàtica a l'afirmació sobre la negació? Segueix una seqüència de fórmules equivalents a la negació:

$\neg \exists x (x \in \mathbb{N} \wedge x < 0)$,
$\forall x \neg (x \in \mathbb{N} \wedge x < 0)$ (apliquem $\neg \exists x P(x) \equiv \forall x \neg P(x)$),
$\forall x (\neg x \in \mathbb{N} \vee \neg x < 0)$ (De Morgan),
$\forall x (\neg x \in \mathbb{N} \vee x \geq 0)$ (reescriptura),
$\forall x (x \in \mathbb{N} \rightarrow x \geq 0)$ (expressió del condicional en termes de negació i disjunció).

Exercici: Negueu $\exists x (x \in \mathbb{Q} \wedge x^2 = 2)$.

L'estructura de negació d'un quantificador universal és, en un cas senzill, $\neg \forall x P(x) \equiv \exists x \neg P(x)$.

Si sabem negar les fórmules amb quantificadors $(\forall, \exists)$, tindrem ja el necessari per a obtenir negacions de qualsevol fórmula de predicats.

Com traduir frases del llenguatge natural a una fórmula de predicats? Alguns consells bàsics. Tot i que hi dedicarem seccions posteriors, vegem-ne ara una primera idea. En els exemples anteriors, ja s'han utilitzat aquestes idees bàsiques, sense explicitar-les.

a) Una frase de la forma “Tots els A són B” es tradueix a $\forall x(A(x) \rightarrow B(x))$. Dins el parèntesi es pot substituir pel contrarecíproc:

$$\forall x(\neg B(x) \rightarrow \neg A(x)).$$

b) Una frase de la forma “Algun A és B” es tradueix per $\exists x(A(x) \wedge B(x))$.

c) Una frase de la forma “Cap A és B” es tradueix per $\forall x(A(x) \rightarrow \neg B(x))$ o bé, substituint pel contrarecíproc, $\forall x(B(x) \rightarrow \neg A(x))$.

Exemple 5.17 Vegem-ne l’exemple clàssic.

Amb l’elecció de les lletres de predicat convenients i òbvies, “**tots els homes són mortals**” es pot formalitzar mitjançant la fórmula de predicat següent:

$H =$ “ser home” ($H(x) =$ “x és home”.

$M =$ “ser mortal” ($M(x) =$ “x és mortal”.

$\forall t(H(t) \rightarrow M(t))$ (tots els homes són mortals)

$H(s)$ (Sòcrates és home, $s =$ “Sòcrates”)

Per tant,

$M(s)$ (Sòcrates és mortal). ■

Altres aspectes: irrellevància de quines són les variables. Considerem la fórmula:

$$\forall n(15|n \rightarrow (3|n \wedge 5|n)), \text{ amb } U = \mathbb{Z}, n \in \mathbb{Z}$$

La variable quantificada n és irrellevant, i pot ser substituïda per alguna altra, com per exemple:

$\forall a(15|a \rightarrow (3|a \wedge 5|a))$

$\forall m(15|m \rightarrow (3|m \wedge 5|m))$

Algunes equivalències amb quantificadors en fórmules de predicat (resum)

$\neg\forall x P(x) \equiv \exists x \neg P(x) \qquad \forall x P(x) \equiv \neg\exists x \neg P(x)$

$\neg\exists x P(x) \equiv \forall x \neg P(x) \qquad \exists x P(x) \equiv \neg\forall x \neg P(x)$

(“existeix i és únic”):

$\exists! x P(x) \equiv \exists x(P(x) \wedge \forall t(P(t) \rightarrow t = x))$ (existeix un únic x tal que $P(x)$). Aquí la unicitat es formula depenent de l’existència prèvia.

(“existeix i és únic”):

$\exists! x P(x) \equiv \exists x P(x) \wedge \forall r \forall s((P(r) \wedge P(s)) \rightarrow r = s)$ (variant, un altre matís, on s’afirma la unicitat amb independència de l’existència).

$\forall x \forall y P(x,y) \leftrightarrow \forall y \forall x P(x,y)$ $\qquad$ $\forall x \forall y P(x,y) \equiv \forall y \forall x P(x,y)$

$\exists x \exists y P(x,y) \leftrightarrow \exists y \exists x P(x,y)$ $\qquad$ $\exists x \exists y P(x,y) \equiv \exists y \exists x P(x,y)$

$\exists x \forall y P(x,y) \rightarrow \forall y \exists x P(x,y)$

$\exists x(A(x) \vee B(x)) \leftrightarrow (\exists x A(x) \vee \exists x B(x))$

$\exists x(A(x) \wedge B(x)) \rightarrow (\exists x A(x) \wedge \exists x B(x))$

$\forall x(A(x) \wedge B(x)) \leftrightarrow (\forall x A(x) \wedge \forall x B(x))$

$\forall x(A(x) \vee B(x)) \rightarrow (\forall x A(x) \vee \exists x B(x))$

$(\forall x A(x) \vee \forall x B(x)) \rightarrow \forall x(A(x) \vee B(x))$

Observeu que, de les dues primeres equivalències (dreta), resulta que *amb un sol quantificador n'hi ha prou*, ja que qualsevol d'ells s'expressa en termes de l'altre (i utilitzant negacions).

Observació sobre $(\forall x A(x) \vee \forall x B(x)) \rightarrow \forall x(A(x) \vee B(x))$. No es pot afirmar l'equivalència. En efecte, suposem que $\Omega = \mathbb{Z}$, i que els predicats són A ("ser parell") i B ("ser senar). Aleshores tindríem que $\forall x(A(x) \vee B(x))$ és cert ("tot enter és parell o és senar") i, en canvi, $\forall x A(x) \vee \forall x B(x)$ no és cert ("tots els enters són parells o tots els enters són senars").

5.3.3. Fórmules de predicat

Amb tot l'anterior, ja tenim tots els ingredients per a formar fórmules de predicats. Vegem alguns exemples de fórmules de predicat (posteriorment, se'n presentarà la sintaxi formal, la gramàtica de generació i la definició de fórmula ben formada):

Exemples 5.18

Exemple 1. Expressió de la propietat de ser múltiple de 3 per a un enter n mitjançant una fórmula de predicats: "n és múltiple de 3 si, i només si, existeix un enter k tal que $n = 3k$". Ho traduïm per:

$\exists k(k \in \mathbb{Z} \wedge n = 3k)$ (observeu que "tal que" és "i").

Si queda sobreentès que $\Omega = \mathbb{Z}$, o s'explicita exteriorment a la fórmula, aleshores és: $\exists k(n = 3k)$.

Fora de la sintaxi estàndard també podem escriure: $\exists k \in \mathbb{Z}(n = 3k)$.

La frase completa és: $3|n \leftrightarrow \exists k(k \in \mathbb{Z} \wedge n = 3k)$.

Exemple 2. Expressió de la propietat de no ser múltiple de 3 per a un enter n mitjançant una fórmula de predicats:

$\neg \exists k(k \in \mathbb{Z} \wedge n = 3k)$

$\forall k \neg(k \in \mathbb{Z} \wedge n = 3k)$

$\forall k(\neg k \in \mathbb{Z} \vee \neg(n = 3k))$

$\forall k(\neg k \in \mathbb{Z} \vee (n \neq 3k))$

$\forall k(k \in \mathbb{Z} \rightarrow n \neq 3k)$

També: $\forall k(n \neq 3k)$

Exemple 3. Escriviu fórmules de predicat corresponents a l'afirmació: "El producte de dos enters senars qualssevol és senar". Escollim les dues variables enteres a, b de les quals parla l'enunciat. Escrivim:

"Si a i b són senars, aleshores ab és senar" mitjançant una fórmula en la qual entenem que $a, b \in \mathbb{Z}$, fórmula que és un condicional:

$(2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab$.

Ara hem d'expressar el "qualssevol", quantificant:

$\forall a \forall b(2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$.

Si es volgués una fórmula autocontinguda,

$\forall a \forall b(a \in \mathbb{Z} \wedge a \in \mathbb{Z} \wedge 2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$.

O, fora de la sintaxi estàndard, $\forall a \in \mathbb{Z} \forall b \in \mathbb{Z}((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$.

Exemple 4. En cada tres nombres enters consecutius, n'hi ha algun que és múltiple de 3. O bé, si tenim tres nombres enters consecutius qualssevol, aleshores algun d'ells és múltiple de 3. Suposant l'universal $\Omega = \mathbb{Z}$, al qual pertanyen totes les variables de la fórmula, i de l'enunciat, podem escriure:

$\forall n(3|n \vee 3|(n+1) \vee 3|(n+2))$.

Exemple 5. L'exemple del principi del capítol:

$\forall x \exists y \forall z(P(x,y,z) \rightarrow (\neg R(x,z) \rightarrow \exists w(\neg S(w))))$

És un exemple abstracte, formal, sense especificar què són les variables ni els predicats.

Les variables són x, y, z, w, que se suposa que pertanyen a universals (pot ser més d'un) que no s'especifiquen.

Tenim quantificadors exteriors ($\forall x \exists y \forall z$) i una quantificació interior ($\exists w$).

P, R, S són predicats (lletres).

La fórmula $P(x,y,z) \rightarrow (\neg R(x,z) \rightarrow \exists w(\neg S(w)))$, subfórmula de la total, és un condicional, d'antecedent $P(x,y,z)$ i conseqüent $\neg R(x,z) \rightarrow \exists w(\neg S(w))$.

Aquesta última fórmula també és un condicional, d'antecedent $\neg R(x,z)$ i conseqüent $\exists w(\neg S(w))$. ■

Això dóna lloc a un llenguatge molt potent per a expressar propietats i coneixement, per a donar precisió a les afirmacions i eliminar-ne les ambigüitats. És molt especialitzat, però pot donar cabuda a una gran quantitat de fórmules, expressar una gran quantitat d'enunciats.

Com es construeix una fórmula de predicat correcte, "ben formada"? S'ha de donar una **gramàtica** per a generar les fórmules, del tipus de la de les fórmules de proposicions, però amb més ingredients:

- lletres de variables
- lletres de constants
- funcions per a fórmules
- parèntesis
- connectives
- lletres de predicats (i predicats especials: $=, <, >, \leq, \geq$ ...)
- regles de formació
- regles de quantificació
- descripció de les subfórmules.

Tot això es descriu a la secció posterior del capítol sobre gramàtica (secció 5.4).

Una fórmula és una cadena de caràcters, però no qualsevol cadena de caràcters és una fórmula. Intuïtivament, una cadena de caràcters és una "fórmula", una "fórmula ben formada", si la podem llegir, entendre, interpretar; com a mínim, llegir. Formalment, ha d'estar generada per les regles de generació. Vegeu secció 5.4 (gramàtica).

Què ens aporta el llenguatge de predicats?

- Permet escriure enunciats explicitant-ne tots els components, cosa que no permet el llenguatge de proposicions, i aspectes que en el llenguatge de proposicions no es poden destriar (variable, per exemple).
- Permet la formalització completa i l'alliberament complet del llenguatge natural.
- Permet expressar un enunciat amb tota precisió i eliminar tota ambigüitat. Fins i tot en els llibres de text es veuen molts enunciats força negligents, que podrien ser mal interpretats si no fos perquè, de vegades, el propi text els explica o bé el lector els llegeix i interpreta amb els seus coneixements. Un cas clar és la definició de límit (d'una successió, per exemple), que moltes vegades podem veure escrita com:

  $$\forall\epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N} (n > n_0 \to |a_n - L| < \epsilon)$$

  De vegades, fins i tot es presenta com:

  $$\forall\epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N} \qquad n > n_0 \to |a_n - L| < \epsilon$$

  Ambdues són manifestament millorables.

- Possibilita el tractament automàtic del coneixement, per exemple, per part de programes que puguin llegir les fórmules i, a partir d'aquest moment, "saber" (per exemple, què és "ser primer" o què és "ser senar"):

Exemple 5.19 Certament per a un programa pot ser més fàcil llegir la descripció següent de n senar (exemple senzill):

$\exists k(k \in \mathbb{Z} \wedge n = 2k+1)$ (100% formalitzat)

que no la versió conceptual semiformalitzada, amb part de llenguatge natural:

"Existeix un nombre enter k tal que $n = 2k+1$" ■

- Permet expressar, de forma unívoca, coneixement (definicions, propietats, resultats), lluny del llenguatge natural. Les fórmules són una formalització completa (0% llenguatge natural), segueixen un estàndard sintàctic i, per aquest motiu, poden ser llegides per un programa que incorpori les regles de formació. Una fórmula de predicats es pot pensar com una manera d'empaquetar coneixement de forma estandarditzada. Pot imaginar el lector una immensa base de dades formada per predicats i fórmules de predicat que descriguin àrees de coneixement (matemàtic, per exemple) i que pugui ser tractada amb programes automàtics, per exemple d'intel·ligència artificial?
- Permet negar, de manera automàtica i segura, enunciats complexos. De vegades, s'ha de formalitzar completament l'enunciat, efectuar la negació i, si es vol, desformalitzar. Per exemple, en el cas de la definició de límit que es troba en molts de llibres de text:

  $\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}(n > n_0 \to |a_n - L| < \epsilon)$

  Resultaria problemàtic negar en aquest format. Cal redreçar la fórmula a format estàndard per a poder escriure la negació amb seguretat i sense problemes. Aquest exercici està resolt posteriorment.

Fórmules (de predicat) en comptes de lletres de predicat

Moltes vegades, preferim utilitzar fórmules de predicat explícites en substitució de les lletres de predicat, que s'han de definir externament.

Així, podem considerar el predicat "ser senar", que expressem amb la lletra S, amb $S(n)$ (si n és un nombre enter), indicant "n és un nombre enter senar". Podem expressar-ho així o substituint $S(n)$ per una propietat més explícita, concretament $2 \nmid n$:

n és senar $\to n^2$ és senar

$S(n) \to S(n^2)$

$2 \nmid n \to 2 \nmid n^2$

També podria ser:

$(\exists k(k \in \mathbb{Z} \wedge n = 2k+1)) \to (\exists k'(k' \in \mathbb{Z} \wedge n = 2k'+1))$

No sempre és convenient fer-ho, ja que amb una lletra de predicat podem expressar fórmules complexes que, si es despleguessin completament en una fórmula final, n'enfosquirien el significat i en dificultarien la lectura.

Per exemple, si volem escriure, per a enters, que "si un nombre primer divideix un producte de dos factors, llavors divideix algun dels factors", és més clar escriure:

$(p|ab \wedge p \text{ primer }) \rightarrow (p|a \vee p|b)$

que escriure el resultat de substituir "p primer" per una fórmula que defineixi "ser primer" (tot enters):

p és primer si, i només si, $p \geq 2 \wedge \forall d((d|p \wedge d > 0) \rightarrow (d = p \vee d = 1))$,

és a dir:

$(p|ab \wedge (p \geq 2 \wedge \forall d((d|p \wedge d > 0) \rightarrow (d = p \vee d = 1)))) \rightarrow (p|a \vee p|b)$

Dependrà de cada circumstància mantenir un equilibri sobre el nivell de detall.

Interpretacions

L'univers del discurs és fonamental. Explicitant-lo interpretem les variables (el significat de les variables, què signifiquen, i ja entrem en el terreny semàntic). També cal dir què són els predicats que hi apareixen, conceptualment o mitjançant una altra fórmula de predicats més senzilla.

La gramàtica de formació de les fórmules de predicat ens permet escriure fórmules molt generals i variades, en un pur exercici sintàctic, i així ens podem trobar amb fórmules de predicat molt abstractes, molt generals, com per exemple:

$\forall x \exists y \forall z((P(x,y) \wedge Q(x,t)) \rightarrow \forall t(\neg(R(x) \rightarrow \neg S(z,t)))$

o, altres amb menys complicació d'estructura:

$\forall x \forall y(P(x,y) = P(y,x))$

Per a saber si aquesta fórmula és certa o no, cal fer una **interpretació** de P i de les variables, és a dir, del seu domini U, "dir què són". El tema de les interpretacions en general, que tenen a veure amb la semàntica (el significat), és molt més complex i no el tractem aquí (vegeu [BENA93]). Només considerem aquest exemple particular, per fer-ne veure la idea.

Tornant a l'última fórmula anterior, si P representa una operació producte en U, és a dir, $P(x,y) = x * y$, aleshores la fórmula anterior es concreta en

$\forall x \forall y(x * y = y * x)$,

que afirma que l'operació és commutativa (de fet, no cal ni pensar que és producte; és simplement: $*$).

Cert o fals? Depèn.

Si $U = \mathbb{R}$, i interpretem l'operació $*$ com el producte ordinari en els reals, aleshores és certa. Simplement afirmem que el producte de nombres reals és commutatiu.

Si U és el conjunt de les matrius quadrades d'ordre n, i interpretem l'operació $*$ com el producte ordinari matricial, aleshores és falsa, ja que l'enunciat "el producte de matrius quadrades és commutatiu" és fals. És suficient *aportar un contraexemple*, per exemple, en el cas de matrius 2×2:

Exemple 5.20 Siguin $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$

És $AB = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$, $BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ i, per tant, $AB \neq BA$.

Amb les fórmules de predicats en tindrem prou per a expressar molts dels enunciats que ens puguin interessar. Malgrat l'especialització i l'aparent estretesa, és un llenguatge molt potent, suficient per a expressar grans quantitats de resultats i de propietats (teoremes, "ser primer", "ser compost", ...).

Normalment, escriurem fórmules que tinguin un significat (i interès!) per a nosaltres. En altres àmbits, pot interessar considerar només l'aspecte formal i general (programació lògica, Prolog, intel·ligència artificial o lògica formal), però això ja depassa els nostres objectius.

Un altre aspecte, lligat a aquesta possibilitat d'escriure fórmules molt generals, és que molts enunciats tenen la mateixa estructura, i són casos particulars d'una fórmula general. Vegem-ho amb alguns exemples:

Exemple 5.21 Amb $U = \mathbb{Z}$, $n \in \mathbb{Z}$:

$$\forall n(P(n) \to (Q(n) \wedge R(n)))$$

$$\forall n(15|n \to (3|n \wedge 5|n)),\ (P(n) = (15|n), Q(n) = (3|n), R(n) = (5|n)\ )$$
$$\forall n(21|n \to (7|n \wedge 3|n)),\ (P(n) = (21|n), Q(n) = (7|n), R(n) = (3|n)\ ).$$

Predicats *n*–aris

Fins aquí només els predicats més freqüents han estat d'una variable. Són els predicats 1–aris. Tot i que en algun exemple hem vist predicats de més d'una variable, no hem ressaltat el fet.
També podem considerar predicats de més variables i tenir així els predicats n–aris, per a $n \geq 1$. Els predicats 2–aris són els predicats binaris. En general, escriurem $Q(x_1, \ldots, x_n)$, fórmula general per a un predicat n–ari.

Exemple 5.22

$P(x,y) = x^2 + y^2 \geq 2$, $x \in U = \mathbb{R}$, $y \in U = \mathbb{R}$

$R(x,y) = (x > y)$, $x \in U = \mathbb{R}$, $y \in U = \mathbb{R}$

$S(x,y) =$"x és fill de y", on U pot ser la col·lecció d'humans d'una ciutat, o els animals d'un zoològic.

$T(x,y) =$"x és més alt que y", on U pot ser la col·lecció d'humans d'una classe, o els animals d'un zoològic.

$W(x,y,z) =$"$(x-y+2z \geq 4)$", on $x,y,z \in U = \mathbb{R}$. ■

En el cas que $n \geq 2$, aleshores els predicats ens permeten expressar **relacions** entre objecte, les variables. El tractament de les relacions es veurà més endavant.

Alguns dels més útils (binaris) ja s'escriuran directament a les fórmules, com la igualtat, desigualtats diverses, i altres. Així, en comptes d'escriure $I(x,y)$, en què $I(x,y) = (x = y)$, ja escriurem directament $x = y$. Anàlogament amb $x < y$, $x \leq y$, $x > y$, $x \geq y$. Els podem incorporar com a predicats destacats del llenguatge (llenguatge amb igualtat, per exemple).

De fet, incorporem tot el que calgui per a poder escriure totes les fórmules de matemàtiques (això inclou, a més, tots els símbols, constants, com dígits, π, e, totes les funcions). Especialitzar amb això voldria dir considerar subllenguatges (variants del llenguatge; també triant conjunts diversos de connectives).

No hi ha una única manera d'escriure les coses. Considerem l'exemple que ja hem vist anteriorment:

Exemple 5.23 Amb $U = \mathbb{Z}$, $n \in \mathbb{Z}$:

$\forall n(15|n \to (3|n \wedge 5|n)), (P(n) = (15|n), Q(n) = (3|n), R(n) = (5|n)\ )$

$\forall n(21|n \to (7|n \wedge 3|n)), (P(n) = (21|n), Q(n) = (7|n), R(n) = (3|n)\ ).$

Es poden considerar altres predicats, com per exemple el predicat 2–ari:

$D(a,b) = (a|b)$ " a divideix b" (cal precisar d'on són les variables).

Amb aquest podríem escriure les anteriors fórmules com:

$\forall n(D(15,n) \to (D(3,n) \wedge D(5,n))),$

$\forall n(D(21,n) \to (D(7,n) \wedge D(3,n))\ ).$ ■

O considerar predicats que, de fet, es poden expressar com a negació d'altres: per exemple, "ser senar" es pot considerar com a $\neg$ "ser parell" o "ser compost" com a negació de "ser nombre primer".

5.4. Gramàtica: llenguatge de predicats

En aquesta secció descrivim formalment el llenguatge de les fórmules de predicats.

Fórmules ben formades (informal). Les fórmules de predicats següents semblen estar ben formades:

$\forall n(2|n \leftrightarrow 2|n^3)$

$\forall n(n \in \mathbb{Z} \to (2 \nmid n^2 \to 2 \nmid n))$

$\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2 \nmid a \wedge 2 \nmid b) \to 2 \nmid ab)$

Per què? Intuïtivament, perquè les podem llegir (i fins i tot interpretar i entendre). Com a mínim, llegir-les. Després veurem que es poden generar/formar/obtenir per les regles de generació del llenguatge de predicats.

En canvi:

$))\forall)\exists(()\vee \rightarrow (x+y=z)\neg\wedge$

no sembla una fórmula ben formada. No la podem llegir. Després veurem que no es pot generar per l'aplicació de cap de les regles que defineixen el llenguatge de predicats i que ens diuen quines són les fórmules correctes des del punt de vista lèxic i sintàctic, és a dir, des del punt de vista del llenguatge o la gramàtica. Una fórmula no pot començar (esquerra) per parèntesi de tancament (cap regla ho genera). Un parèntesi de tancament sempre ha d'estar precedit per l'esquerra per un parèntesi d'obertura; un parèntesis obrint sempre ha de ser seguit a la dreta per algun parèntesi tancant.

Equilibrament de parèntesis. Una regla bàsica que no s'especifica explícitament a la gramàtica és que els parèntesis en una fórmula han d'estar equilibrats: "tot parèntesi que s'obre, s'ha de tancar". Amb independència de si els parèntesis estan ben escrits, en els llocs que cal, s'ha de complir que el nombre de parèntesis que obren "(" ha de ser igual al nombre de parèntesis que tanquen ")" ; en cas contrari, la fórmula és incorrecta. No s'explicita, però deriva clarament de les regles de formació que veurem; en resulta implícita.

Exemple 5.24 L'exemple gràfic del principi del capítol és:

$\forall x \exists y \forall z((P(x,y,z) \rightarrow (\neg R(x,z) \rightarrow \exists w(\neg S(w))))$

Nombre de parèntesis "(": 7

Nombre de parèntesis ")": 6

Conclusió: la fórmula és incorrecta.

Error: $\forall x \exists y \forall z(\; (\; P(x,y,z) \rightarrow (\neg R(x,z) \rightarrow \exists w(\neg S(w))))$.

Correcció: $\forall x \exists y \forall z(P(x,y,z) \rightarrow (\neg R(x,z) \rightarrow \exists w(\neg S(w))))$. ■

Volem poder dir, doncs, quan una fórmula de predicats està ben construïda. Disposar de les regles de generació també pot ser útil per a programes analitzadors de fórmules d'aquest tipus (*parsers*) o generadors de fórmules.

5.4.1. Les fórmules del llenguatge de predicats

Definim el **lèxic** i la **sintaxi**. No tractem qüestions de semàntica (significació).

L'alfabet. Format per:

– Parèntesis (,), comes i altres possibles signes de puntuació; opcionalment, espais en blanc, però només per a millorar-ne la legibilitat (humana).

- Les variables: $x, y, z, \ldots, x_1, x_2, x_3, \ldots$, eventualment amb subíndexs (hi ha provisió infinita).
- Les constants: $a, b, a_1, a_2, \ldots, 0, 1, 2, \pi$, s (per “Sòcrates”), ... (hi ha provisió infinita).
- Les funcions admeses, $f_1, f_2, \ldots$, que poden variar depenent del que es vulgui poder expressar (per exemple, operacions): $f(x,y) = x + y$, $g(x) = e^x$, $h(x) = x^2$, la funció “següent” $s(n) = n + 1$, integrals i moltes altres. S’inclouen aquí les funcions i/o els símbols que utilitzen: $+, -, *, \ldots$. Tenen, com a mínim, un argument. Es podria donar més precisió notacional amb f_i^j, indicatiu d’una i-èsima funció de j arguments.
- Les lletres indicatives de predicats, de diverses aritats (nombre de variables, en notació funcional; com a mínim, un argument); s’inclou la igualtat $=$. Serien: $A, B, \ldots, P, Q, R, S, T, U, V, W, P_1, \ldots$ (amb subíndexs, tenim provisió infinita). Per exemple, $I(x,y) = (x = y)$ (“x és igual a y”), o $M(x,y) = (x < y)$. En alguns casos, es podrà escriure a les fórmules finals $x = y$, en comptes de $I(x,y)$ (o similars). $(x + y = 4)$ s’obtindrà formalment com $I(f(x,y), 4)$, fórmula en què apareixen parèntesis, constants, variables, funcions i predicats. Així podem expressar relacions, amb predicats 2-aris. Es podria donar més precisió notacional amb P_i^a, on a és l’aritat.
- Les connectives lògiques: $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ (joc estàndard). N’hi pot haver menys o més, i així tindríem més variants possibles de llenguatges.
- Els símbols de quantificació: $\forall, \exists$. Amb un dels dos n’hi hauria prou, i així tindríem una altra variant de llenguatge, però les fórmules serien de lectura (humana) més difícil. També s’hi podria incorporar un tercer quantificador: “existeix i és únic”, que en alguns textos es representa com $\exists! x$; aquí no l’incorporem.

Els termes. Són expressions, cadenes de caràcters sobre l’alfabet, d’acord amb les regles:

- Variables i constants són termes.
- Si f és una funció de n arguments i $t_1, \ldots, t_n$ són termes, aleshores $f(t_1, \ldots, t_n)$ és un terme.
- Els termes són les expressions que es poden obtenir per aplicació de les regles anteriors, un nombre finit de vegades.

Exemple 5.25

x, y, x_3, (variables)

a, $a_1, a_2, \ldots$, b_3, (constants).

La distinció notacional entre constants i variables és relativa: depèn del paper que juguen en una fórmula. Per exemple, s pot semblar una variable, però si és $s =$“Sòcrates”, aleshores està actuant com a constant.

1, 0, (constants)

$x + y$, $2x + y - 1$, $x^2 - y^2$, $\sin(xy)$, $x + \cos(y^2))$,

$f_1(t_1, t_2, f_2(a_1, t_2, t_3, f_3(t_4, 25)), a_2)$.

Per exemple, si $f(x,y) = x + y$, $g(x,y) = xy$, $h(t) = t^2$, aleshores l’expressió aritmètica $(x + y)^2 + xy$ és $f(h(f(x,y)), g(x,y))$. ■

La sintaxi dels termes està controlada per les funcions, que se suposa que són "correctes". En concret, depèn del tipus d'expressions que es considerin. Per exemple, si es consideren fórmules aritmètiques, l'estructura dels termes és dictada per la *gramàtica corresponent*. Per exemple, amb les variables x,y,z, són fórmules correctes $(x+(y+x))$, $((x+y)+x)$. Ambdues són termes. No ho serien, per exemple, $(a+b$, $)a+b$, $)(a+b$, $a(+b$, en comptes de $(a+b)$. Naturalment, una fórmula com $(x+y$ podria ser correcta si convenim que les fórmules només s'escriuran amb parèntesi esquerre. A cada tipus de fórmula, s'ha d'especificar la gramàtica corresponent.

Les fórmules de predicat. **a) Les fórmules atòmiques**. Són les que es formen a partir dels termes i les lletres de predicat. L'estructura és $P(t_1,\ldots,t_n)$, on P és una lletra de predicat n-ària.

Exemple 5.26

$(x+3=y)$ és $P(x+3,y)$, on $P(z,t) := (z=t)$, i s'aplica als termes t_1,t_2, on $t_1 = x+3 = s(x,3)$, on $s(u,v) = u+v$ és la funció suma, i $t_2 = y$. Altres exemples: $(x-y > z-1)$, $x^2+y^2 = z$. ■

Són les fórmules més senzilles, indescomponibles, sense connectives lògiques ni quantificadors.

Exemple 5.27 Són fórmules atòmiques: $P(x,y)$, $N(t)$, $Q(x,y,z)$, $(x<y)$, $(x-y<z)$, $(x^2=y^2)$, $2|a$.
No són atòmiques: $\neg(x=y)$ (conté connectives), $\exists x(x>0)$ (conté quantificadors), $2|a \vee 2\nmid a$ (conté connectives).

No és atòmica: $\forall x \exists y((P(x,y)\wedge\neg Q(x,y)) \to \neg R(x,y))$ (conté quantificadors i connectives). ■

b) Les fórmules no atòmiques. A partir de les fórmules atòmiques, es formen les altres mitjançant connectives lògiques i quantificadors.

c) Regles de generació de les fórmules o fórmules "ben formades" (redundant ja que, si no són ben formades, ja no són fórmules).

Les fórmules (ben formades) són les que es generen per l'aplicació d'un nombre **finit** de vegades de les regles següents.

P1: Les fórmules atòmiques són fórmules.

P2: Si F és una fórmula, també ho és $\neg F$.

P3a: Si F,G són fórmules, també ho és $(F\wedge G)$.

P3b: Si F,G són fórmules, també ho és $(F\vee G)$.

P3c: Si F,G són fórmules, també ho és $(F\to G)$.

P3d: Si F,G són fórmules, també ho és $(F\leftrightarrow G)$.

P4a: Si F és una fórmula, també ho és $\forall xF$, per a qualsevol variable x (no cal que F contingui la variable x).

P4b: Si F és una fórmula, també ho és $\exists xF$, per a qualsevol variable x (no cal que F contingui la variable x).

S'eliminaran parèntesis sempre que no s'hi introdueixi ambigüitat; sobretot es farà els parèntesis exteriors a la fórmula definitiva.

Vegem l'ús d'aquestes regles en uns casos senzills.

Exemple 5.28 Una nofórmula.

Estudieu si és una fórmula: $))\forall)\exists(()\vee \rightarrow (x+y=z)\neg\wedge$.

La cadena de caràcters de l'alfabet $))\forall)\exists(()\vee \rightarrow (x+y=z)\neg\wedge$ no és una fórmula (ben formada). Per exemple, no hi ha cap regla que generi)…. ■

Exemple 5.29 Indiqueu si $)\forall\exists\neg)xP(\neg x,y)$ és una fórmula de predicats.

No, no correspon a les regles de generació, de bona formació, de fórmules de predicats. ■

Vegem ara quina fórmula es genera per l'aplicació d'una seqüència de regles.

Exemple 5.30 Donem una seqüència ordenada d'aplicacions de les regles i veiem quina fórmula es genera.

Partim de les variables x,y,z i de les lletres de predicat P,Q,R, corresponents a predicats binaris (2–aris).

1. Apliquem la regla P1 per a generar les fórmules $P(x,y)$, $Q(y,z)$, $R(x,z)$.
2. Apliquem la regla P2 a $P(x,y)$ per a produir $\neg P(x,y)$.
3. Apliquem la regla P4a a $Q(y,z)$ per a produir $\forall zQ(y,z)$.
4. Apliquem la regla P4b a $R(x,z)$ per a produir $\exists xR(x,z)$.
5. Apliquem la regla P3b a $\neg P(x,y)$ i a $\forall zQ(y,z)$ per a produir $(\neg P(x,y) \vee \forall zQ(y,z))$.
6. Apliquem la regla P3c a $(\neg P(x,y) \vee \forall zQ(y,z))$ i a $\exists xR(x,z)$ per a produir $((\neg P(x,y) \vee \forall zQ(y,z)) \rightarrow \exists xR(x,z))$.
7. Apliquem la regla P4a a $((\neg P(x,y) \vee \forall zQ(y,z)) \rightarrow \exists xR(x,z))$ per a produir $\forall y((\neg P(x,y) \vee \forall zQ(y,z)) \rightarrow \exists xR(x,z))$.
8. Apliquem la regla P4b a $\forall y((\neg P(x,y) \vee \forall zQ(y,z)) \rightarrow \exists xR(x,z))$ per a produir $\exists x\forall y((\neg P(x,y) \vee \forall zQ(y,z)) \rightarrow \exists xR(x,z))$.
9. Apliquem la regla P2 a $\exists x\forall y((\neg P(x,y) \vee \forall zQ(y,z)) \rightarrow \exists xR(x,z))$ per a produir $\neg\exists x\forall y((\neg P(x,y) \vee \forall zQ(y,z)) \rightarrow \exists xR(x,z))$.

Quina és la fórmula generada?

$\neg\exists x\forall y((\neg P(x,y)\vee\forall zQ(y,z))\rightarrow\exists xR(x,z))$. ■

Exemple 5.31 Una altra versió expositiva, per a la mateixa fórmula anterior:

1. Apliquem la regla P1 per a generar les fórmules $P(x,y)$, $Q(y,z)$, $R(x,z)$.
2. Apliquem la regla P2 a $P(x,y)$ per a produir la fórmula F_1.
3. Apliquem la regla P4a a $Q(y,z)$ per a produir F_2.
4. Apliquem la regla P4b a $R(x,z)$ per a produir F_3.
5. Apliquem la regla P3b a F_1 i a F_2 per a produir F_4.
6. Apliquem la regla P3c a F_4 i a F_3 per a produir F_5.
7. Apliquem la regla P4a a F_5 per a produir F_6.
8. Apliquem la regla P4b a F_6 per a produir F_7.
9. Apliquem la regla P2 a F_7 per a produir F_8.

Quina és la fórmula final generada?

$\neg\exists x\forall y((\neg P(x,y)\vee\forall zQ(y,z))\rightarrow\exists xR(x,z))$.

Vegem per què seguint els resultats de cada acció anterior d'aplicació de les regles:

$F1=\neg P(x,y)$ (traiem parèntesi exterior).
$F2=\forall zQ(y,z)$ (traiem parèntesi exterior).
$F3=\exists xR(x,z)$ (traiem parèntesi exterior).
$F4=(F1\vee F2)=(\neg P(x,y)\vee\forall zQ(y,z))$ (traiem parèntesi exterior).
$F5=(F4\rightarrow F3)=((\neg P(x,y)\vee\forall zQ(y,z))\rightarrow\exists xR(x,z))$ (traiem parèntesi exterior).
$F6=\forall yF5=\forall y((\neg P(x,y)\vee\forall zQ(y,z))\rightarrow\exists xR(x,z))$ (traiem parèntesi exterior).
$F7=\exists xF6=\exists x\forall y((\neg P(x,y)\vee\forall zQ(y,z))\rightarrow\exists xR(x,z))$ (traiem parèntesi exterior).
$F8=\neg F7=\neg\exists x\forall y((\neg P(x,y)\vee\forall zQ(y,z))\rightarrow\exists xR(x,z))$ (traiem parèntesi exterior) (fórmula final).

El que segueix és interessant en relació amb el que veurem sobre *subfórmules*. Quines són les fórmules generades en el procés? La subfórmula final és la fórmula total.

Llista de les subfórmules:

$P(x,y)$, $Q(y,z)$, $R(x,z)$
$\neg P(x,y)$
$\forall zQ(y,z)$
$\exists xR(x,z)$
$(\neg P(x,y)\vee\forall zQ(y,z))$

$((\neg P(x,y) \vee \forall z Q(y,z)) \rightarrow \exists x R(x,z))$
$\forall y((\neg P(x,y) \vee \forall z Q(y,z)) \rightarrow \exists x R(x,z))$
$\exists x \forall y((\neg P(x,y) \vee \forall z Q(y,z)) \rightarrow \exists x R(x,z))$
$\neg \exists x \forall y((\neg P(x,y) \vee \forall z Q(y,z)) \rightarrow \exists x R(x,z))$. ■

Donada una fórmula (correcta), vegem com es pot generar per una seqüència d'aplicació de les regles.

Exemple 5.32 Anem a veure com es genera la fórmula de predicats:

$\forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$

per aplicació de les regles del llenguatge.

Nivell preliminar (els "termes"): Les variables, constants i (possible) aplicació de funcions a les variables.

Les variables són: x, y. No hi ha constants. No s'apliquen funcions (llevat que es consideri la identitat).

Els predicats. Els predicats no estan definits explícitament. Només tenim les lletres de predicat P, Q, R, tots binaris, amb dues variables/arguments.

Fórmules:

Fórmules atòmiques: $P(x,y)$, $Q(x,y)$, $R(x,y)$ (no hi ha connectives ni quantificadors). Per tant:

► Regla P1: $P(x,y)$, $Q(x,y)$, $R(x,y)$ són fórmules, per ser fórmules atòmiques.
Llista de fórmules generades després de l'aplicació de la regla: $P(x,y)$, $Q(x,y)$, $R(x,y)$.

Fórmules no atòmiques (amb quantificadors i/0 connectives):

► Regla P2: Apliquem la regla P2 per a generar la fórmula $\neg Q(x,y)$ a partir de la fórmula prèviament obtinguda $Q(x,y)$.
Llista de fórmules generades fins al moment després de l'aplicació de la regla: $P(x,y)$, $Q(x,y)$, $R(x,y)$, $\neg Q(x,y)$.

► Regla P2: Apliquem la regla P2 per a generar la fórmula $\neg R(x,y)$ a partir de la fórmula prèviament obtinguda $R(x,y)$.

Llista de fórmules generades fins al moment després de l'aplicació de la regla: $P(x,y)$, $Q(x,y)$, $R(x,y)$, $\neg Q(x,y)$, $\neg R(x,y)$.

► Regla P3a: Apliquem la regla P3a per a generar la fórmula $(P(x,y) \wedge \neg Q(x,y))$ a partir de les fórmules prèviament obtingudes $P(x,y)$ i $\neg Q(x,y))$, en aquest ordre.

Llista de fórmules generades fins al moment després de l'aplicació de la regla: $P(x,y)$, $Q(x,y)$, $R(x,y)$, $\neg Q(x,y)$, $\neg R(x,y)$, $(P(x,y) \wedge \neg Q(x,y))$.

▶ Regla P3c: Apliquem la regla P3c per a generar la fórmula $((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$ a partir de les fórmules prèviament obtingudes $(P(x,y) \wedge \neg Q(x,y))$ i $\neg R(x,y))$, en aquest ordre.

Llista de fórmules generades fins al moment després de l'aplicació de la regla: $P(x,y)$, $Q(x,y)$, $R(x,y)$, $\neg Q(x,y)$, $\neg R(x,y)$, $(P(x,y) \wedge \neg Q(x,y))$,

$((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$.

▶ Regla P4b: Apliquem la regla P4b per a generar la fórmula $\exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$ a partir de la fórmula prèviament obtinguda $((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$.

Llista de fórmules generades fins al moment després de l'aplicació de la regla: $P(x,y)$, $Q(x,y)$, $R(x,y)$, $\neg Q(x,y)$, $\neg R(x,y)$, $(P(x,y) \wedge \neg Q(x,y))$,

$((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$, $\exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$.

▶ Regla P4a: Apliquem la regla P4a per a generar la fórmula (final) $\forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$ a partir de la fórmula prèviament obtinguda $\exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$.

Llista de fórmules generades fins al moment després de l'aplicació de la regla: $P(x,y)$, $Q(x,y)$, $R(x,y)$, $\neg Q(x,y)$, $\neg R(x,y)$, $(P(x,y) \wedge \neg Q(x,y))$,

$((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$, $\exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$,

$\forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$.

Encara que es veu més endavant, la llista de fórmules generades en el procés constructiu és la col·lecció de les *subfórmules* de la fórmula:

$P(x,y)$, $Q(x,y)$, $R(x,y)$, (apliquem P1)

$\neg Q(x,y)$, $\neg R(x,y)$, (apliquem P2)

$(P(x,y) \wedge \neg Q(x,y))$, (apliquem P3a)

$((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$, (apliquem P3c)

$\exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$, (apliquem P4b)

$\forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$ (apliquem P4a). ■

L'exemple anterior correspon a uns predicats genèrics.

Exemple 5.33 Vegem una fórmula concreta, la traducció de l'enunciat: "el producte de dos nombres enters senars qualssevol és un nombre senar" (que són enters es diu fora de la fórmula).

$\forall a \forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$

Variables: a, b

Constants: 2

Termes: ab (es pot escriure com a resultat d'aplicar la funció producte $f(x,y) = xy$ a les variables a,b; $ab = f(a,b)$).

Predicats (expressats com a fórmula, corresponents a "no ser divisible per 2").

Observació: també es podria fer servir $D(z,t) = (z|t)$, o la negació $N(z,t) = z \nmid t$.

Regla P1. Fórmules atòmiques: $2 \nmid a$, $2 \nmid b$, $2 \nmid ab$.

Regla P3b aplicada a $2 \nmid a$, $2 \nmid b$ per a formar $(2 \nmid a \wedge 2 \nmid b)$.

Regla P3c aplicada a $(2 \nmid a \wedge 2 \nmid b)$ i $2 \nmid ab$ per a formar $((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$.

Regla P4a aplicada a $((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$ per a formar
$\forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$.

Regla P4a aplicada a $\forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$ per a formar

$\forall a \forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$.

Llista de les fórmules generades (subfórmules):

$2 \nmid a$, $2 \nmid b$, $2 \nmid ab$

$(2 \nmid a \wedge 2 \nmid b)$

$((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$ $\forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$

$\forall a \forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$

Observació: L'aplicació de les últimes regles és intercanviable, ja que, en fer-ho, es generaria una fórmula equivalent a l'anterior:

$\forall b \forall a((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$. ■

5.4.2. Subfórmules d'una fórmula del llenguatge de predicats

Informal

Donada la fórmula de predicats:

$\forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$

una subfórmula n'és una subcadena (subcadena de caràcters). Ara bé, no sembla que les subcadenes

$(P(x,y) \wedge \neg Q(x$

$\forall x \exists y($

$\rightarrow \neg R(x,y))$

siguin subfórmules. No es poden generar per cap regla de la gramàtica.

En canvi, semblen ser-ho (les podem llegir):

$(P(x,y) \wedge \neg Q(x,y))$

$\neg R(x,y)$

$\exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$

Es poden generar per les regles de la gramàtica.

La idea és que una subfórmula és una subcadena (que pot ser la total) tal que ella mateixa és una fórmula (segons les regles sintàctiques). Són subcadenes que són fórmules. Són les subcadenes que es generen amb les regles de generació de les fórmules, o que s'han generat en algun pas de la generació de la fórmula total per les regles.

Regles descriptives de les subfórmules

Les subfórmules són les fórmules que apareixen en el procés de generació de la fórmula per aplicació de les regles de generació anteriors. Són subcadenes de la fórmula que, al seu torn, són fórmules segons la definició donada per la gramàtica. Intuïtivament, són subcadenes que podem llegir. La definició precisa és inductiva o recursiva, paral·lelitzant la definició de fórmula segons la gramàtica.

C1: Si F és una fórmula atòmica, l'única subfórmula és F.

C2: Si $F = \neg G$, les subfórmules de F són F i les subfórmules de G.

C3a: Si $F = (G \wedge H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.

C3b: Si $F = (G \vee H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.

C3c: Si $F = (G \rightarrow H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.

C3d: Si $F = (G \leftrightarrow H)$, aleshores les subfórmules de F són: F, les subfórmules de G, les subfórmules de H.

C4a: Si $F = \forall x G$, aleshores les subfórmules de F són F i les subfórmules de G.

C4b: Si $F = \exists x G$, aleshores les subfórmules de F són F i les subfórmules de G.

Exemple 5.34 Obtenció sistematitzada de les subfórmules de la fórmula F següent.

$$F = \forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$$

És força intuïtiu la manera de procedir per obtenir les subfórmules. Vegem com s'obtenen com a resultat de les regles anteriors.

S'ha d'identificar l'estructura de la fórmula i de les subfórmules que vagin apareixent per tal d'aplicar-hi la regla apropiada.

És F atòmica? No. No s'aplica la C1.

És $F = \neg G$? No. No s'aplica la regla C2.

...

La primera regla aplicable és C4a, de manera que les subfórmules de F són:

F i les subfórmules de F_1, essent $F = \forall x F_1$, amb

$F_1 = \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$. Per tant, són subfórmules:

- $\forall x \exists y((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$,
- les subfórmules de $\exists y((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$ (F_1).

Estudiem les subfórmules de F_1. És aplicable la regla C4b, amb $F_1 = \exists x F_2$, amb $F_2 = ((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$. Les subfórmules de F_1 són F_1 i les subfórmules de F_2. Per tant, són subfórmules:

- $\exists y((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$,
- les subfórmules de $((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$ (F_2).

Estudiem les subfórmules de F_2. És aplicable la regla C3c, amb $F_2 = F_3 \to F_4$, on $F_3 = (P(x,y) \land \neg Q(x,y))$, $F_4 = \neg R(x,y)$, amb

$F_2 = ((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$. Les subfórmules de F_2 són F_2, més les subfórmules de F_3 i les subfórmules de F_4. Per tant, són subfórmules:

- $((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$,
- les subfórmules de $((P(x,y) \land \neg Q(x,y))$ (F_3),
- les subfórmules de $\neg R(x,y))$ (F_4).

Estudiem separadament les subfórmules de F_3 i les de F_4:

- Subfórmules de F_3, on $F_3 = (P(x,y) \land \neg Q(x,y))$. Atès que és una conjunció, $F_3 = (F_5 \land F_6)$, s'aplica la regla C3a i resulta que les subfórmules de F_3 són:
  - F_3,
  - Les subfórmules de $F_5 = P(x,y)$. Només ella mateixa, ja que en ser atòmica s'aplica la regla C1.
  - Les subfórmules de $F_6 = \neg Q(x,y)$. Les subfórmules són ella mateixa i, en aplicació de C2, les subfórmules de $Q(x,y)$; només ella mateixa en ser atòmica.

- Subfórmules de F_4, on $F_4 = \neg R(x,y))$. S'aplica la regla C2, ja que és negació i, per tant, les subfórmules són F_4 i les subfórmules de $R(x,y)$. Com que és atòmica i en aplicació de C1, l'única subfórmula de $R(x,y)$ és ella mateixa, $R(x,y)$.

Les subfórmules són subcadenes de caràcters que són fórmules elles mateixes. Les subfórmules de la fórmula de predicats F són les subcadenes de caràcters de F que són fórmules segons les regles de generació de fórmules de predicats (és a dir, que es poden generar amb aquestes regles). Són les fórmules que es van generant en el procés de construcció de la fórmula total.

En resum, la llista de les subfórmules de

$\forall x \exists y((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$

és

$P(x,y)$, $Q(x,y)$, $R(x,y)$ (les atòmiques),

$\neg Q(x,y)$, $\neg R(x,y)$, (no atòmiques)

$(P(x,y) \land \neg Q(x,y))$, (no atòmiques)

$((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$, (no atòmiques)

$\exists y((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$, (no atòmiques)

$\forall x \exists y((P(x,y) \land \neg Q(x,y)) \to \neg R(x,y))$ (no atòmiques). ■

En els exemples anteriors, s'ha indicat al final de cada exemple la llista de subfórmules, que coincideix amb les fórmules generades en el procés.

Aquí s'ha descrit de manera detallada l'aplicació de la gramàtica per a l'obtenció de les subfórmules. Tanmateix, és un procés força intuïtiu que es pot fer gairebé per simple inspecció visual si la fórmula no és extremament complicada, "anant de dintre cap enfora", "a major complexitat".

Exemple 5.35 Escriviu les subfórmules de:

$\forall x \exists y(P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))))$

x, y són les variables.

Les subfórmules són:

$P(x,y)$, $Q(x,y)$, $R(x,y)$, $S(x,y)$ (atòmiques)

$\neg Q(x,y)$, $\neg S(x,y)$

$(R(x,y) \to \neg S(x,y))$

$(\neg Q(x,y) \land (R(x,y) \to \neg S(x,y)))$

$(P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))))$

$\exists y(P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))))$

$\forall x \exists y(P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))))$. ■

A nivell pràctic, intuïtiu, de vegades es fa una lectura de "fora cap endins", com podem mostrar amb el mateix exemple anterior:

Exemple 5.36 Fórmula: $\forall x \exists y(P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))))$.

Subfórmules (lectura o anàlisi a l'inrevés):

$\forall x \exists y(P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))))$

$\exists y(P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))))$

$P(x,y) \to (\neg Q(x,y) \land (R(x,y) \to \neg S(x,y)))$

$P(x,y)$

$\neg Q(x,y) \land (R(x,y) \to \neg S(x,y))$

$\neg Q(x,y)$

$Q(x,y)$

$R(x,y) \rightarrow \neg S(x,y)$
$R(x,y)$
$\neg S(x,y)$
$S(x,y)$. ■

Exemple 5.37 Escriviu les subfórmules de la fórmula

$F = \exists x \forall y(\neg(P(x,y) \vee \neg Q(x,y)) \leftrightarrow \neg R(x,y))$.

Són:

$P(x,y)$, $Q(x,y)$, $R(x,y)$ (atòmiques)
$\neg P(x,y)$, $\neg Q(x,y)$, $\neg R(x,y)$
$\neg(P(x,y) \vee \neg Q(x,y))$
$(\neg(P(x,y) \vee \neg Q(x,y)) \leftrightarrow \neg R(x,y))$
$\forall y(\neg(P(x,y) \vee \neg Q(x,y)) \leftrightarrow \neg R(x,y))$
$\exists x \forall y(\neg(P(x,y) \vee \neg Q(x,y)) \leftrightarrow \neg R(x,y))$. ■

5.4.3. Arbre (jeràrquic) de la fórmula

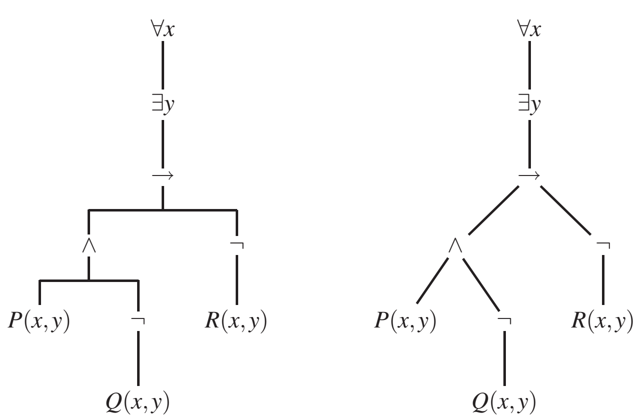
L'arbre de la fórmula en descriu la jerarquia, les dependències de les parts i el procés generador.

Exemple 5.38 Vegem-ho mitjançant l'exemple de la fórmula anterior:

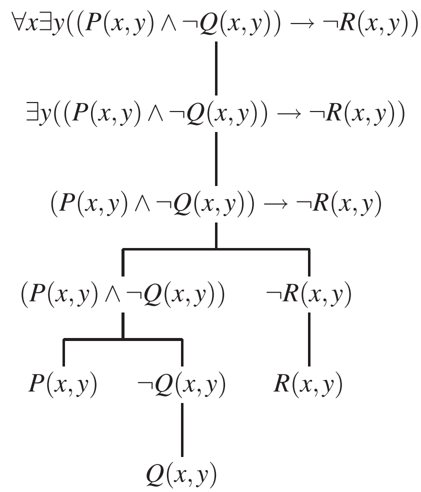
$\forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \rightarrow \neg R(x,y))$

L'arbre, en diverses versions:

Versió conceptual, on s'indiquen als nodes o vèrtexs les operacions o aplicacions de connectives o quantificacions:



Versió completa, on s'inclouen les fórmules completes del procés de generació (subfórmules):



Les subfórmules són les fórmules que ocupen els nodes o vèrtexs a la versió completa de l'arbre. ■

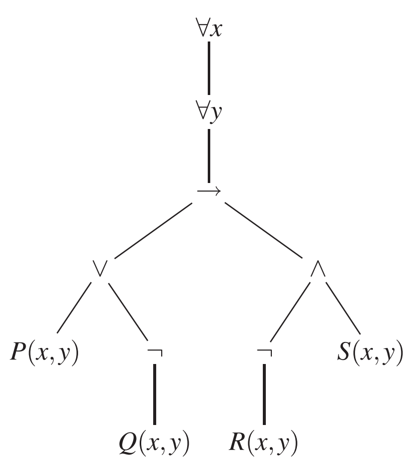
PROBLEMA 5.1

Escriviu un arbre de generació de la fórmula.

$\forall x \forall y((P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y)))$

Escriviu una versió en què es vegin totes les subfórmules.

Solució. Arbre de la fórmula:



Amb les subfórmules:

- $\forall x \forall y((P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y)))$
  - $\forall y((P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y)))$
    - $(P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y))$
      - $P(x,y) \vee \neg Q(x,y)$
        - $P(x,y)$
        - $\neg Q(x,y)$
          - $Q(x,y)$
      - $\neg R(x,y) \wedge S(x,y)$
        - $\neg R(x,y)$
          - $R(x,y)$
        - $S(x,y)$

Les variables són: x, y.

Les (sub)fórmules atòmiques són: $P(x,y)$, $Q(x,y)$, $R(x,y)$, $S(x,y)$.

Observació sobre el domini de les variables

Com expressar la pertinença al domini

Hi ha diverses maneres de fer-ho, segons els diversos graus de formalització possibles.

Se suposa que les variables pertanyen a dominis o conjunts, on "varien". S'indiquen amb el nom d'"universal" i se solen denotar genèricament per Ω. Si, per exemple, són nombres reals, aleshores $\Omega = \mathbb{R}$; si són nombres enters, llavors $\Omega = \mathbb{Z}$.

Aquests conjunts poden ser més d'un: per exemple, a la fórmula del límit d'una successió hi ha variables reals (ϵ) i variables naturals n. Hi poden haver, per tant, variables de tipologia diferent, pertanyent a diferents conjunts o universals.

Vegem diversos exemples possibles:

Exemple 5.39 "La suma de dos enters parells qualssevol és un nombre parell"

Versió 1. Siguin a i b nombres enters qualssevol. Aleshores:

$(2|a \wedge 2|b) \rightarrow 2|(a+b)$.

Versió 2. Per a a, b nombres enters qualssevol, $(2|a \wedge 2|b) \rightarrow 2|(a+b)$.

Versió 3. Si a, b són nombres enters qualssevol, aleshores: $(2|a \wedge 2|b) \rightarrow 2|(a+b)$.

Versió 4. Per tot $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $(2|a \wedge 2|b) \to 2|(a+b)$.

Versió 5. Si $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $\forall a \forall b((2|a \wedge 2|b) \to 2|(a+b))$.

Versió 6. $\forall a \forall b((2|a \wedge 2|b) \to 2|(a+b))$, amb $a \in \mathbb{Z}$, $b \in \mathbb{Z}$.

Les versions anteriors corresponen a fórmules completament estàndard d'acord amb la gramàtica. Donem-ne algunes versions més, ja fora de l'estàndard, però que són d'ús molt corrent:

Incorporant el domini a la fórmula de predicats ("híbrid"):

Versió 7. $\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2|a \wedge 2|b) \to 2|(a+b))$

Versió 8. $\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \to ((2|a \wedge 2|b) \to 2|(a+b)))$

O bé:

Versió 9. $\forall a \in \mathbb{Z} \forall b \in \mathbb{Z}((2|a \wedge 2|b) \to 2|(a+b))$

Versió 10. $\forall a, b \in \mathbb{Z}((2|a \wedge 2|b) \to 2|(a+b))$

O fins i tot:

Versió 11. $(2|a \wedge 2|b) \to 2|(a+b)$, $\forall a, b \in \mathbb{Z}$.

Versió 12. $(2|a \wedge 2|b) \to 2|(a+b)$, $\forall a, b$ nombres enters.

Aquestes últimes fórmules poden tenir problemes amb la integració en fórmules superiors que les continguin, i poden produir-se confusions en negar-les. En aquest últim cas, davant del dubte, és millor reformalitzar-les a forma estàndard i fer la negació segons el procediment habitual, gairebé automatitzat. ■

Exemple 5.40 A la manera estàndard, l'universal o domini de variables s'ha de declarar externament a la fórmula. Per exemple, si afirmem que:

"per als enters a, b, si ab és parell, aleshores a o b també ho són", que expressem amb una fórmula com:

$2|ab \to (2|a \vee 2|b)$

Si es vol fer la fórmula autocontinguda i sense declarar externament l'universal:

$(a \text{ enter } \wedge b \text{ enter } \wedge 2|ab) \to (2|a \vee 2|b)$
$(E(a) \wedge E(b) \wedge 2|ab) \to (2|a \vee 2|b)$ $(E =$ "ser enter")
$(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2|ab) \to (2|a \vee 2|b)$
$(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \to (2|ab \to (2|a \vee 2|b))$

Encara que no correspongui a l'enunciat, podem generalitzar, cosa que ens porta a la quantificació universal:

$\forall a \forall b(2|ab \to (2|a \vee 2|b))$ (estàndard)
$\forall a \in \mathbb{Z} \forall b \in \mathbb{Z}(2|ab \to (2|a \vee 2|b))$
$\forall a \forall b(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2|ab) \to (2|a \vee 2|b)$
$\forall a \forall b(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \to (2|ab \to (2|a \vee 2|b))$. ■

Observació: Interpretacions. Recuperem aquest tema considerant la gramàtica de predicats.

Aquestes són fórmules de predicat típiques:

$\forall x \forall y(P(x,y) = P(y,x))$
$I(s(x,y), p(x,y))$
$\forall x \forall y \forall z I(s(x,y), p(x,y))$

Què volen dir aquestes fórmules?

En principi, són fórmules buides, sense significat. No voldran dir alguna cosa, formular alguna propietat, fins que no hi donem una **interpretació**.

De fet, per a moltes fórmules que hem anat trobant ja s'estan donant interpretacions, tot i que no de manera sistemàtica, només de forma suficient per al que ens interessa a nosaltres: escriure amb precisió, formalització o simbolització. I parcialment ja s'ha incorporat a la fórmula: per exemple, quan escrivim:

$(2|a \wedge 2|b) \to 2|(a+b)$

això és un cas particular de la fórmula de predicats general:

$(P(x) \wedge P(y)) \to P(f(x,y))$

on diem què és la funció s, què és el predicat P (i cal dir quin és el domini de les variables).

Aquí és $f(x,y) = x+y$, $P(x) = 2|x$ ("ser múltiple de 2", "ser parell"), $\Omega = \mathbb{Z}$.

Canviant algun dels f, P, Ω, la mateixa fórmula de predicats es concreta en un altre enunciat; per exemple, tenen la mateixa estructura:

$(2|a \wedge 2|b) \to 2|(a+b)$
$(2 \nmid a \wedge 2 \nmid b) \to 2 \nmid ab$
$(2 \nmid a \wedge 2 \nmid b) \to 2|a+b$
$(3|a \wedge 3|b) \to 3|(a+b)$
$(3 \nmid a \wedge 3 \nmid b) \to 3 \nmid ab$

Donant-hi una interpretació, la fórmula adquireix sentit/significat (semàntica) i podem preguntar-nos si és certa o no.

Sobre la fórmula $(P(x) \wedge P(y)) \rightarrow P(f(x,y))$, no podem afirmar veracitat ni falsedat. Depèn de com s'interpreti.

5.5. Negació de quantificadors (continuació)

Negació del quantificador universal

Considerem la fórmula de predicat més simple, en què se suposa que l'objecte x és d'algun domini (universal) Ω:

$\forall x P(x)$ ("per a tot x, $P(x)$ (és cert)"), que pot ser certa o falsa.

Exemple 5.41 Per exemple, i suposant que l'universal és $\Omega = \mathbb{R}$, $\forall x(x^2 \geq 0)$. És a dir, en paraules, "el quadrat de tot nombre real és no negatiu". La negació és "no tot nombre real és de quadrat no negatiu". Intuïtivament, negar aquesta afirmació és afirmar que, per a algun nombre real x, la propietat no és certa, és a dir, que existeix un x tal que la propietat no és certa: $\exists x(x^2 < 0)$, o bé $\exists x(x^2 \not\geq 0)$. En forma completa, seria $\exists x(x \in \mathbb{R} \wedge x^2 < 0)$. La negació de "tot home és mortal" ("no tot home és mortal") és "algun home és no mortal", és a dir, "existeix algun home no mortal". ■

Exemple 5.42 Exemple-evidència de com ha de ser la negació: considerem l'enunciat "tots els homes tenen els ulls blaus". La negació "no tots els homes tenen els ulls blaus" es pot reexpressar intuïtivament com "algun home no té els ulls blaus" (i no: "tots els homes no tenen els ulls blaus", que és dir "cap home té els ulls blaus", que seria una afirmació més forta que la que busquem). És a dir, "existeix algun home que no té els ulls blaus" ("existeix algun objecte que és home i no té els ulls blaus"). Així, si considerem els predicats: H ("ser home"; $H(x) = x$ és home), B ("tenir els ulls blaus"; $B(x) = x$ té els ulls blaus), l'afirmació "tots els homes tenen els ulls blaus" es formalitza o simbolitza mitjançant $\forall x(H(x) \rightarrow B(x))$ i la negació com $\exists x(H(x) \wedge \neg B(x))$, de manera que:

$\neg\forall x(H(x) \rightarrow B(x)) \equiv \exists x(H(x) \wedge \neg B(x))$

Però $\exists x(H(x) \wedge \neg B(x)) \equiv \exists x \neg(H(x) \rightarrow B(x))$.

Així doncs, $\neg\forall x(H(x) \rightarrow B(x)) \equiv \exists x \neg(H(x) \rightarrow B(x))$ i, en general, l'estructura de negació és:

$\neg\forall x P(x) \equiv \exists x \neg P(x)$ ■

La fórmula de negació del quantificador universal és natural:

$\neg\forall x P(x) \equiv \exists x \neg P(x)$

En aquest context, el sentit d'aquest símbol $\equiv$ és que les fórmules "diuen" o signifiquen el mateix. Es podria tractar aquest aspecte amb més rigor, però aleshores hauríem de parlar d'"interpretacions" amb més profunditat, cosa que depassa els nostres objectius.

A partir d'aquesta base, es poden negar fórmules més complexes (vegeu exemples i exercicis).

Observació: P pot dependre d'altres variables.

$\forall x P(x,y)$

$\forall x(x+y>5)$

$\forall x_i P(\ldots,x_i,\ldots)$

$\neg\forall x_i P(\ldots,x_i,\ldots) \equiv \exists x_i \neg P(\ldots,x_i,\ldots)$.

Més en general, per a una fórmula F,

$\neg\forall xF \equiv \exists x\neg F$

Negació del quantificador existencial

Considerem la fórmula simple, on se suposa que l'objecte x és d'algun domini (universal) Ω:

$\exists x P(x)$ ("existeix un x tal que $P(x)$ (és cert)"), afirmació que pot ser certa o falsa.

La negació ve donada per la fórmula següent:

$\neg\exists x P(x) \equiv \forall x\neg P(x)$

A partir d'aquesta base, es poden negar fórmules més complexes (vegeu exemples).

Observació: P pot dependre d'altres variables.

$\exists x_i P(\ldots,x_i,\ldots)$

$\neg\exists x_i P(\ldots,x_i,\ldots) \equiv \forall x_i \neg P(\ldots,x_i,\ldots)$.

Més en general, per a una fórmula F:

$\neg\exists xF \equiv \forall x\neg F$

Més d'un quantificador. S'utilitzen les regles anteriors sistemàticament, una per una, pas a pas.

Exemple 5.43 Suposem que hem d'obtenir fórmules equivalents a la negació de $\forall x\exists y\ \exists z\ \forall t\forall wP$.

Totes les següents són negacions de la fórmula:

$\neg\forall x\exists y\exists z\forall t\forall wP$
$\exists x\neg\exists y\exists z\forall t\forall wP$
$\exists x\forall y\neg\exists z\forall t\forall wP$
$\exists x\forall y\forall z\neg\forall t\forall wP$
$\exists x\forall y\forall z\exists t\neg\forall wP$
$\exists x\forall y\forall z\exists t\exists w\neg P$. ■

Expressió d'un quantificador en termes de l'altre i dues negacions

El quantificador universal $\forall$ es pot expressar en termes de negació $\neg$ i del quantificador existencial $\exists$. En efecte, de la fórmula anterior, i aplicant doble negació:

$$\forall x P(x) \equiv \neg\neg\forall x P(x) \equiv \neg(\neg\forall x P(x)) \equiv \neg\exists x \neg P(x)$$

El quantificador existencial $\exists$ es pot expressar en termes de negació $\neg$ i del quantificador universal $\forall$. En efecte, de la fórmula anterior, i aplicant doble negació,

$$\exists x P(x) \equiv \neg\neg\exists x P(x) \equiv \neg(\neg\exists x P(x)) \equiv \neg\forall x \neg P(x)$$

Així doncs, atès que tot quantificador s'expressa en funció de l'altre i negacions, segons les fórmules anteriors, es podria prescindir d'un d'ells. El problema és que aleshores les fórmules resultarien innecessàriament complicades, antiintuïtives i difícils de llegir (per a un humà). De manera que *mantenim l'ús dels dos quantificadors*. Alguns textos defensen el criteri d'utilitzar-ne només un, per minimalitat i economia.

Exemple 5.44 Escriviu diverses fórmules de predicats equivalents a la negació de la fórmula:

$$F = \forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \to \neg R(x,y))$$

Escrivint $\neg F$, ja tindríem una negació de F. Obtenim altres fórmules equivalents a la negació (seqüència d'equivalències):

1. $\neg\forall x \exists y((P(x,y) \wedge \neg Q(x,y)) \to \neg R(x,y))$
2. $\exists x \neg\exists y((P(x,y) \wedge \neg Q(x,y)) \to \neg R(x,y))$ (per negació del quantificador existencial)
3. $\exists x \forall y \neg((P(x,y) \wedge \neg Q(x,y)) \to \neg R(x,y))$ (per negació del quantificador universal).

   La fórmula interior $(P(x,y) \wedge \neg Q(x,y)) \to \neg R(x,y)$ és un condicional, que negarem d'acord amb l'equivalència lògica $\neg(\alpha \to \beta) \equiv \alpha \wedge \neg\beta$ (fixats x,y, podem considerar-la com si fos una fórmula de proposicions i com a tal es negarà).

   Així:

4. $\exists x \forall y((P(x,y) \wedge \neg Q(x,y)) \wedge \neg\neg R(x,y))$ (per $\neg(\alpha \to \beta) \equiv \alpha \wedge \neg\beta$)

   Continuem la seqüència de fórmules:

5. $\exists x \forall y((P(x,y) \wedge \neg Q(x,y)) \wedge R(x,y))$ (per doble negació: $\neg\neg\alpha \equiv \alpha$)
6. $\exists x \forall y(P(x,y) \wedge \neg Q(x,y) \wedge R(x,y))$ (per associativitat de $\wedge$). ■

PROBLEMA 5.2

Considerem la fórmula F:

$$\forall x \exists y \forall z((P(x,y) \wedge \neg Q(x,y,z)) \to (T(x,y) \to \forall t(\neg R(x,y,z,t) \to \neg W(x,y)))).$$

Obteniu fórmules equivalents a la negació de F (a més de $\neg F$). Utilitzeu els resultats següents i indiqueu quins en seqüència:

a) *(1)* $\neg\forall x G \equiv \exists x \neg G$

b) *(2)* $\neg\exists x G \equiv \forall x \neg G$

c) *(3)* $\neg(\alpha \to \beta) \equiv \alpha \wedge \neg\beta$

d) *(4)* $\neg\neg\alpha \equiv \alpha$

e) *(5)* $\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$

Solució. N'escriurem unes quantes, mitjançant una seqüència d'equivalències.

$\neg\forall x\exists y\forall z((P(x,y)\wedge\neg Q(x,y,z)) \to (T(x,y) \to \forall t(\neg R(x,y,z,t) \to \neg W(x,y)))).$
$\exists x\neg\exists y\forall z((P(x,y)\wedge\neg Q(x,y,z)) \to (T(x,y) \to \forall t(\neg R(x,y,z,t) \to \neg W(x,y)))).$
$\exists x\forall y\neg\forall z((P(x,y)\wedge\neg Q(x,y,z)) \to (T(x,y) \to \forall t(\neg R(x,y,z,t) \to \neg W(x,y)))).$
$\exists x\forall y\exists z\neg((P(x,y)\wedge\neg Q(x,y,z)) \to (T(x,y) \to \forall t(\neg R(x,y,z,t) \to \neg W(x,y)))).$
$\exists x\forall y\exists z((P(x,y)\wedge\neg Q(x,y,z)) \wedge \neg(T(x,y) \to \forall t(\neg R(x,y,z,t) \to \neg W(x,y)))).$
$\exists x\forall y\exists z((P(x,y)\wedge\neg Q(x,y,z)) \wedge (T(x,y) \wedge \neg\forall t(\neg R(x,y,z,t) \to \neg W(x,y)))).$
$\exists x\forall y\exists z((P(x,y)\wedge\neg Q(x,y,z)) \wedge (T(x,y) \wedge \exists t\neg(\neg R(x,y,z,t) \to \neg W(x,y)))).$
$\exists x\forall y\exists z((P(x,y)\wedge\neg Q(x,y,z)) \wedge (T(x,y) \wedge \exists t(\neg R(x,y,z,t) \wedge \neg\neg W(x,y)))).$
$\exists x\forall y\exists z((P(x,y)\wedge\neg Q(x,y,z)) \wedge (T(x,y) \wedge \exists t(\neg R(x,y,z,t) \wedge W(x,y)))).$

Alternativament, i per a més claredat, s'hauria pogut considerar estrictament l'estructura, encara que la fórmula sigui incompleta:

$\neg\forall x\exists y\forall z((P\wedge\neg Q) \to (T \to \forall t(\neg R \to \neg W))).$
$\exists x\neg\exists y\forall z((P\wedge\neg Q) \to (T \to \forall t(\neg R \to \neg W))).$
$\exists x\forall y\neg\forall z((P\wedge\neg Q) \to (T \to \forall t(\neg R \to \neg W))).$
$\exists x\forall y\exists z\neg((P\wedge\neg Q) \to (T \to \forall t(\neg R \to \neg W))).$
$\exists x\forall y\exists z((P\wedge\neg Q) \wedge \neg(T \to \forall t(\neg R \to \neg W))).$
$\exists x\forall y\exists z((P\wedge\neg Q) \wedge (T \wedge \neg\forall t(\neg R \to \neg W))).$
$\exists x\forall y\exists z((P\wedge\neg Q) \wedge (T \wedge \exists t\neg(\neg R \to \neg W))).$
$\exists x\forall y\exists z((P\wedge\neg Q) \wedge (T \wedge \exists t(\neg R \wedge \neg\neg W))).$
$\exists x\forall y\exists z((P\wedge\neg Q) \wedge (T \wedge \exists t(\neg R \wedge W))).$
$\exists x\forall y\exists z(P\wedge\neg Q \wedge T \wedge \exists t(\neg R \wedge W)).$

La seqüència aplicada és: $(1),(2),(1),(3),(3),(1),(3),(4),(5)$

PROBLEMA 5.3

Neguem, pas a pas, l'enunciat següent (no s'admet el símbol $\neg$ a l'esquerra). Escrivim uns quants enunciats equivalents a la negació):

$$F = \forall x \exists y ((P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y)))$$

Es tracta de dir quines propietats s'han fet servir a cada pas de la seqüència de fórmules equivalents següent:

$\neg \forall x \exists y ((P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y)))$ [1]

$\exists x \neg \exists y ((P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y)))$ [2]

$\exists x \forall y \neg ((P(x,y) \vee \neg Q(x,y)) \rightarrow (\neg R(x,y) \wedge S(x,y)))$ [3]

$\exists x \forall y ((P(x,y) \vee \neg Q(x,y)) \wedge \neg(\neg R(x,y) \wedge S(x,y)))$ [4]

$\exists x \forall y ((P(x,y) \vee \neg Q(x,y)) \wedge (\neg\neg R(x,y) \vee \neg S(x,y)))$ [5]

$\exists x \forall y ((P(x,y) \vee \neg Q(x,y)) \wedge (R(x,y) \vee \neg S(x,y)))$ [6]

$\exists x \forall y (Q(x,y) \rightarrow P(x,y)) \wedge (S(x,y) \rightarrow R(x,y)))$ [7]

Solució

[1]: és simplement la negació de la fórmula F, és a dir, $\neg F$.

de [1] a [2]: negació de $\forall xG$, és a dir, $\neg \forall wG \equiv \exists w \neg G$.

de [2] a [3]: negació de $\exists xG$, és a dir, $\neg \exists wG \equiv \forall w \neg G$.

de [3] a [4]: negació del condicional, és a dir, $\neg(\alpha \rightarrow \beta) \equiv \alpha \wedge \neg \beta$,

de [4] a [5]: De Morgan.

de [5] a [6]: per doble negació.

de [6] a [7]: per commutativitat de la disjunció i $\neg \alpha \vee \beta \equiv \alpha \rightarrow \beta$.

PROBLEMA 5.4

Sigui $\alpha := \forall x \forall y ((P(x,y,z) \wedge Q(x,y)) \rightarrow \neg R(x,y,t))$. *Expresseu la fórmula de predicat anterior com a negació, en la forma* $\neg \beta$*, en què* β *és una fórmula de predicat sense* $\neg$.

Solució. Es pot resoldre de manera sistemàtica: α equival a $\neg\neg\alpha \equiv \neg(\neg\alpha)$ i aleshores podem escriure la seqüència següent de fórmules equivalents:

$\alpha := \forall x \forall y ((P(x,y,z) \wedge Q(x,y)) \rightarrow \neg R(x,y,t))$

$\neg\neg \forall x \forall y ((P(x,y,z) \wedge Q(x,y)) \rightarrow \neg R(x,y,t))$

$\neg(\neg \forall x \forall y ((P(x,y,z) \wedge Q(x,y)) \rightarrow \neg R(x,y,t)))$ (mantindrem la negació a l'esquerra a partir d'aquí).

$\neg(\exists x \neg \forall y ((P(x,y,z) \wedge Q(x,y)) \rightarrow \neg R(x,y,t)))$

$\neg(\exists x \exists y \neg ((P(x,y,z) \wedge Q(x,y)) \rightarrow \neg R(x,y,t)))$

$\neg(\exists x \exists y ((P(x,y,z) \wedge Q(x,y)) \wedge \neg\neg R(x,y,t)))$

$\neg(\exists x \exists y ((P(x,y,z) \wedge Q(x,y)) \wedge R(x,y,t)))$

Que el lector indiqui què s'aplica, i on, a cada pas de la seqüència anterior: negació dels quantificadors, del condicional, doble negació i associativitat.

PROBLEMA 5.5

Considereu la fórmula $\forall x \exists y \neg \forall z P(x,y,z,t)$*. Digueu si es pot escriure com a negació (*$\neg\alpha$*) (i digueu com).*

Solució. Un mètode és desplaçant $\neg$ cap a l'esquerra, fent servir les equivalències corresponents:

$$\forall x \exists y \neg \forall z P(x,y,z,t)$$

$$\forall x \neg \forall y \forall z P(x,y,z,t)$$

$$\neg \exists x \forall y \forall z P(x,y,z,t)$$

PROBLEMA 5.6

Escriviu $\forall x \forall y (P(x,y,z) \wedge (Q(x,y) \rightarrow \neg R(x,y,z,t)))$ *com a negació.*

Solució. Podríem fer servir $F \equiv \neg\neg F \equiv \neg(\neg F)$. Procedirem alternativament:

$$\forall x \forall y (P(x,y,z) \wedge (Q(x,y) \rightarrow \neg R(x,y,z,t)))$$

$$\forall x \forall y (P(x,y,z) \wedge (\neg Q(x,y) \vee \neg R(x,y,z,t)))$$

$$\forall x \forall y (P(x,y,z) \wedge \neg (Q(x,y) \wedge R(x,y,z,t)))$$

$$\forall x \forall y (\neg\neg P(x,y,z) \wedge \neg (Q(x,y) \wedge R(x,y,z,t)))$$

$$\forall x \forall y \neg (\neg P(x,y,z) \vee (Q(x,y) \wedge R(x,y,z,t)))$$

$$\forall x \neg \exists y (\neg P(x,y,z) \vee (Q(x,y) \wedge R(x,y,z,t)))$$

$$\neg \exists x \exists y (\neg P(x,y,z) \vee (Q(x,y) \wedge R(x,y,z,t)))$$

Opcionalment:

$$\neg \exists x \exists y (P(x,y,z) \rightarrow (Q(x,y) \wedge R(x,y,z,t)))$$

El lector justificarà cada pas.

PROBLEMA 5.7

Considereu la fórmula de predicats F *donada per:*

$$\forall y \exists x (R(x,y) \rightarrow \forall z (T(x) \rightarrow \neg W(x,z)))$$

on R, T, W *són predicats (lletres de predicat).*

Obtenim pas a pas una fórmula de predicats equivalent a $\neg F$ *sense connectives* $\neg$*. Justifiqueu cada pas.*

Totes les fórmules que es van escrivint a continuació són equivalents a la negació de F:

És a dir, si denotem:

F1: $\neg\forall y\exists x(R(x,y)\to\forall z(T(x)\to\neg W(x,z)))$
F2: $\exists y\neg\exists x(R(x,y)\to\forall z(T(x)\to\neg W(x,z)))$
F3: $\exists y\forall x\neg(R(x,y)\to\forall z(T(x)\to\neg W(x,z)))$
F4: $\exists y\forall x(R(x,y)\wedge\neg\forall z(T(x)\to\neg W(x,z)))$
F5: $\exists y\forall x(R(x,y)\wedge\exists z\neg(T(x)\to\neg W(x,z)))$
F6: $\exists y\forall x(R(x,y)\wedge\exists z(T(x)\wedge\neg\neg W(x,z)))$
F7: $\exists y\forall x(R(x,y)\wedge\exists z(T(x)\wedge W(x,z)))$

és $\neg F\equiv F1\equiv F2\equiv F3\equiv F4\equiv F5\equiv F6\equiv F7$*, amb* $F7$ *sense* $\neg$.

Solució. Justificacions:

$\neg\forall y\exists x(R(x,y)\to\forall z(T(x)\to\neg W(x,z)))$

Aplicant $\neg\forall zP(z)\equiv\exists z\neg P(z)$ (de fet, més en general, $\neg\forall zP(\ldots,z,\ldots)\equiv\exists z\neg P(\ldots,z,\ldots)$):

$\exists y\neg\exists x(R(x,y)\to\forall z(T(x)\to\neg W(x,z)))$

Aplicant $\neg\exists zP(z)\equiv\forall z\neg P(z)$:

$\exists y\forall x\neg(R(x,y)\to\forall z(T(x)\to\neg W(x,z)))$

Aplicant $\neg(\alpha\to\beta)\equiv\alpha\wedge\neg\beta$:

$\exists y\forall x(R(x,y)\wedge\neg\forall z(T(x)\to\neg W(x,z)))$

Aplicant $\neg\forall zP(z)\equiv\exists z\neg P(z)$:

$\exists y\forall x(R(x,y)\wedge\exists z\neg(T(x)\to\neg W(x,z)))$

Aplicant $\neg(\alpha\to\beta)\equiv\alpha\wedge\neg\beta$:

$\exists y\forall x(R(x,y)\wedge\exists z(T(x)\wedge\neg\neg W(x,z)))$

Aplicant $\neg\neg\alpha\equiv\alpha$:

$\exists y\forall x(R(x,y)\wedge\exists z(T(x)\wedge W(x,z)))$, sense negacions.

PROBLEMA 5.8

Considerem els predicats $P(x,y)$ *i* $Q(x,y)$*. Establiu una seqüència de fórmules equivalents que ens portin de:*

$\forall x\forall y(\neg P(x,y)\to\neg Q(x,y))$

a:

$\neg\exists x\exists y(\neg P(x,y)\wedge Q(x,y))$

Solució. Una possibilitat és:

$\forall x\forall y(\neg P(x,y)\rightarrow\neg Q(x,y))$

$\forall x\forall y(\neg\neg P(x,y)\vee\neg Q(x,y))$, per l'equivalència lògica $a\rightarrow b\equiv\neg a\vee b$

$\forall x\forall y(\neg(\neg P(x,y)\wedge Q(x,y)))$, per l'equivalència lògica de De Morgan,

$\forall x\neg\exists y(\neg P(x,y)\wedge Q(x,y))$, per $\forall x\neg S\equiv\neg\exists xS$,

$\neg\exists x\exists y(\neg P(x,y)\wedge Q(x,y))$, per $\forall x\neg S\equiv\neg\exists xS$,

Una altra possibilitat seria partir de $\neg\neg\forall x\forall y(\neg P(x,y)\rightarrow\neg Q(x,y))$:

$\neg\neg\forall x\forall y(\neg P(x,y)\rightarrow\neg Q(x,y))$
$\neg(\neg\forall x\forall y(\neg P(x,y)\rightarrow\neg Q(x,y)))$
$\neg(\exists x\neg\forall y(\neg P(x,y)\rightarrow\neg Q(x,y)))$
$\neg\exists x\exists y\neg(\neg P(x,y)\rightarrow\neg Q(x,y)))$
$\neg\exists x\exists y(\neg P(x,y)\wedge\neg\neg Q(x,y)))$
$\neg\exists x\exists y(\neg P(x,y)\wedge Q(x,y)))$

PROBLEMA 5.9

Considereu la fórmula de predicats G donada per:

$\exists y\forall x((A(x)\wedge B(x,y))\rightarrow(C(x,y)\wedge\neg D(x,y)))$

on A,B,C,D són predicats (lletres de predicat).

Obteniu pas a pas la fórmula de predicats que s'indica a continuació, equivalent a $\neg G$ sense connectives $\neg$ (no hi introduïu nous predicats). Justifiqueu cada pas.

$\forall y\exists x((A(x)\wedge B(x,y))\wedge(C(x,y)\rightarrow D(x,y)))$

Solució

$\neg G$

$\forall y\neg\forall x((A(x)\wedge B(x,y))\rightarrow(C(x,y)\wedge\neg D(x,y)))$ (negació de $\exists$)

$\forall y\exists x\neg((A(x)\wedge B(x,y))\rightarrow(C(x,y)\wedge\neg D(x,y)))$ (negació de $\forall$)

$\forall y\exists x((A(x)\wedge B(x,y))\wedge\neg(C(x,y)\wedge\neg D(x,y)))$ (negació de $\rightarrow$)

$\forall y\exists x((A(x)\wedge B(x,y))\wedge(\neg C(x,y)\vee\neg\neg D(x,y)))$ (De Morgan)

$\forall y\exists x((A(x)\wedge B(x,y))\wedge(\neg C(x,y)\vee D(x,y)))$ (per doble negació)

$\forall y\exists x((A(x)\wedge B(x,y))\wedge(C(x,y)\rightarrow D(x,y)))$ (per $\alpha\rightarrow\beta\equiv\neg\alpha\vee\beta$)

PROBLEMA 5.10

Considereu la fórmula F donada per $\forall x P(x) \wedge \exists t(Q(t) \to \neg R(t))$. Escriviu unes quantes fórmules equivalents a F amb una única negació $\neg$ al principi.

Solució. És $F \equiv \neg\neg F$, per l'equivalència de la doble negació.

$F \equiv \neg\neg F \equiv \neg(\neg F)$

$\equiv \neg(\neg(\forall x P(x) \wedge \exists t(Q(t) \to \neg R(t))))$

$\equiv \neg(\neg\forall x P(x) \vee \neg\exists t(Q(t) \to \neg R(t)))$, per equivalència de De Morgan,

$\equiv \neg(\exists x \neg P(x) \vee \forall t \neg(Q(t) \to \neg R(t)))$, per equivalències de negació de quantificadors,

$\equiv \neg(\exists x \neg P(x) \vee \forall t(Q(t) \wedge \neg\neg R(t)))$, per equivalència de negació del condicional,

$\equiv \neg(\exists x \neg P(x) \vee \forall t(Q(t) \wedge R(t)))$, per l'equivalència de la doble negació.

Vegem algunes exemples de negació de fórmules de predicat.

PROBLEMA 5.11

Considereu la fórmula de predicats:

$\forall x \exists y(P(x,y) \to (A(x) \vee B(y)))$

Escriviu diverses fórmules equivalents a la negació de l'anterior, amb algunes que satisfacin:

a) sense la connectiva $\vee$
b) amb només $\neg, \to$

Solució. La negació de la fórmula és simplement

$\neg\forall x \exists y(P(x,y) \to (A(x) \vee B(y)))$.

a) Ara apliquem diverses equivalències lògiques per obtenir equivalents a aquesta negació.

$\neg\forall x \exists y(P(x,y) \to (A(x) \vee B(y)))$, que és equivalent a (per (1)) (vegeu més avall)

$\exists x \neg\exists y(P(x,y) \to (A(x) \vee B(y)))$, que és equivalent a (per (2))

$\exists x \forall y \neg(P(x,y) \to (A(x) \vee B(y)))$, que és equivalent a (per (3))

$\exists x \forall y(P(x,y) \wedge \neg(A(x) \vee B(y)))$, que és equivalent a (per (4))

$\exists x \forall y(P(x,y) \wedge (\neg A(x) \wedge \neg B(y)))$ (sense les connectives $\vee, \to$)

Justificacions:

(1): $\neg\forall tT \equiv \exists t\neg T$

(2): $\neg\exists tT \equiv \forall t\neg T$

(3): $\neg(A \to B) \equiv (A \land \neg B)$

(4): Per De Morgan.

b) Podem substituir a la tercera fórmula anterior $A(x) \lor B(y)$ per l'equivalent següent:

$A(x) \lor B(y)$, que equival a (per (5))
$(\neg(\neg A(x))) \lor B(y)$, que equival a (per (6))
$((\neg A(x)) \to B(y)$

Justificacions:

(5): per l'equivalència de doble negació

(6): per $C \to D \equiv \neg C \lor D$

I ara, substituint:

$\exists x\forall y\neg(P(x,y) \to (A(x) \lor B(y)))$
$\exists x\forall y\neg(P(x,y) \to (\neg A(x) \to B(y)))$

PROBLEMA 5.12

Considereu l'afirmació $x < y \Rightarrow x^2 < y^2$, per a x,y nombres reals arbitraris.

Equivalents:

$x < y \Rightarrow x^2 < y^2$, per a x,y nombres reals qualssevol.
$x < y \Rightarrow x^2 < y^2$, per a tot x,y nombres reals.

a) Formalitzeu l'afirmació amb una fórmula de predicat.
b) Negueu l'afirmació aportant diverses fórmules equivalents a la negació.
c) És certa l'afirmació?

Solució

a) No s'inclou el conjunt universal $\mathbb{R}$ a la fórmula:

$\forall x\forall y(x < y \to x^2 < y^2)$.

Podem incloure el domini:

$\forall x \forall y((x \in \mathbb{R} \wedge x \in \mathbb{R}) \to (x < y \to x^2 < y^2))$

$\forall x \forall y((x \in \mathbb{R} \wedge x \in \mathbb{R} \wedge x < y) \to x^2 < y^2))$

$\forall x \in \mathbb{R} \forall y \in \mathbb{R}(x < y \to x^2 < y^2)$

b) $\neg \forall x \forall y(x < y \to x^2 < y^2)$

$\exists x \neg \forall y(x < y \to x^2 < y^2)$ (per $\neg \forall t P \equiv \exists t \neg P$)

$\exists x \exists y \neg(x < y \to x^2 < y^2)$ (per $\neg \forall t P \equiv \exists t \neg P$)

$\exists x \exists y(x < y \wedge \neg(x^2 < y^2))$ (per $\neg(P \to Q) \equiv P \wedge \neg Q$)

$\exists x \exists y(x < y \wedge x^2 \not< y^2)$. O bé:

$\exists x \exists y(x < y \wedge x^2 \geq y^2)$

c) No és certa, com es pot veure aportant un contraexemple: $x = -2$, $y = 1$.

PROBLEMA 5.13

Considereu la fórmula del càlcul de predicats:

$$\forall x \exists y \forall z((P(x,y,z) \wedge Q(y,z)) \to (R(x,y) \to \exists w \neg S(w)))$$

Es demana d'escriure negacions equivalents fins a aconseguir que no hi figuri cap connectiva $\neg$, és a dir, fórmules equivalents a

$$\neg \forall x \exists y \forall z((P(x,y,z) \wedge Q(y,z)) \to (R(x,y) \to \exists w \neg S(w)))$$

però sense $\neg$.

Solució. Farem servir sistemàticament

$$\neg \forall x T(x) \equiv \exists x \neg T(x) \qquad \neg \exists x T(x) \equiv \forall x \neg T(x)$$

Escrivim la seqüència de fórmules equivalents:

$\neg \forall x \exists y \forall z((P(x,y,z) \wedge Q(y,z)) \to (R(x,y) \to \exists w \neg S(w)))$ [1]

$\exists x \neg \exists y \forall z((P(x,y,z) \wedge Q(y,z)) \to (R(x,y) \to \exists w \neg S(w)))$ [2]

$\exists x \forall y \neg \forall z((P(x,y,z) \wedge Q(y,z)) \to (R(x,y) \to \exists w \neg S(w)))$ [3]

$\exists x \forall y \exists z \neg((P(x,y,z) \wedge Q(y,z)) \to (R(x,y) \to \exists w \neg S(w)))$ [4]

$\exists x \forall y \exists z((P(x,y,z) \wedge Q(y,z)) \wedge \neg(R(x,y) \to \exists w \neg S(w)))$ [5]

$\exists x \forall y \exists z((P(x,y,z) \wedge Q(y,z)) \wedge (R(x,y) \wedge \neg \exists w \neg S(w)))$ [6]

$\exists x \forall y \exists z((P(x,y,z) \wedge Q(y,z)) \wedge (R(x,y) \wedge \forall w \neg \neg S(w)))$ [7]

$\exists x \forall y \exists z((P(x,y,z) \wedge Q(y,z)) \wedge (R(x,y) \wedge \forall w S(w)))$ [8]

Justificacions:

pas de [1] a [2]: per $\neg\forall x T(x) \equiv \exists x \neg T(x)$

pas de [2] a [3]: per $\neg\exists x T(x) \equiv \forall x \neg T(x)$

pas de [3] a [4]: per $\neg\forall x T(x) \equiv \exists x \neg T(x)$

pas de [4] a [5]: per $\neg(A \to B) \equiv A \wedge \neg B$

pas de [5] a [6]: per $\neg(A \to B) \equiv A \wedge \neg B$

pas de [6] a [7]: per $\neg\exists x T(x) \equiv \forall x \neg T(x)$

pas de [7] a [8]: per l'equivalència de doble negació.

És important saber negar fórmules de predicat, ja que pot ser necessari com a punt de partida de demostracions per reducció a l'absurd.

Negació de fórmules de sintaxi híbrida (semiformal, no ajustada a la gramàtica o a les regles generatives)

Considerem la fórmula $\forall x \in B \;\; P(x)$. Per a negar la fórmula, cal reformular-la i escriure-la en forma estàndard (és a dir, generada per la gramàtica). Posteriorment, es negarà de manera automatitzada:

$\forall x \in B \;\; P(x)$

$\forall x(x \in B \to P(x))$

Negació: $\neg\forall x(x \in B \to P(x)) \equiv \exists x \neg(x \in B \to P(x)) \equiv \exists x(x \in B \wedge \neg P(x)$

I ara, si volem podem retornar a la sintaxi híbrida: $\exists x \in B \;\; \neg P(x)$

Anàlogament, per a negar $\exists x \in B \;\; P(x)$ es procedeix de forma similar. Vegeu l'exercici següent:

PROBLEMA 5.14

Negueu l'enunciat genèric en formalització intermèdia:

$\exists x \in B \; (P(x))$

Solució. S'ha de reescriure en forma estàndard, segons la gramàtica del llenguatge de predicats, posteriorment es nega i finalment es restableix la formalització intermèdia.

$\exists x \in B \; (P(x))$

$\exists x(x \in B \wedge P(x)) \; \neg\exists x(x \in B \wedge P(x))$

$\forall x \neg(x \in B \wedge P(x))$ (per negació de $\exists$)

$\forall x(\neg x \in B \vee \neg P(x))$ (per De Morgan)

$\forall x(x \in B \to \neg P(x))$ (per $\neg\alpha \vee \beta \equiv \alpha \to \beta$)

$\forall x \in B(\neg P(x))$

El que s'ha explicat abans s'ha de fer en moltes fórmules que s'enuncien de manera deficient, des del punt de vista formal, tot i que normalment se solen entendre afegint-hi altres explicacions. Un exemple típic és el de la definició de límit.

És convenient saber formalitzar en forma estàndard, d'acord amb la gramàtica, per tal de poder obtenir negacions de forma segura i gairebé automatitzada. Un exemple clar és els dels diversos conceptes de límit de successions, de funcions, de continuïtat, que moltes vegades apareixen als llibres de text expressats d'una forma millorable.

Exemple 5.45 Vegem el cas de la definició de límit: formalització per a poder negar amb seguretat.

Pot ser convenient en una demostració per reducció a l'absurd.

Suposem que tenim una versió informal semiformalitzada del concepte de límit d'una successió de nombres reals: $\lim\limits_{n\to\infty} a_n = L$ com:

$\forall\epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}(n > n_0 \to |a_n - L| < \epsilon)$

Quan es nega, resulta:

$\exists\epsilon > 0 \forall n_0 \in \mathbb{N}\ldots$

Perquè la negació no és:

$\exists\epsilon \leq 0 \forall n_0 \notin \mathbb{N}\ldots?$

Solució. Per veure per què, s'ha de formalitzar completament la fórmula i després negar-la (s'inclouen els dominis a la fórmula):

$\forall\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \to \exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \to |a_n - L| < \epsilon)))$

Observem l'estructura principal de la fórmula:

$\forall\epsilon(\alpha \to \beta)$, on:

$\alpha := (\epsilon \in \mathbb{R} \wedge \epsilon > 0)$
$\beta := \exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \to |a_n - L| < \epsilon))$

Hi destaquem el condicional (primer, a l'esquerra de la fórmula):

$\forall\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \to \exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \to |a_n - L| < \epsilon)))$

L'estructura de β és una conjunció dintre del quantificador existencial:

$\beta := \exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \to |a_n - L| < \epsilon))$

Si considerem $\gamma := (n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon$, l'estructura bàsica és la d'un condicional:

$\gamma := (n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon$

Si n'obtenim la negació de manera sistemàtica, resulta:

$$\neg\forall\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \rightarrow \exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))) \quad (1)$$
$$\exists\epsilon\neg((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \rightarrow \exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))) \quad (2)$$
$$\exists\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \wedge \neg\exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))) \quad (3)$$
$$\exists\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \wedge \forall n_0\neg(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))) \quad (4)$$
$$\exists\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \wedge \forall n_0(\neg n_0 \in \mathbb{N} \vee \neg\forall n((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))) \quad (5)$$
$$\exists\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \wedge \forall n_0(\neg n_0 \in \mathbb{N} \vee \exists n\neg((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))) \quad (6)$$
$$\exists\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \wedge \forall n_0(n_0 \in \mathbb{N} \rightarrow \exists n\neg((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))) \quad (7)$$
$$\exists\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \wedge \forall n_0(n_0 \in \mathbb{N} \rightarrow \exists n((n \in \mathbb{N} \wedge n > n_0) \wedge \neg|a_n - L| < \epsilon))) \quad (8)$$
$$\exists\epsilon((\epsilon \in \mathbb{R} \wedge \epsilon > 0) \wedge \forall n_0(n_0 \in \mathbb{N} \rightarrow \exists n((n \in \mathbb{N} \wedge n > n_0) \wedge |a_n - L| \geq \epsilon))) \quad (9)$$

Perquè:

1]: Simplement negació de la fórmula.

2]: Negació del quantificador universal: $\neg\forall\epsilon\ldots \equiv \exists\epsilon\neg\ldots$.

3]: Negació d'un condicional: $\neg(\alpha \rightarrow \beta) \equiv (\alpha \wedge \neg\beta)$.

4]: Negació del quantificador existencial: $\neg\exists n_0(\ldots) \equiv \forall n_0\neg(\ldots)$.

5]: Negació d'una disjunció (De Morgan).

6]: Negació del quantificador universal.

7]: S'aplica $\neg p \vee q \equiv p \rightarrow q$.

8]: Negació del condicional.

Exposició alternativa, detallant més l'estructura abans de començar a negar

Estructura principal de la fórmula:

$F := \forall\epsilon(\alpha \rightarrow \beta)$, amb:

$\alpha := (\epsilon \in \mathbb{R} \wedge \epsilon > 0)$

$\beta := \exists n_0(n_0 \in \mathbb{N} \wedge \forall n((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon))$

$\beta := \exists n_0(\beta_1 \wedge \beta_2)$, on

$\beta_1 = n_0 \in \mathbb{N}$, $\beta_2 := \forall n((n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon)$

$\gamma := (n \in \mathbb{N} \wedge n > n_0) \rightarrow |a_n - L| < \epsilon$, on $\gamma_1 := n \in \mathbb{N} \wedge n > n_0)$, $\gamma_2 := |a_n - L| < \epsilon$

Amb aquestes subfórmules:

$F = \forall\epsilon(\alpha \to \beta)$

$F = \forall\epsilon(\alpha \to \exists n_0(\beta_1 \wedge \beta_2))$

$F = \forall\epsilon(\alpha \to \exists n_0(\beta_1 \wedge \forall n\gamma))$

$F = \forall\epsilon(\alpha \to \exists n_0(\beta_1 \wedge \forall n(\gamma_1 \to \gamma_2))$, que podem negar rutinàriament:

$$\neg F = \neg\forall\epsilon(\alpha \to \exists n_0(\beta_1 \wedge \forall n(\gamma_1 \to \gamma_2)))$$
$$= \exists\epsilon\neg(\alpha \to \exists n_0(\beta_1 \wedge \forall n(\gamma_1 \to \gamma_2))) = \exists\epsilon(\alpha \wedge \neg\exists n_0(\beta_1 \wedge \forall n(\gamma_1 \to \gamma_2)))$$
$$= \exists\epsilon(\alpha \wedge \forall n_0\neg(\beta_1 \wedge \forall n(\gamma_1 \to \gamma_2)))$$
$$= \exists\epsilon(\alpha \wedge \forall n_0(\neg\beta_1 \vee \neg\forall n(\gamma_1 \to \gamma_2)))$$
$$= \exists\epsilon(\alpha \wedge \forall n_0(\neg\beta_1 \vee \exists n\neg(\gamma_1 \to \gamma_2)))$$
$$= \exists\epsilon(\alpha \wedge \forall n_0(\neg\beta_1 \vee \exists n(\gamma_1 \wedge \neg\gamma_2))) = \exists\epsilon(\alpha \wedge \forall n_0(\beta_1 \to \exists n(\gamma_1 \wedge \neg\gamma_2)))$$

Finalment, només cal substituir, escrivint $\neg\gamma_2 = \neg(|a_n - L| < \epsilon) = |a_n - L| \geq \epsilon$.

Exercici: Escriviu l'arbre de la fórmula del límit i el de la seva negació. ■

5.6. Traducció: formalització (simbolització) i desformalització

Tot aquest capítol és essencialment de traducció de llenguatge natural a formalitzat, i a l'inrevés, i amb diversos graus o nivells de formalització (simbolització).

Els exercicis són només de formalització i de comprensió dels enunciats. No es tracta aquí de demostrar cap enunciat. De fet, alguna de les propietats que s'enuncien podrien no ser certes: es tracta d'exercicis formals.

Com traduir frases del llenguatge natural a una fórmula de predicats? Segueixen alguns consells (vegeu [MEND66]), que ja s'han explicitat anteriorment.

1. Una frase de la forma "Tots els A són B" es tradueix a $\forall x(A(x) \to B(x))$. Internament al parèntesi es pot substituir pel contrarecíproc: $\forall x(\neg B(x) \to \neg A(x))$
2. Una frase de la forma "Algun A és B" es tradueix per $\exists x(A(x) \wedge B(x))$
3. Una frase de la forma "Cap A és B" es tradueix per $\forall x(A(x) \to \neg B(x))$ o bé, substituint pel contrarecíproc, $\forall x(B(x) \to \neg A(x))$

En aquesta secció, es tracta de resoldre problemes de traducció en els dos sentits:

a) Formalització, traducció, simbolització: del llenguatge natural a la fórmula de predicats. Es tracta de traduir frases a fórmules de predicat.
b) Lectura, desformalització: de la fórmula de predicats al llenguatge natural.

Convé tenir present que, de vegades, per raó de les característiques del llenguatge natural, que permet un gran desordre i desgavell, la frase està a l'inrevés (començant enunciant la conclusió), i també està amagada, implícita, part de l'estructura lògica, com el condicional i la quantificació. Això es posa de manifest especialment a la secció sobre *anàlisi d'enunciats*. Alguns enunciats són ambigus; algunes frases s'han d'endreçar (fer-ne endreça, des del punt de vista lògic) i refer. S'ha de "donar la volta" a la frase. Se n'analitza l'estructura lògica, s'hi detecten quantificadors i condicionals "amagats".

En aquesta secció, oferim, sense massa ordre, problemes diversos sobre el tema.

5.6.1. Problemes diversos de simbolització (i viceversa)

Lectura d'una fórmula:

Exemple 5.46 Com es llegeix la fórmula següent, on se suposa que totes les variables són de A:

$\exists x \forall y (xy > 0)$ $(A = \mathbb{Z})$

Hi ha diverses variants equivalents:

"Existeix x tal que, per a tot y, es compleix $xy > 0$"

"Existeix x tal que $xy > 0$, per a tot y".

"Existeix x tal que per a cada y, es compleix $xy > 0$"

"Per a algun x, és $xy > 0$, per a tot y".

"Existeix x tal que, per a qualsevol y, es compleix $xy > 0$".

Si volem incorporar la pertinença al conjunt A, aleshores una possible versió seria

"Existeix $x \in \mathbb{Z}$ tal que, per a tot $y \in \mathbb{Z}$, es compleix $xy > 0$"

"Existeix un nombre enter x tal que, per a tot enter y, es compleix $xy > 0$" ■

Exemple 5.47 En alguns casos, els enunciats en llenguatge natural són ambigus, tot i que el significat és ben clar per exclusió, per eliminació per absurd de qualsevol altre. Considerem, per exemple, la frase:

"Algú és robat cada hora".

"Cada hora roben algú".

"Cada hora es roba a algú".

Hi introduïm el predicat 2-ari:

$R(x,t)$:="x és robat a l'hora t"

Podem escriure dues formalitzacions possibles, si no atenem el significat del que estem dient:

$\forall t \exists x R(x,t)$

$\exists x \forall t R(x,t)$

La segona fórmula no és la traducció correcta, segons el significat, ja que s'estaria dient que "una mateixa persona s'estaria robant cada hora", que no és el que es vol dir (suposadament). Per tant:

$\forall t \exists x R(x,t)$ (correcte)

$\exists x \forall t R(x,t)$ (incorrecte)

En aquest exemple s'observa que l'ordre dels quantificadors pot ser important. ■

Diferents nivells d'explicitació. Quan expressem enunciats o propietats o definicions, es poden utilitzar, depenent del que sigui possible o el que més convingui, fórmules de predicat a "alt nivell', mitjançant "lletres de predicat". En altres situacions, de nivell mitjà o de baix nivell, utilitzarem notacions més descriptives de la propietat (nivell mitjà) o, fins i tot, la definició detallada (baix nivell), a través d'una fórmula de predicats. Per exemple, per "ser parell" podem fer servir per a a: $P(a)$ (lletra de predicat), $2|a$ (notació de divisibilitat), $\exists k(k \in \mathbb{Z} \wedge a = 2k)$ (definició de divisibilitat).

Vegem-ne alguns exemples.

Amb lletres de predicat:

PROBLEMA 5.15

Considereu l'afirmació:

"Hi ha exactament tres nens a la classe".

Proposeu algunes formalitzacions (simbolitzacions) utilitzant lletres de predicat.

Solució. Hi ha quantificadors (existencial).

Introduïm el predicat $N(x)$:="x és (un) nen". Conceptualment: "ser un nen". O bé encara alguna variant: "ser un nen de la classe".

$\exists x \exists y \exists z (N(x) \wedge N(y) \wedge N(z) \wedge \forall t (N(t) \rightarrow (t = x \vee t = y \vee t = z)))$.

$N(z) \wedge (x \neq y) \wedge (x \neq z) \wedge (y \neq z) \wedge$.

A partir d'aquesta fórmula, es poden escriure variants equivalents (utilitzem les equivalències lògiques de la doble negació, de De Morgan, i la negació del condicional):

$\exists x \exists y \exists z (N(x) \wedge N(y) \wedge N(z) \wedge \neg\neg \forall t (N(t) \rightarrow (t = x \vee t = y \vee t = z)))$ (doble negació)

$\exists x \exists y \exists z (N(x) \wedge N(y) \wedge N(z) \wedge \neg \exists t \neg (N(t) \rightarrow (t = x \vee t = y \vee t = z)))$ (negació de quantificadors)

$\exists x \exists y \exists z(N(x) \wedge N(y) \wedge N(z) \wedge \neg \exists t(N(t) \wedge \neg(t = x \vee t = y \vee t = z)))$ (negació del condicional)

$\exists x \exists y \exists z(N(x) \wedge N(y) \wedge N(z) \wedge \neg \exists t(N(t) \wedge (t \neq x \wedge t \neq y \wedge t \neq z)))$ (De Morgan)

Una altra variant deriva del contrarecíproc i de De Morgan:

$\exists x \exists y \exists z(N(x) \wedge N(y) \wedge N(z) \wedge \forall t(\neg(t = x \vee t = y \vee t = z) \rightarrow \neg N(t)))$ (contrarecíproc del condicional intern)

$\exists x \exists y \exists z(N(x) \wedge N(y) \wedge N(z) \wedge \forall t((t \neq x \wedge t \neq y \wedge t \neq z) \rightarrow \neg N(t)))$ (De Morgan).

Amb els tres nivells abans indicats:

PROBLEMA 5.16

Considereu l'enunciat:

"la suma de dos nombres parells és parell"

"si a i b són parells, aleshores $a+b$ és parell"

Proposeu diverses formalitzacions de l'enunciat.

Solució

a) *Amb lletres de predicat*. Denotem la propietat "ser parell" per P. Així, $P(x)$ significa "x és parell".

   Aleshores l'enunciat es pot formalitzar simplement per:

   $(P(a) \wedge P(b)) \rightarrow P(a+b)$.

   O també:

   $P(a) \rightarrow (P(b) \rightarrow P(a+b))$.

   $P(b) \rightarrow (P(a) \rightarrow P(a+b))$.

b) Fem servir la notació de divisibilitat, la que diu què és ser parell.

   $(2|a \wedge 2|b) \rightarrow 2|a+b$

   $2|a \rightarrow (2|b \rightarrow 2|a+b)$

   $2|b \rightarrow (2|a \rightarrow 2|a+b)$

c) Fem servir la definició de divisibilitat, expressada mitjançant una fórmula de predicat.

   $(\exists k(k \in \mathbb{Z} \wedge a = 2k) \wedge \exists k'(k' \in \mathbb{Z} \wedge b = 2k')) \rightarrow \exists k''(k'' \in \mathbb{Z} \wedge a+b = 2k'')$
   $(\exists k \in \mathbb{Z}(a = 2k) \wedge \exists k' \in \mathbb{Z}(b = 2k')) \rightarrow \exists k'' \in \mathbb{Z}(a+b = 2k''))$

La propietat de ser parell ja inclou la de ser enter. Ara bé, també es podria considerar un altre predicat, "ser enter", denotat per la lletra E, de manera que $E(x)$ significa "x és enter", o "$x \in \mathbb{Z}$". I aleshores tindríem:

$(P(a) \wedge E(a) \wedge P(b) \wedge E(b)) \to P(a+b)$, o bé

$(E(a) \wedge E(b)) \to ((P(a) \wedge P(b)) \to P(a+b))$

PROBLEMA 5.17

Es demana proposar una possible formalització dels enunciats en el llenguatge de predicats.

Expliciteu el domini de les variables a la mateixa fórmula. En podeu donar una versió sense incloure el domini a la fórmula. en podeu donar versions fent servir lletres de predicat. Indiqueu si la fórmula està quantificada i amb quin quantificador. Indiqueu si és generalitzable (amb quantificador universal).

a) *Siguin a i b nombres enters. Si a i b són senars, aleshores $a+b$ és parell.*
b) *La suma d'un nombre enter senar i d'un nombre enter parell és senar.*
c) *Per a tota parella x,y de nombres enters amb x senar i y parell, la suma $x+y$ és senar.*
d) *La suma de dos nombres enters senars és parell.*
e) *La suma de dos nombres enters parells qualssevol és parell.*
f) *Els quadrats dels nombres enters parells són parells.*
g) *Si n és enter i senar, n^3 és senar.*
h) *Per a tot nombre enter parell n, n^5 és parell.*
i) *Per a tot a,b nombres enters, on a és senar i b és parell, la diferència $a-b$ és senar.*
j) *Per a tot a,b nombres enters senars, el producte ab és senar*
k) *Si a,b són enters, ab és senar si ambdós ho són.*
l) *Si a,b són enters, ab és parell si algun d'ells ho és.*
m) *Si a,b són enters, ab és senar si a i b són senars.*
n) *El cub de qualsevol nombre enter senar és senar.*
o) *Sigui n un nombre enter senar qualsevol. Aleshores n^2 és senar.*
p) *Tot nombre real és de quadrat no negatiu.*
q) *El quadrat de tot nombre real no nul és positiu.*
r) *Per a tot $x,y \in \mathbb{R}$, si el producte xy és positiu, aleshores tenen el mateix signe.*
s) *Si el producte de tota parella de nombres reals és positiu, aleshores són del mateix signe.*

Solució. A partir de l'apartat *(b)*, a més de la solució que s'indica, són possibles altres solucions, com a l'apartat *(a)*.

a) $(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \to ((2 \nmid a \wedge 2 \nmid b) \to 2|a+b)$

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2 \nmid a \wedge 2 \nmid b) \to 2|a+b)$

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2 \nmid a \wedge 2 \nmid b) \to 2|a+b)$

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2 \nmid a) \to (2 \nmid b \to 2|a+b)$

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2 \nmid b) \to (2 \nmid a \to 2|a+b)$

$(2 \nmid a \wedge 2 \nmid b) \to 2|a+b$ $(\Omega = \mathbb{Z})$.

b) $(a \in \mathbb{Z} \wedge 2 \nmid a \wedge b \in \mathbb{Z} \wedge 2|b) \to 2 \nmid (a+b)$

c) Conjunt universal: $\Omega = \mathbb{Z}$

$\forall x \forall y((2 \nmid x \wedge 2 \nmid y) \to 2 \nmid (x+y)$

d) La fórmula no està quantificada, tot i que és generalitzable per un quantificador universal, atès que a i b són arbitraris

$(a \in \mathbb{Z} \wedge 2 \nmid a \wedge b \in \mathbb{Z} \wedge 2 \nmid b) \to 2|(a+b)$

e) La fórmula corresponent haurà de ser quantificada degut a "qualssevol"

$\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2|a \wedge 2|b) \to 2|a+b)$

f) És una afirmació quantificada i correspon a un condicional.

$\forall n((n \in \mathbb{Z} \wedge 2|n)) \to 2|n^2)$

$\forall n((n \in \mathbb{Z} \to (2|n \to 2|n^2))$

$\forall n \in \mathbb{Z}(2|n \to 2|n^2)$

$\forall n(2|n \to 2|n^2)$ $\Omega = \mathbb{Z}$

g) $(n \in \mathbb{Z} \wedge 2 \nmid n) \to 2 \nmid n^3$

h) $\forall n((n \in \mathbb{Z} \wedge 2|n)) \to 2|n^5)$

i) $\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \wedge 2 \nmid a \wedge 2|b) \to 2 \nmid (a-b))$

j) $\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \wedge 2 \nmid a \wedge 2 \nmid b) \to 2 \nmid ab)$

k) $(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \wedge 2 \nmid a \wedge 2 \nmid b) \to 2 \nmid ab$ $2 \nmid a \to (2 \nmid b \to 2 \nmid ab)$.

l) $(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \wedge (2|a \vee 2|b)) \to 2|ab$

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \to ((2|a \vee 2|b) \to 2|ab)$

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \to (2 \nmid ab \to (2 \nmid a \wedge 2 \nmid b))$ (equivalent)

m) $(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2 \nmid a \wedge 2 \nmid b) \to 2 \nmid ab$

n) $\forall n((n \in \mathbb{Z} \wedge 2 \nmid n)) \to 2 \nmid n^5)$

o) $\forall n((n \in \mathbb{Z} \wedge 2 \nmid n)) \to 2 \nmid n^2)$

p) $\forall x(x \in \mathbb{R} \to x \geq 0)$

$\forall x \in \mathbb{R}(x \geq 0)$

q) $\forall x((x \in \mathbb{R} \wedge x \neq 0) \to x > 0)$

r) $\forall x \forall y((x \in \mathbb{R} \wedge x \in \mathbb{R} \wedge xy > 0) \to ((x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)))$

s) $\forall x \forall y((x \in \mathbb{R} \wedge y \in \mathbb{R} \wedge xy > 0) \to ((x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)))$.

PROBLEMA 5.18

*Recordeu una frase famosa: "*You can fool all the people some of the time, and some of the people all the time, but you cannot fool all the people all the time*". Formalitzeu-la mitjançant una fórmula de predicats.*

Solució. Traduïm la frase: "Pots enganyar tothom alguna vegada, pots enganyar algú sempre, però no pots enganyar tothom sempre". Es por formular en impersonal: "Es pot enganyar tothom alguna vegada, es pot enganyar algú sempre, però no es pot enganyar tothom sempre". O bé "x pot enganyar tothom alguna vegada, x pot enganyar algú sempre, però x no pot enganyar tothom sempre".

En donem una resposta oberta, ateses les diverses possibilitats d'interpretació.

Suposem que és un x genèric el que enganya i formulem la frase per a un x abstracte (que fa el paper de "tu", "vosaltres", un qualsevol, pot ser una persona genèrica o altres). Després podrem particularitzar a un valor constant: "En Joan pot enganyar ...".

La frase és la conjunció de tres frases, que formalitzarem separadament, però amb els mateixos predicats.

Els predicats que escollim corresponen a les accions o situacions: ser persona, enganyar i ser en un temps. Concretament:

$P(r)$:="r és una persona (people)"

$E(a,b,s)$:="a enganya (pot enganyar) a b durant un temps s" (o en el temps s)

$T(s)$:="s és un temps (possibles tipus de temps: un instant, un període, una època, uns quants anys; no s'especifica)"

Considerem les frases "parcials":

Frase $F(x)$: x pot enganyar tothom alguna vegada (pots enganyar tothom alguna vegada)

Frase $G(x)$: x pot enganyar algú sempre (pots enganyar algú sempre)

Frase $H(x)$: x pot enganyar tothom sempre (pots enganyar tothom sempre)

La frase completa és $F(x) \wedge G(x) \wedge \neg H(x)$. Donem ara una formalització de cada frase parcial.

Frase $F(x)$: $\forall p(P(p) \to \exists t(T(t) \wedge E(x,p,t)))$

Frase $G(x)$: $\exists p(P(p) \wedge \forall t(T(t) \to E(x,p,t)))$

Frase $H(x)$: $\forall p(P(p) \to \forall t(T(t) \to E(x,p,t)))$

Per tant, finalment:

$$\forall p(P(p) \to \exists t(T(t) \wedge E(x,p,t))) \wedge \exists p(P(p) \wedge \forall t(T(t) \\ \to E(x,p,t))) \wedge \forall p(P(p) \to \forall t(T(t) \to E(x,p,t)))$$

Tot seguit, es pot considerar una versió impersonal:

Concretament:

$P(r)$:="r és una persona, people"

$F(b,s)$:="s'enganya (es pot enganyar) a la persona b durant un temps s" (o en el temps s)

$T(s)$:="s és un temps (possibles tipus de temps: un instant, un període, una època, uns anys; no s'especifica)"

Considerem les frases "parcials":

Frase A: *es pot* enganyar tothom alguna vegada (pots enganyar tothom alguna vegada)

Frase B: *es pot* enganyar algú sempre (pots enganyar algú sempre)

Frase C: *es pot* enganyar tothom sempre (pots enganyar tothom sempre)

La frase completa és $A \wedge B \wedge \neg C$. Formalització proposada:

Frase A: $\forall p(P(p) \to \exists t(T(t) \wedge F(p,t)))$

Frase B: $\exists p(P(p) \wedge \forall t(T(t) \to F(p,t)))$

Frase C: $\forall p(P(p) \to \forall t(T(t) \to F(p,t)))$

Per tant, finalment:

$$\forall p(P(p) \to \exists t(T(t) \wedge F(p,t))) \wedge \exists p(P(p) \wedge \forall t(T(t) \\ \to F(p,t))) \wedge \forall p(P(p) \to \forall t(T(t) \to F(p,t)))$$

PROBLEMA 5.19

"Tal que" es tradueix per "i" (conjunció).

Formalitzeu l'enunciat següent mitjançant una fórmula del llenguatge de predicats:

"Per a tot enter a existeix un enter b tal que, per a tot enter c, la relació $a < b$ implica $c-1 < a$"

Solució

$\forall a(a \in \mathbb{Z} \to \exists b(b \in \mathbb{Z} \land \forall c(c \in \mathbb{Z} \to (a < b \to c-1 < a))))$

Variants possibles:

Variant 1. Utilitzant l'equivalència $P \to (R \to S) \equiv (P \land R) \to S$:

$\forall a(a \in \mathbb{Z} \to \exists b(b \in \mathbb{Z} \land \forall c((c \in \mathbb{Z} \land a < b) \to c-1 < a))))$

Variant 2. Substituint $a < b \to c-1 < a$ pel contrarecíproc:

$\forall a(a \in \mathbb{Z} \to \exists b(b \in \mathbb{Z} \land \forall c(c \in \mathbb{Z} \to (\neg(c-1 < a) \to \neg(a < b)))))$
$\forall a(a \in \mathbb{Z} \to \exists b(b \in \mathbb{Z} \land \forall c(c \in \mathbb{Z} \to (c-1 \geq a \to a \geq b))))$

Si queda sobreentès el domini o universal de les variables ($\Omega = \mathbb{Z}$), resulta:

$\forall a \exists b \forall c(a < b \to c-1 < a)$

També podríem admetre una sintaxi no totalment estàndard (fórmula no generada per la gramàtica):

$\forall a \in \mathbb{Z}\ \exists b \in \mathbb{Z} \forall c \in \mathbb{Z}(a < b \to c-1 < a)$

PROBLEMA 5.20

Expresseu en llenguatge natural l'enunciat formalitzat com:

$\forall x(x \in \mathbb{R} \to x^2 \geq 0)$

Si suposem que l'universal és el conjunt dels nombres reals i no s'inclou a la fórmula, aleshores:

$\forall x(x^2 \geq 0)$

Solució. Es pot expressar de moltes maneres. Algunes són molt properes a la literalitat de la fórmula; d'altres, en són més llunyanes. Algunes són completament de llenguatge natural; d'altres són enunciats barreja de llenguatge natural i formalització. Vegem-ne algunes:

a) El quadrat de qualsevol nombre real és no negatiu.
b) Els quadrats dels nombres reals són no negatius.

c) Els nombres reals són de quadrat no negatiu.
d) El quadrat de cada nombre real és no negatiu.
e) El quadrat de tot nombre real és no negatiu.
f) El quadrat de qualsevol nombre real és no negatiu.
g) El quadrat d'un nombre real arbitrari és no negatiu.
h) Si x és un nombre real qualsevol, aleshores x^2 és no negatiu.
i) Per a tot nombre real x, $x^2 \geq 0$.
j) Per a qualsevol nombre real x, $x^2 \geq 0$.
k) Cada nombre real és de quadrat no negatiu.
l) Tot nombre real és de quadrat no negatiu.
m) Qualsevol nombre real és de quadrat no negatiu.
n) Per a cada nombre real x, és $x \geq 0$.
o) Si x és un nombre real arbitrari, $x^2 \geq 0$.

Diverses maneres de definir la propietat (predicat) "ser senar":

PROBLEMA 5.21

Definiu el predicat "ser senar" per a un nombre enter n (doneu-ne diverses versions).

Solució. Suposem que n és enter, de manera que l'universal és $\Omega = \mathbb{Z}$. No s'inclou a la definició ni a les fórmules. Se'n pot proposar una altra versió, amb inclusió del domini de n.

a) "no ser divisible per 2" (n no és divisible per 2)
b) $2 \nmid n$
c) existeix un nombre enter k tal que $n = 2k + 1$
d) existeix un nombre enter k tal que $n = 2k - 1$
e) existeix un nombre enter k per al qual $n = 2k + 1$
f) existeix $k \in \mathbb{Z}$ tal que $n = 2k + 1$
g) $n = 2k + 1$ per a un nombre enter k convenient
h) $n = 2k + 1$ per a un $k \in \mathbb{Z}$ convenient
i) $n = 2k + 1$ per a un nombre enter k adequat
j) $n = 2k + 1$ per a un cert nombre enter k
k) $n = 2k + 1$ per a algun nombre enter k
l) $\exists k(k \in \mathbb{Z} \wedge n = 2k + 1)$ (fórmula de predicat)
m) $\exists t(t \in \mathbb{Z} \wedge n = 2t - 1)$ (fórmula de predicat)
n) $\exists k(n = 2k + 1)$ (fórmula de predicat)
o) $\exists t(n = 2t - 1)$ (fórmula de predicat)

PROBLEMA 5.22

Doneu una fórmula de predicat per als predicats següents:

a) *"Ser parell", per a un nombre enter.*
b) *"Ser senar", per a un nombre enter.*
c) *"No ser senar", per a un nombre enter.*
d) *"Ser nombre primer", per a un enter.*
e) *"Ser nombre compost", per a un enter.*
f) *"Ser quadrat perfecte", per a un enter.*
g) *"No ser quadrat perfecte", per a un enter.*
h) *"Ser múltiple de 3", per a un enter.*
i) *"No ser múltiple d'enter", per a un enter.*

Solució

a) "Ser parell", per a un nombre enter. Per a $n \in \mathbb{Z}$:

$\exists k(k \in \mathbb{Z} \wedge n = 2k)$

$\exists k \in \mathbb{Z} n = 2k)$ (amb sintaxi menys estàndard)

$2|n$ (suposant que hem definit abans la relació de divisibilitat).

Així, si $P(n) :=$"n és parell", tenim

$P(n) := \exists k(k \in \mathbb{Z} \wedge n = 2k)$ o $P(n) := 2|n$.

b) "ser senar" (un nombre enter n):

$\exists k(k \in \mathbb{Z} \wedge n = 2k+1)$

$\exists k \in \mathbb{Z}(n = 2k+1)$

$\forall t(t \in \mathbb{Z} \to n \neq 2t)$

c) "No ser senar", per a un nombre enter n.

És ser parell. Alternativament, escrivim la negació de "ser senar":

$\neg\forall t(t \in \mathbb{Z} \to n \neq 2t)$

$\exists t \neg(t \in \mathbb{Z} \to n \neq 2t)$

$\exists t(t \in \mathbb{Z} \wedge \neg n \neq 2t)$

$\exists t(t \in \mathbb{Z} \wedge n = 2t)$

d) "Ser nombre primer", per a un enter n.

$p \in \mathbb{N} \wedge p \geq 2 \wedge \forall d((d \in \mathbb{N} \wedge d \geq 1 \wedge d|p) \rightarrow (d = 1 \vee d = p))$

Hi ha altres variants:

$p \in \mathbb{N} \wedge p \geq 2 \wedge \forall d((d \in \mathbb{N} \wedge d > 1 \wedge d|p) \rightarrow d = p))$

$p \in \mathbb{N} \wedge p \geq 2 \wedge \forall d((d \in \mathbb{N} \wedge d \geq 1 \wedge d|p \wedge d \neq p) \rightarrow d = 1))$

Atès que, d'inici, queda dit que p és enter, podríem escriure:

$p \geq 2 \wedge \forall d((d \in \mathbb{N} \wedge d \geq 1 \wedge d|p) \rightarrow (d = 1 \vee d = p))$

També podríem suprimir la pertinença al conjunt dels nombres naturals $d \in \mathbb{N}$ si queda sobreentès o es declara externament.

e) "Ser nombre compost", per a un enter n.

Convindrem que $n > 1$.

$\exists a \exists b(a \in \mathbb{N} \wedge b \in \mathbb{N} \wedge n = ab \wedge 1 < a < n \wedge 1 < b < n)$

Se'n poden escriure altres variants: escriure $1 < a < n$ com $(1 < a) \wedge (a < n)$. També tenim que una de les condicions $1 < a < n$, $1 < b < n$ és redundant: qualsevol d'elles es dedueix a partir de l'altra, aplicant $n = ab$.

És negació de "ser primer". La fórmula que hem escrit equival a la negació, però no és literalment la negació.

$p < 2 \vee \exists d((d \in \mathbb{N} \wedge d \geq 1 \wedge d|p) \wedge (d \neq 1) \wedge d \neq p)$

$p < 2 \vee \exists d(d \in \mathbb{N} \wedge d|p \wedge (d > 1) \wedge d < p)$

Així, $p = dd'$, amb $1 < d < p$, i anàlogament per a d'.

f) "Ser quadrat perfecte", per a un enter n.

$\exists k(k \in \mathbb{Z} \wedge n = k^2)$

g) "No ser quadrat perfecte", per a un enter n.

Neguem la propietat anterior:

$\neg \exists k(k \in \mathbb{Z} \wedge n = k^2)$

$\forall k \neg (k \in \mathbb{Z} \wedge n = k^2)$

$\forall k(\neg k \in \mathbb{Z} \vee \neg n = k^2)$

$\forall k(\neg k \in \mathbb{Z} \vee n \neq k^2)$

$\forall k(k \in \mathbb{Z} \rightarrow n \neq k^2)$

h) "Ser múltiple de 3", per a un enter n.

$\exists q(q \in \mathbb{Z} \wedge n = 3q)$

i) "No ser múltiple de 3", per a un enter n.

Negació de l'anterior:

$\neg\exists q(q \in \mathbb{Z} \wedge n = 3q)$

$\forall q \neg(q \in \mathbb{Z} \wedge n = 3q)$

$\forall q(\neg q \in \mathbb{Z} \vee \neg n = 3q)$

$\forall q(\neg q \in \mathbb{Z} \vee n \neq 3q)$

$\forall q(q \in \mathbb{Z} \rightarrow n \neq 3q)$

Es pot expressar d'una altra manera si tenim en compte la divisió entera de n entre 3:

$\exists q(q \in \mathbb{Z} \wedge (n = 3q+1 \vee n = 3q+2))$

$\exists q(q \in \mathbb{Z} \wedge n = 3q+1) \vee \exists p(p \in \mathbb{Z} \wedge n = 3p+2)$

$\exists q \exists r((q \in \mathbb{Z} \wedge r \in \mathbb{N} \wedge n = 3q+r) \rightarrow (r = 1 \vee r = 2))$

$\exists q \exists r((q \in \mathbb{Z} \wedge r \in \mathbb{N} \rightarrow (n = 3q+r \rightarrow (r = 1 \vee r = 2)))$

PROBLEMA 5.23

Es tracta de formalitzar un predicat binari (2–ari) per a nombres enters (relació simètrica). Siguin a i b nombres enters. La paritat és la propietat de ser parell o senar (dicotomia) (a $\mathbb{Z}$).

a) Expresseu en una fórmula de predicats la relació:

"ser de la mateixa paritat"

"a i b són de la mateixa paritat"

"a i b tenen la mateixa paritat"

"a és de la mateixa paritat que b"

"a i b són ambdós parells o ambdós senars"

b) Expresseu en una fórmula de predicats la relació:

"ser de paritat diferent"

Solució

a) *Resposta 1*. Podem expressar la propietat de ser a, b de la mateixa paritat amb:

$(2|a \wedge 2|b) \vee (2 \nmid a \wedge 2 \nmid b)$

Així:

a, b són de la mateixa paritat $\Leftrightarrow (2|a \wedge 2|b) \vee (2 \nmid a \wedge 2 \nmid b)$.

Resposta 2. Si és $M(a,b) := ((2|a \wedge 2|b) \vee (2 \nmid a \wedge 2 \nmid b))$.

Resposta 3. Més abstractament, si $P(x)$ és el predicat "ser parell" i $S(x)$ és el predicat "ser senar", aleshores es pot expressar amb lletres de predicat:

$(P(a) \wedge P(b)) \vee (S(a) \wedge S(b))$

Resposta 4. Hi ha d'altres possibilitats, com per exemple: $2|a+b$, que és equivalent a ser a, b de la mateixa paritat.

b) Que siguin de paritat diferent es pot expressar de diverses maneres equivalents:

- exactament un és parell (i, per tant, l'altre és senar)
- exactament un és senar (i, per tant, l'altres és parell)
- un és parell i l'altre, senar.

Resposta 1. Formalment:

$(2|a \wedge 2 \nmid b) \vee (2 \nmid a \wedge 2|b)$

Resposta 2. En termes de lletres de predicat:

$(P(a) \wedge S(b)) \vee (S(a) \wedge P(b))$ (de l'apartat (a)).

Resposta 3. Hi ha altres possibilitats, com per exemple: $2 \nmid a+b$, que és equivalent a ser a, b de paritats diferents.

Resposta 4. També òbviament es pot escriure com a negació de "ser de la mateixa paritat":

$\neg((2|a \wedge 2|b) \vee (2 \nmid a \wedge 2 \nmid b))$

Com a exercici de tècnica demostrativa, vegem que és equivalent a

$(2|a \wedge 2 \nmid b) \vee (2 \nmid a \wedge 2|b)$.

En efecte:

$\neg((2|a \wedge 2|b) \vee (2 \nmid a \wedge 2 \nmid b))$
$\equiv \neg(2|a \wedge 2|b) \wedge \neg(2 \nmid a \wedge 2 \nmid b)$ (per De Morgan)

$\equiv \neg(2|a) \vee \neg(2|b)) \wedge (\neg(2 \nmid a) \vee \neg(2 \nmid b)$ (per De Morgan)

$\equiv (2 \nmid a \vee 2 \nmid b) \wedge (2|a \vee 2|b)$ (per doble negació)

$\equiv [(2 \nmid a \vee 2 \nmid b) \wedge 2|a] \vee [(2 \nmid a \vee 2 \nmid b) \wedge 2|b]$ (distributivitat de $\wedge$ respecte de $\vee$)

$\equiv [(2 \nmid a \wedge 2|a) \vee (2 \nmid b \wedge 2|a)] \vee [(2 \nmid a \wedge 2|b) \vee (2 \nmid b \wedge 2|b)]$ (distributivitat de $\wedge$ respecte de $\vee$)

$\equiv [\mathbb{F} \vee (2 \nmid b \wedge 2|a)] \vee [(2 \nmid a \wedge 2|b) \vee \mathbb{F}]$ (contradicció)

$\equiv [(2 \nmid b \wedge 2|a)] \vee [(2 \nmid a \wedge 2|b)]$ (per $\mathbb{F} \vee A \equiv A$)

PROBLEMA 5.24

Formalitzeu "Tot enter de la forma $4n+1$ és primer". Observeu que no estem afirmant que sigui cert ni que sigui fals: només volem una formalització de l'enunciat en el llenguatge de predicats.

Solució. Hi ha diverses variants possibles:

$\forall n(n \in \mathbb{Z} \to 4n+1 \text{ és primer})$

$\forall n \in \mathbb{Z}(4n+1 \text{ és primer})$

$\forall n(4n+1 \text{ és primer})$ (domini sobreentès: $\Omega = \mathbb{Z}$)

$\forall m((m \in \mathbb{Z} \wedge \exists n(n \in \mathbb{Z} \wedge m = 4n+1) \to m \text{ és primer})$

PROBLEMA 5.25

Considerem les proposicions següents, referides a elements del conjunt A:

a) $\exists x \forall y(xy > 0)$ $(A = \mathbb{Z})$

b) $\exists x \forall y(xy = 0)$ $(A = \mathbb{Z})$

c) $\forall x \exists y(xy > 0)$ $(A = \mathbb{Z})$

d) $\forall x \forall y(xy > 0)$ $(A = \mathbb{Z})$

e) $\exists x \exists y(xy > 0)$ $(A = \mathbb{Z})$

f) $\exists x \exists y(xy = x)$ $(A = \mathbb{Z})$

g) $\exists x \forall y(xy = x)$ $(A = \mathbb{Z})$

h) $\forall y \exists x(xy = x)$ $(A = \mathbb{Z})$

A) Digueu si són certes o falses les afirmacions anteriors, i justifiqueu-ne les respostes.

B) Negueu les fórmules (no s'accepta $\neg$ a l'esquerra de la fórmula).

C) Digueu si són certes o falses les negacions anteriors, i justifiqueu-ne les respostes.

Es pot escriure alternativament. Per exemple, per a la primera (i, anàlogament, per a les altres):

$\exists x \in A \forall y \in A(xy > 0)$

$\exists x(x \in A \wedge \forall y(y \in A \to xy > 0))$

Solució

a) $\exists x \forall y(xy > 0)$ $(A = \mathbb{Z})$

No és cert.

Si $x = 0$, és $xy = 0$ per a tot y. Si $x > 0$, aleshores $xy < 0$ per a tot $y < 0$. Per a $x < 0$, és $xy < 0$ per a tot $y > 0$. Per tant, per a tot x, existeix algun y tal que $xy \not> 0$.

Negació de la fórmula:

$\neg \exists x \forall y(xy > 0)$

$\forall x \neg \forall y(xy > 0)$

$\forall x \exists y \neg(xy > 0)$

$\forall x \exists y(xy \not> 0)$

$\forall x \exists y(xy \leq 0)$

És certa la negació. L'argumentació que s'ha fet abans s'hauria pogut fer aquí, estudiant els casos possibles ($x = 0$, $x > 0$, $x < 0$).

b) $\exists x \forall y(xy = 0)$ $(A = \mathbb{Z})$

Cert. Amb $x = 0$ es compleix l'afirmació.

Per tant, la negació és falsa:

$\neg \exists x \forall y(xy = 0)$

$\forall x \neg \forall y(xy = 0)$

$\forall x \exists y \neg(xy = 0)$

$\forall x \exists y(xy \neq 0)$

Ja s'ha deduït que la negació és falsa, perquè és negació d'una afirmació certa. Ara bé, sense aquests antecedents, podem provar directament la falsedat de $\forall x \exists y(xy \neq 0)$; n'hi ha prou d'aportar un contraexemple: $x = 0$.

c) $\forall x \exists y(xy > 0)$ $(A = \mathbb{Z})$

No és cert: vegeu $x = 0$. És certa la negació:

$\neg \forall x \exists y(xy > 0)$

$\exists x \neg \exists y(xy > 0)$

$\exists x \forall y \neg(xy > 0)$

$\exists x \forall y(xy \not> 0)$

En canvi, si $A = \mathbb{Z} - \{0\}$, aleshores és cert. Per a $x > 0$, amb qualsevol $y > 0$ es compleix la desigualtat; per a $x < 0$, es compleix amb tot $y < 0$.

d) $\forall x \forall y (xy > 0)$ $(A = \mathbb{Z})$

No és cert, n'hi ha prou a agafar $x = 0$ o $y = 0$. O també, per a un $x < o$, considerar $y > 0$, i viceversa (xy de signe diferent).

És certa la negació:

$\neg \forall x \forall y (xy > 0)$

$\exists x \neg \forall y (xy > 0)$

$\exists x \exists y \neg (xy > 0)$

$\exists x \exists y (xy \leq 0)$

En canvi, si $A = \mathbb{N} - \{0\}$, aleshores l'afirmació és certa.

e) $\exists x \exists y (xy > 0)$ $(A = \mathbb{Z})$

Cert. N'hem d'aportar l'exemple corresponent. Per exemple, per a x, y no nuls del mateix signe.

La negació és falsa:

$\neg \exists x \exists y (xy > 0)$

$\forall x \neg \exists y (xy > 0)$

$\forall x \forall y \neg (xy > 0)$

$\forall x \forall y (xy \leq 0)$. Contraexemple: qualsevol x, y positius (per exemple $x = 3$, $y = 2$).

És falsa perquè és la negació d'una afirmació certa. Però també directament es pot veure:

f) $\exists x \exists y (xy = x)$ $(A = \mathbb{Z})$

Cert. Per exemple, per a $x = 0$ o $y = 1$. Per tant, la negació serà falsa, per bé que també es podria veure directament.

Negació: $\forall x \forall y (xy \neq x)$. És fals. Contraexemple: $x = 1$, $y = 1$. O bé $x = 0$, y qualsevol.

g) $\exists x \forall y (xy = x)$ $(A = \mathbb{Z})$. És cert, amb $x = 0$.

Per tant, la negació és falsa:

$\neg \exists x \forall y (xy = x)$

$\forall x \neg \forall y (xy = x)$

$\forall x \exists y \neg (xy = x)$

$\forall x \exists y (xy \neq x)$ (no és cert amb $x = 0$).

Amb $A = \mathbb{Z} - \{0\}$, l'afirmació seria falsa, ja que només hi hauria un valor de y que satisfés la relació: $y = 1$, cosa que contradiu que és per a tot y.

h) $\forall y \exists x (xy = x)$ $(A = \mathbb{Z})$

Cert amb $x = 0$, vàlid per a qualsevol y. Per tant, la negació és falsa:

$\neg \forall y \exists x (xy = x)$

$\exists y \neg \exists x (xy = x)$

$\exists y \forall x \neg (xy = x)$

$\exists y \forall x (xy \neq x)$

Vegem directament que no és certa (*per reducció a l'absurd*). Si fos certa i, per tant, existís y_0 tal que $xy_0 \neq x$, per a tota x, aleshores $xy_0 - x \neq 0$, és a dir, $x(y_0 - 1) \neq 0$, d'on, en particular, $x \neq 0$. Per tant, no podria ser per a tot x, contradicció. Per tant, $\exists y \forall x (xy \neq x)$ no és certa.

5.6.2. Anàlisi d'enunciats. Quantificadors i condicionals ocults

Els enunciats de matemàtiques i d'altres àrees es formulen de diverses maneres pel que fa al grau de formalització. Als texts, es poden observar diversos estadis de formalització, que van des de la formulació donada completament en termes del llenguatge natural, passant per diversos estadis intermedis de formalització creixent, fins a la formalització o simbolització completa, en termes d'una fórmula de predicats, sense llenguatge natural.

Els avantatges d'una fórmula de predicats són la precisió i l'exactitud; l'inconvenient és la possible poca llegibilitat (per als humans, però no per a un programa, per exemple). En canvi, en una formulació completament en llenguatge natural, la llegibilitat pot ser màxima per als humans (si no és molt complicada), però no per a un programa.

Amb llenguatge natural, de vegades no és totalment clar què diu exactament l'enunciat en una primera lectura, sinó que cal analitzar-lo curosament. Pot passar que la frase sigui altament desordenada, que calgui adreçar-la i, moltes vegades, extreure'n o posar de manifest la seva estructura lògica, que pot estar amagada, i si hi ha quantificadors implícits o ocults, o condicionals. És un exercici interessant veure què diuen (exactament) els enunciats. Farem una anàlisi de l'estructura lògica d'alguns enunciats (formulats en llenguatge natural).

Vegem-ne alguns exemples, amb els qual farem molt detalladament la progressió cap a diversos enunciats de formalització o simbolització creixent:

Exemple 5.48 [simbolització o formalització: del llenguatge natural a la fórmula de predicats] Considerem la frase: "Les cireres no són taronges". És una frase de nivell imprecís, pel to generalitzant. En podem millorar la precisió per tal d'expressar-la en termes d'estructura lògica i de quantificació. De fet, són aspectes lògics implícits o amagats, com es veurà:

Estadi 1 de simbolització: 100 % llenguatge natural, 0 % formalització

En dir "les" (les cireres), estem dient que l'afirmació val per a tota cirera, per a totes les cireres, per a qualsevol cirera, per a una cirera arbitrària; és l'estructura exterior de la fórmula, la quantificació universal; és un aspecte que no queda completament explicitat en el llenguatge.

"Tota cirera no és una taronja"

"Qualsevol cirera no és una taronja"

"Cap cirera és una taronja"

"Cada cirera no és una taronja"

Internament, a la fórmula hem de dir què s'afirma per a una cirera arbitrària, però fixa pel que fa a l'afirmació que sigui: "una cirera no és una taronja". Es pot expressar com un condicional, que hi estava "ocult":

"Si un objecte és una cirera, aleshores no és una taronja" (amb quantificador)

"Per a tot objecte que sigui una cirera, aleshores no és una taronja"

"Per a tot objecte, si és una cirera, aleshores no és una taronja"

En aquest estadi, desenredem la frase, l'endrecem, n'identifiquem part de l'estructura lògica.

Estadi 2 de simbolització. Semiformalització (1): introduïm variables.

Aquestes expressions anteriors comencen a fer-se artificioses. Convé introduir-hi notació, com a mínim variables: "x" per a una cirera qualsevol, que ens permetrà construir frases amb més comoditat i progressar cap a la simbolització. Així, tindrem:

"Per a tota cirera x, x no és una taronja"

"Per a qualsevol cirera x, x no és una taronja"

"Per a cada cirera x, x no és una taronja"

"Per a una cirera qualsevol x, x no és una taronja"

"Per a tota x, si x és una cirera, aleshores x no és una taronja"

"Si x és una cirera qualsevol, aleshores x no és una taronja"

"Si x és una cirera arbitrària, aleshores x no és una taronja".

Estadi 3 de simbolització. Semiformalització (2): avancem en la simbolització.

Avancem en la formalització utilitzant connectives i quantificadors. El nucli de l'afirmació és el condicional:

"Si x és una cirera, aleshores x no és una taronja", que podem simbolitzar amb:

"x és una cirera $\rightarrow$ x no és una taronja".

Amb quantificador universal (per al “qualsevol”),

“Per tota x, (x és una cirera $\to$ x no és una taronja)”

“Per tota x, x és una cirera $\to$ x no és una taronja”

“$\forall x$ (x és una cirera $\to$ x no és una taronja)”

Estadi 4 de simbolització. Simbolització completa: 0 % llenguatge natural, 100 % formalització:

Escollint les lletres de predicat següents:

C “ser cirera”: $C(x)$ és “x és una cirera” o, simplement, “x és cirera”.

T “ser taronja”: $T(x)$ és “x és una taronja” o, simplement, “x és taronja”.

Aleshores:

“Per a tota x, ($C(x) \to \neg T(x)$)”

Simbolització completa:

$$\forall x(C(x) \to \neg T(x))$$

Versió 2. Podem substituir $C(x) \to \neg T(x)$ per l’equivalent contrarecíproc, $\neg\neg T(x) \to \neg C(x)$, que equival a $T(x) \to \neg C(x)$.
I així tenim una alternativa equivalent:

$$\forall x(T(x) \to \neg C(x)) \,.$$

Correspondria equivalentment a l’enunciat: “Les taronges no són cireres”. ■

Exemple 5.49 Considerem l’enunciat: “Els quadrats dels nombres enters senars són senars”.

És una afirmació per a *tots* els nombres enters? Sí, per “dels”. La frase és substituïble per:

“El quadrat *dels* nombres enters senars és senar”

És un cas de quantificador ocult per l’estructura de la frase. És una frase altament desendreçada. N’anirem desenredant l’estructura. Es pot explicitar més i fer-hi aparèixer el caràcter d’expressió quantificada, amb frases equivalents:

“El quadrat de *tot* nombre enter senar és senar”

“El quadrat de *qualsevol* nombre enter senar és senar”

“El quadrat d’un nombre enter senar *qualsevol* és senar”

“El quadrat de *cada* nombre enter senar és senar”

Des d'un punt de vista lògic, la frase està capgirada, ja que comença per la conclusió o tesi ("a l'inrevés"). Tenim aquí un condicional "amagat"; la frase es clarifica:

"Per a tot/qualsevol enter senar, el quadrat és senar". "Per a cada enter senar, el quadrat és senar" "Per a un nombre enter senar arbitrari, el quadrat és senar".

Millor encara: "*Si* un nombre enter qualsevol és senar, *aleshores* el quadrat és senar", on s'explicita el condicional ocult.

No considerant *de moment* les parts de la frase: "qualsevol", "per a cada ...", "per a tot ...", tenim una estructura interna condicional:

"Si un nombre enter és senar, aleshores el seu quadrat és senar".

Posteriorment, quantifiquem amb "per a tot".

Per tant, l'estructura global és clara: generalització d'un condicional.

Procedim ara a la formalització o simbolització, és a dir, a transcriure l'afirmació del llenguatge ordinari a una fórmula de predicats. Suposem, en primera instància, que totes les variables són enteres ($\Omega = \mathbb{Z}$) i que no cal indicar-ho a la fórmula.

Hem d'introduir una variable, n, nombre enter; és imprescindible per a la simbolització i permetrà avançar; també aclarirà l'enunciat, que anirà quedant més nítid.

Aleshores tenim una primera possibilitat, encara poc formalitzada:

"Si n és un enter senar, aleshores n^2 és un enter senar"

Generalització:

"Si n és un enter senar qualsevol, aleshores n^2 és un enter senar"

"Per a tot n que sigui enter senar, n^2 és un enter senar"

"Per a tot n enter senar, n^2 és un enter senar".

Expressem formalment la propietat de ser senar (enter) en termes de no-divisibilitat per 2, avançant en la simbolització:

"si $2 \nmid n$, aleshores $2 \nmid n^2$"

"per a tot n tal que $2 \nmid n$, $2 \nmid n^2$"

"si n és un enter qualsevol tal que $2 \nmid n$, és $2 \nmid n^2$

Introduïm la connectiva del condicional, progressant en la simbolització:

$2 \nmid n \rightarrow 2 \nmid n^2$

Finalment, generalitzem:

$\forall n(2 \nmid n \rightarrow 2 \nmid n^2)$.

Alternativament, ara indicant la pertinença al conjunt dels enters:

$\forall n((n \in \mathbb{Z} \wedge 2 \nmid n) \to 2 \nmid n^2)$.

$\forall n \in \mathbb{Z}(2 \nmid n \to 2 \nmid n^2)$.

$\forall n(n \in \mathbb{Z} \to (2 \nmid n \to 2 \nmid n^2))$. ■

Exemples 5.50

Exemple 1. "La suma de dos nombres enters senars qualssevol és un nombre parell"

Adrecem la frase de manera que segueixi l'ordre d'un condicional, amb quantificació final.

1. Universal: $\Omega = \mathbb{Z}$
2. Variables: a, b
3. Predicats: "x divideix y" ($x|y$, $D(x,y)$).
4. Estructura condicional: $(2 \nmid a \wedge 2 \nmid b) \to 2|(a+b)$,$((\alpha \wedge \beta) \to \gamma)$
5. Quantificació: $\forall a \forall b(2 \nmid a \wedge 2 \nmid b) \to 2|(a+b)$.

Estructura:

$\forall a \forall b((\neg D(2,a) \wedge \neg D((2,b)) \to D(2,a+b))$

$\forall a \forall b((\neg D(2,a) \wedge \neg D((2,b)) \to D(2,s(a,b)))$ (s, suma). ■

Exemple 2. "La suma de dos nombres enters parells qualssevol és un nombre parell"

Adrecem la frase de manera que segueixi l'ordre d'un condicional, amb quantificació final.

1. Universal: $\Omega = \mathbb{Z}$
2. Variables: a, b
3. Predicats: "x divideix y" ($x|y$, $D(x,y)$)
4. Estructura condicional: $(2|a \wedge 2|b) \to 2|(a+b)$,$((\alpha \wedge \beta) \to \gamma)$
5. Quantificació: $\forall a \forall b(2|a \wedge 2|b) \to 2|(a+b)$.

Estructura:

$\forall a \forall b((D(2,a) \wedge D((2,b)) \to D(2,a+b))$

$\forall a \forall b((D(2,a) \wedge D((2,b)) \to D(2,s(a,b)))$ (s, suma). ■

Exemple 5.51 Un altre tipus d'anàlisi és el que es fa sobre l'estructura d'una *fórmula de predicats* amb la qual enunciem una propietat, per finalment acabar enunciant-la en llenguatge natural segons diverses versions possibles.

Inicialment:

$\forall a \forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$ (a, b enters, sobreentès).

Finalment:

"El producte de dos nombres enters senars qualssevol és senar" (comença pel final, per la conclusió).

Convé desfer el camí que s'ha seguit en els altres exemples:

1. Univers de discurs: $\Omega = \mathbb{Z}$
2. Variables: enters a, b ($a, b \in \mathbb{Z}$)
3. Predicats: ser senar ($2 \nmid n$)
4. Quantificació universal de les dues variables: $\forall a \forall b(\ldots)$
5. Propietat nuclear $(2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab$: si a, b són senars, el seu producte també ho és (és un condicional $\alpha \rightarrow \beta$)

   "El producte de dos nombres enters senars és senar"
6. Generalitzant (pel quantificador universal): "El producte de dos nombres enters senars qualssevol és senar".

   "Per a cada parella de nombres enters senars, el seu producte és senar" És senar el producte de dos nombres enters senars qualssevol". ■

5.7. Qüestions i exemples diversos

Aquesta secció consta d'exercicis i qüestions variades, entre les quals:

a) definició de predicats

b) descripció de predicats per fórmules de predicat

c) exercicis de traducció en els dos sentits:

   i) formalització: del llenguatge natural al llenguatge formal (fórmules de predicat)

   ii) desformalització: del llenguatge formal (fórmules de predicat) al llenguatge natural.

15 Proposeu exemples de predicats. Proposeu exemples d'ús en fórmules de predicats.

15* *Resposta:*

a) "ser home" (concepte)

– és home (ús).

$H(x)$:="x és home" (notació funcional amb variables).

$H(Pere)$ simbolitza "en Pere és home" (ús amb constant).

$\forall x(H(x) \to M(x))$ (ús en una fórmula de predicat).

b) ser ric – és ric x és ric $R(x) :=$ "x és ric".
c) anar amb tren – va amb tren
d) tocar el piano – toca el piano
e) ser més gran que – és més gran que – $G(x,y) :=$ "x és més gran que y".
f) "ser més vell que"

16 Indiqueu si la fórmula següent és una fórmula del llenguatge de proposicions:

$$\forall x \exists y(P(x,y) \to (\neg Q(x,y) \wedge (R(x,y) \to (S(x,y) \vee T(x,y)))))$$

16⋆ *Resposta:* No, és del llenguatge de predicats.

17 Per al predicat $P(x)$, on x pertany al conjunt universal U, quins enunciats es generen si $U = \{u_1, u_2, u_3\}$?

17⋆ *Resposta:* $P(u_1), P(u_2), P(u_3)$

18 Expresseu el quantificador:

a) existencial $\exists$ en termes de $\forall$ i $\neg$ b) universal $\forall$ en termes de $\exists$ i $\neg$

18⋆ *Resposta:*

a) $\exists x P(x) \equiv \neg \forall x \neg P(x)$
En efecte, $\exists x P(x) \equiv \neg\neg \exists x P(x) \equiv \neg \forall x \neg P(x)$.
b) $\forall x P(x) \equiv \neg \exists x \neg P(x)$
En efecte, $\neg \exists x \neg P(x) \equiv \forall x \neg\neg P(x) \equiv \forall x P(x)$.

19 Es podria construir un llenguatge de predicats amb només un dels quantificadors $\exists, \forall$?

19⋆ *Resposta:* Sí, ja que cada un d'ells es pot expressar mitjançant l'altre i la negació $\neg$.

$\exists x P(x) \equiv \neg \forall x \neg P(x)$

$\forall x P(x) \equiv \neg \exists x \neg P(x)$

20 Proposeu fórmules de predicats per a expressar les propietats de les operacions aritmètiques de la suma en $\mathbb{R}$:

a) propietat associativa de la suma.
b) propietat commutativa de la suma.
c) existència d'element neutre 0 per a la suma.
d) existència d'oposat de qualsevol nombre real respecte de la suma.

20* *Resposta:*

a) $\forall x \forall y \forall z(x+(y+z)=(x+y)+z)$

$\forall x \forall y \forall z((x \in \mathbb{R} \wedge y \in \mathbb{R} \wedge z \in \mathbb{R}) \rightarrow x+(y+z)=(x+y)+z)$

Hi ha altres variants de sintaxi menys estàndard o més informal:

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

$\forall x \forall y \forall z(x+(y+z)=(x+y)+z)$ $(\Omega 0=\mathbb{R})$

$(x+(y+z)=(x+y)+z), \forall x \forall y \forall z$ (i altres variants)

b) $\forall x \forall y(x+y=y+x)$

c) $\forall x(x+0=x \wedge 0+x=x)$ (indicant explícitament quin és l'element neutre)

$\exists x_0 \forall w(w+x_0=w \wedge x_0+w=w)$ (sense explicitar l'element neutre)

d) $\forall x \exists x'(x+x'=0 \wedge (x'+x=0))$ (sense especificar quin és).

21 Proposeu fórmules de predicats per a expressar les propietats de les operacions aritmètiques del producte en

a) propietat associativa del producte
b) propietat commutativa del producte
c) propietat d'existència d'element neutre 1 per al producte
d) existència d'oposat (invers, recíproc) de qualsevol nombre real no nul respecte del producte
e) propietat distributiva del producte respecte de la suma

21* *Resposta:* És similar a l'anterior sobre la suma. Escrivim només el relatiu a l'existència d'invers:

$\forall x(x \neq 0 \rightarrow \exists x'(xx'=1 \wedge x'x=1))$.

22 Proposeu fórmules de predicats per a expressar diverses fórmules en relació amb les operacions aritmètiques de suma i producte en $\mathbb{R}$ (que queda sobreentès) (només algunes variants possibles):

a) quadrat de la suma
b) quadrat de la diferència
c) suma per diferència

22* *Resposta:*

a) $\forall x \forall y((x+y)^2=x^2+2xy+y^2)$

$\forall x \forall y((x \in \mathbb{R} \wedge y \in \mathbb{R}) \rightarrow (x+y)^2=x^2+2xy+y^2)$

b) $\forall x \forall y((x-y)^2=x^2-2xy+y^2)$

c) $\forall x \forall y((x+y)(x-y)=x^2-y^2)$

23 Formalitzeu: "La suma de dos nombres enters consecutius qualssevol és senar" ($\Omega = \mathbb{R}$).

23* *Resposta:* L'afirmació "La suma de dos nombre enters consecutius qualssevol és senar" es formalitza de diverses maneres:

$\forall n(2 \not| (n+(n+1)))$
$\forall n \forall k(2 \not| ((n+k)+(n+k+1)))$
$\forall n \forall k((a = n+k \wedge b = n+k+1) \to 2 \not| a+b)$
$\forall n \forall k((n \in \mathbb{Z} \wedge k \in \mathbb{Z} \wedge a = n+k \wedge b = n+k+1) \to 2 \not| a+b)$
$\forall n,k \in \mathbb{Z}((a = n+k \wedge b = n+k+1) \to 2 \not| a+b)$
$\forall a \forall b((a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge b = a+1) \to 2 \nmid a+b)$

i altres variants. A les dues primeres, resulta sobreentès que el domini o universal és $\mathbb{Z}$, o bé s'ha de declarar a part de la fórmula.

24 Considereu diversos enunciats. Tots diuen el mateix? Feu-ne formulacions verbals:

$$\forall n((n \in \mathbb{N} \wedge n \geq 1) \longrightarrow 1+2+\cdots+n \;=\; \frac{n(n+1)}{2})$$

$$\forall n(n \in \mathbb{N} \to (n \geq 1 \longrightarrow 1+2+\cdots+n \;=\; \frac{n(n+1)}{2}))$$

$$\forall n \in \mathbb{N}(n \geq 1 \longrightarrow 1+2+\cdots+n \;=\; \frac{n(n+1)}{2})$$

$$\forall n((n \in \mathbb{N} \wedge n \geq 1) \longrightarrow \textstyle\sum_{k=1}^{n} k \;=\; \displaystyle\frac{n(n+1)}{2})$$

24* *Resposta:* Tots diuen el mateix. Hi ha diverses possibilitats de descripció verbal:

Per a tot nombre natural $n \geq 1$, es compleix $1+2+\cdots+n = \frac{n(n+1)}{2}$.

Sigui n un nombre natural qualsevol, amb $n \geq 1$ (o: tal que $n \geq 1$). Aleshores:

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

Sigui n un nombre natural qualsevol. Si $n \geq 1$, aleshores $1+2+\cdots+n = \dfrac{n(n+1)}{2}$.

Per a tot nombre natural $n \geq 1$, es compleix $1+2+\cdots+n = \dfrac{n(n+1)}{2}$.

Per a tot nombre natural n, si $n \geq 1$, $1+2+\cdots+n = \dfrac{n(n+1)}{2}$.

Sigui n un nombre natural no nul qualsevol. Aleshores $1+2+\cdots+n = \dfrac{n(n+1)}{2}$.

Sigui n un nombre natural no nul arbitrari. Aleshores $1+2+\cdots+n = \dfrac{n(n+1)}{2}$.

La igualtat $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ és vàlida per a tot nombre natural $n \geq 1$.

25 Expresseu en llenguatge natural:

a) $\forall n((n \in \mathbb{Z} \wedge 2|n) \to 2 \not| 2n^2+5n+3)$
b) $\forall n((n \in \mathbb{Z} \wedge 2 \not| n) \to 4|11n^2-7)$
c) $\forall n((n \in \mathbb{Z} \wedge 2|n^2+3n) \to 2|n)$
d) $\forall n(n \in \mathbb{Z} \to (2|n^2+3n \to 2|n))$
e) $(\forall n \in \mathbb{Z})(2|n^2+3n \to 2|n)$
f) $\forall n\ (n \in \mathbb{N} \wedge 2|(n^3-n+1))$
g) $\forall x \in \mathbb{N} \forall n \in \mathbb{N}(n \geq 2 \to (2|x^n) \leftrightarrow 2|x))$
h) $\forall x \forall n((x \in \mathbb{N} \wedge n \in \mathbb{N} \wedge n \geq 2) \to (2|x^n) \leftrightarrow 2|x))$
i) $\forall n((n \in \mathbb{N} \wedge n \geq 4) \to n! > 2^n)$

$\forall n(n \in \mathbb{N} \to (n \geq 4 \to n! > 2^n))$

$\forall n \in \mathbb{N}(n \geq 4 \to n! > 2^n)$

j) $\forall x \forall n((x \in \mathbb{R} \wedge x > -1 \wedge n \in \mathbb{Z} \wedge n > 0) \to (1+x)^n \geq 1+nx)$
k) $\forall x((x \in \mathbb{Z}) \to (2 \not| 5x-7) \to 2|9x+2)$

$\forall x((x \in \mathbb{Z}) \wedge (2 \not| 5x-7)) \to 2|9x+2)$

25* *Resposta:*

a) Si n és un enter parell qualsevol, aleshores $2n^2+5n+3$ és senar.
b) Per a cada enter senar n, l'enter $11n^2-7$ és divisible per 4.
c) Sigui $n \in \mathbb{Z}$ un nombre enter qualsevol. Si n^2+3n és parell, aleshores n és parell.
d) Sigui $n \in \mathbb{Z}$ un nombre enter qualsevol. Si n^2+3n és parell, aleshores n és parell.
e) Sigui $n \in \mathbb{Z}$ un nombre enter qualsevol. Si n^2+3n és parell, aleshores n és parell.
f) Per a tot nombre enter n, n^3-n+1 és parell.
g) Per a tot $x \in \mathbb{N}$ i per a tot enter $n \geq 2$, x^n és parell si, i només si, x és parell.

Siguin x, n enters qualssevol. Si $n \geq 2$, llavors que x^n sigui parell és condició necessària i suficient per tal que x sigui parell.

Siguin x, n enters qualssevol, amb (i) $n \geq 2$. Aleshores x^n és parell si, i només si, x és parell.

h) Sigui x un nombre natural qualsevol. Per a tot enter $n \geq 2$, x^n és parell si, i només si, x és parell.
i) $n! > 2^n$ per a tot nombre natural $n \geq 4$.
j) Per a tot nombre real $x > -1$ i per a tot n enter positiu, $(1+x)^n \geq 1+nx$.
k) Sigui $x \in \mathbb{Z}$ qualsevol. Si $5x-7$ és senar, aleshores $9x+2$ és parell.

26 En un examen, s'ha d'escriure la negació de:

a) $\forall x(P(x) \rightarrow Q(x))$ (on $x \in U$, un universal).
La resposta que es dóna és:
$\exists x(\neg P(x) \rightarrow \neg Q(x))$.
És correcte?

b) $\forall x(\neg P(x) \rightarrow \neg Q(x))$ (on $x \in U$, un universal).
La resposta que es dóna és: $\exists x(P(x) \rightarrow Q(x))$.
És correcte?

26* *Resposta:*

a) No és correcte. La negació és:
$\exists x(P(x) \wedge \neg Q(x))$.

b) No. La resposta és $\exists x(\neg P(x) \wedge Q(x))$.

27 Considerant el conjunt $U = \{a,b,c,d\}$ com a "univers" o "univers de referència", i entenent que "x" pertany a U, indiqueu què significa (si hi ha algun cas que s'hi ajusti) $\forall x Q(x)$, on $Q(x)$ és una afirmació que es formula en termes de la variable x:

a) $Q(a) \vee Q(b) \vee Q(c) \vee Q(d)$
b) $Q(a) \wedge Q(b) \wedge Q(c) \wedge Q(d)$
c) $\neg Q(a) \vee \neg Q(b) \vee \neg Q(c) \vee Q(d)$
d) $\neg Q(a) \wedge \neg Q(b) \wedge \neg Q(c) \wedge \neg Q(d)$

27* *Resposta:*

a) Fals   b) Cert   c) Fals   d) Fals

28 Considerant el conjunt $U = \{a,b,c,d\}$ com a "univers" o "univers de referència", i entenent que "x" pertany a U, considereu els enunciats següents, on $Q(x)$ és una afirmació que es formula en termes de la variable x (predicat). Estudieu si es poden expressar com a enunciat amb les variables quantificades (per exemple, $\neg\forall x Q(x)$):

a) $\neg Q(a) \vee \neg Q(b) \vee \neg Q(c) \vee \neg Q(d)$
b) $Q(a) \wedge Q(b) \wedge Q(c) \wedge Q(d)$
c) $Q(a) \vee Q(b) \vee Q(c) \vee Q(d)$
d) $\neg Q(a) \wedge \neg Q(b) \wedge \neg Q(c) \wedge \neg Q(d)$
e) $\neg(Q(a) \wedge Q(b) \wedge Q(c) \wedge Q(d))$

28* *Resposta:*

a) $\neg\forall x Q(x)$ (equivalent a $\exists x \neg Q(x)$)
b) $\forall x Q(x)$
c) $\exists x Q(x)$
d) $\neg\exists x Q(x)$ (equivalentment, $\forall x \neg Q(x)$)
e) $\neg\forall x Q(x)$ (equivalentment, $\exists x \neg Q(x)$)

29 La negació de $\forall x Q(x)$ és (equivalent a) $\forall x \neg Q(x)$. Cert o fals?

29* *Resposta:* Fals. La negació $\neg \forall x Q(x)$ de $\forall x Q(x)$ és $\exists x \neg Q(x)$.

30 L'enunciat $\forall x \neg Q(x)$ és negació de...

30* *Resposta:* $\neg \exists x Q(x)$.

En efecte, $\forall x \neg Q(x) \equiv \neg\neg \forall x \neg Q(x) \equiv \neg(\neg \forall x \neg Q(x)) \equiv \neg(\exists x \neg\neg Q(x)) \equiv \neg(\exists x Q(x))$.

31 Indiqueu si són certes les afirmacions següents, per a un predicat $Q(x)$:

a) La negació de $\forall x Q(x)$ és $\forall x \neg Q(x)$.
b) La negació de $\exists x Q(x)$ és $\exists x \neg Q(x)$.
c) $\forall x Q(x) \to \exists x Q(x)$.
d) $\exists x Q(x) \to \forall x Q(x)$.

31* *Resposta:*

a) Fals b) Fals c) Cert d) Fals

32 Considerem el predicat $Q(x)$ on $x \in U = \{a,b,c\}$. Escriviu expressions desplegades, sense quantificador, amb la variable substituïda pels valors de l'"univers" corresponents als enunciats amb quantificador universal i existencial:

a) $\forall x Q(x)$ b) $\exists x Q(x)$ c) $\neg \forall x Q(x)$ d) $\neg \exists x Q(x)$

32* *Resposta:*

a) $Q(a) \wedge Q(b) \wedge Q(c)$
b) $Q(a) \vee Q(b) \vee Q(c)$
c) $\neg Q(a) \vee \neg Q(b) \vee \neg Q(c)$
d) $\neg Q(a) \wedge \neg Q(b) \wedge \neg Q(c)$

33 Si $Q(x)$ és un predicat (amb $x \in U$, "univers de discurs"), es fa servir la notació $\exists! x Q(x)$ per a indicar que existeix un *únic* x que satisfà $Q(x)$. Expresseu aquesta propietat d'existència i unicitat mitjançant un enunciat que eviti aquesta notació.

33* *Resposta:* $(\exists x Q(x)) \wedge (\forall z \forall t (Q(z) \wedge Q(t) \to z = t))$,

o bé, equivalentment:

$(\exists x Q(x)) \wedge (\forall z \forall t (z \neq t \to \neg(Q(z) \wedge Q(t))))$

A la formulació anterior, existència i unicitat són independents. A la que segueix, podem expressar la unicitat suposant existència prèvia:

$\exists x (Q(x) \wedge \forall y (Q(y) \to y = x))$, o bé

$\exists x (Q(x) \wedge \forall y (y \neq x \to \neg Q(y)))$

34 Si $U = \{a,b,c\}$ i $Q(x)$ és un predicat, amb $x \in U$, escriviu una fórmula proposicional, sense quantificadors, amb les variables substituïdes, que correspongui a "existeix un únic x tal que $Q(x)$".

34* *Resposta:* Una possibilitat és:

$$(Q(a) \wedge \neg Q(b) \wedge \neg Q(c)) \vee (\neg Q(a) \wedge Q(b) \wedge \neg Q(c)) \vee (\neg Q(a) \wedge \neg Q(b) \wedge Q(c)).$$

35 Expresseu formalment "tot nombre real té arrel cúbica real" (equivalent a "existeix arrel cúbica de tot nombre real").

35* *Resposta:* $\forall x \exists y (y^3 = x)$, on suposem que l'univers al qual pertanyen les variables és $\mathbb{R}$. Si s'inclou l'universal al propi enunciat, aleshores seria $\forall x (x \in \mathbb{R} \to (\exists y)(y \in \mathbb{R} \wedge y^3 = x))$. O bé, sense notació conjuntista, $\forall x(x$ nombre real $\to (\exists y)(y$ nombre real $\wedge$ $y^3 = x))$.

36 Per a demostrar $\neg \exists x P(x)$, és equivalent demostrar:

a) $\exists x \neg P(x)$ b) $\forall x P(x)$ c) $\forall x \neg P(x)$ d) $\neg \forall x P(x)$

36* *Resposta:*

a) No b) No c) Sí d) No

37 Indiqueu quines afirmacions són equivalents a $\neg \forall x P(x)$, on $P(x)$ és un predicat:

a) $\forall x \neg P(x)$
b) $\exists x P(x)$
c) $\exists x \neg P(x)$
d) $\neg \exists x P(x)$
e) $\neg \exists x \neg P(x)$
f) $\neg\neg\neg \forall x P(x)$

37* *Resposta:*

a) No b) No c) Sí d) No e) No f) Sí

38 Indiqueu quines afirmacions són equivalents a la negació de $\exists \neg P(x)$, on $P(x)$ és un predicat.

a) $\neg \exists x \neg P(x)$
b) $\forall x \neg P(x)$
c) $\forall x P(x)$
d) $\forall x \neg\neg P(x)$
e) $\exists x \neg\neg P(x)$

38* *Resposta:*

a) Sí b) No c) Sí d) Sí e) No

39 Escriviu una fórmula equivalent a $\neg \exists x P(x)$, de manera que $\neg$ no aparegui a l'esquerra.

39* *Resposta:* $\forall x \neg P(x)$

40 Escriviu una fórmula equivalent a $\neg\forall x(P(x) \to Q(x))$, sense cap $\to$ i de manera que $\neg$ no aparegui a l'esquerra.

40* *Resposta:*

$\neg\forall x(P(x) \to Q(x))$

$\exists x\neg(P(x) \to Q(x))$

$\exists x(P(x) \wedge \neg Q(x))$

41 Escriviu una fórmula equivalent a $\neg\forall xP(x)$, de manera que $\neg$ no aparegui a l'esquerra.

41* *Resposta:* $\exists x\neg P(x)$

42 Escriviu una fórmula equivalent a $\neg\exists x(\neg P(x) \vee \neg Q(x))$ sense cap $\neg$.

42* *Resposta:*

$\neg\exists x(\neg P(x) \vee \neg Q(x))$

$\forall x\neg(\neg P(x) \vee \neg Q(x))$

$\forall x(\neg\neg P(x) \wedge \neg\neg Q(x))$

$\forall x(P(x) \wedge Q(x))$

43 Escriviu com a negació $\forall x\neg P(x)$.

43* *Resposta:* Ja sabem que $\forall x\neg P(x)$ és equivalent a $\neg\exists xP(x)$. Però, en general, es podria procedir de manera més sistemàtica, escrivint:

$\forall x\neg P(x)$

$\neg\neg(\forall x\neg P(x))$

$\neg(\neg(\forall x\neg P(x)))$

$\neg(\exists x\neg\neg P(x))$

$\neg(\exists xP(x))$

44 Formalitzeu completament l'afirmació: "per a tot nombre natural n, la suma dels n primers nombres naturals és $\frac{n(n+1)}{2}$".

44* *Resposta:* $\forall n(\sum_{i=0}^{n} i = \frac{n(n+1)}{2})$ (opció alternativa: introduir $\mathbb{N}$)

45 La fórmula de predicats $\forall x\neg\forall yP(x)$ equival a:

a) $\forall x\exists yP(x)$ b) $\forall x\exists y\neg P(x)$ c) $\forall x\exists yP(\neg x)$

45* *Resposta:*

a) No. b) Sí. c) No té sentit.

46 Escriviu $\forall x \neg \forall y P(x,y)$ com a negació.

46* *Resposta:* $\neg \exists x \forall y P(x,y)$

47 Escriviu formalment la condició de ser tres objectes diferents. Expresseu-ho en termes d'un predicat. Expresseu-ho en termes del predicat de ser dos objectes diferents.

Denotant els objectes per x, y, z, en relació amb aquest problema, indiqueu quines afirmacions són correctes.

a) $x \neq y \wedge y \neq z \wedge z \neq x$
b) $x \neq y \wedge y \neq z$
c) $|\{x,y,z\}| = 3$
d) $x \notin \{y,z\}, y \notin \{x,z\}$ (no hi ha elements repetits en un conjunt)

47* *Resposta:* Una possible solució és $P(x,y,z) := (x \neq y) \wedge (y \neq z) \wedge (z \neq x)$ (observació: els parèntesis de la fórmula anterior no són estrictament necessaris; només s'hi inclouen per facilitar-ne la llegibilitat). Si es considera el predicat $D(a,b) := (a \neq b)$, es pot reexpressar com $P(x,y,z) := D(x,y) \wedge D(y,z) \wedge D(z,x)$. També es podria considerar un predicat auxiliar, el de "ser iguals", $I(a,b) := (a = b)$; aleshores es podria expressar com $P(x,y,z) := \neg I(x,y) \wedge \neg I(y,z) \wedge \neg I(z,x)$.

Encara hi ha altres variants possibles:

$P(x,y,z) := \neg(x = y) \wedge \neg(y = z) \wedge \neg(z = x) = \neg((x = y) \vee (y = z) \vee (z = x)) = \neg(I(x,y) \vee I(y,z) \vee I(z,x))$.

Pel que fa a les preguntes:

a) Cert.
b) Fals. Pot ser $x = z$.
c) Cert.
d) Cert, però redundant.

Observeu com, a partir d'un predicat bàsic com el de "ser diferents (dos objectes)", podem construir predicats més complexos (per exemple, "ser 4 objectes diferents").

48 Formalitzeu completament l'afirmació següent (no cal que sigui certa; només cal saber escriure una fórmula de predicat que es correspongui amb l'enunciat). "Per a tot nombre natural n, la suma dels cubs dels n primers nombres naturals senars és el quadrat d'un nombre natural múltiple de 4".

48* *Resposta:* Entenent que el conjunt de referència és $\mathbb{N}$ (domini universal), en proposem diverses variants:

$\forall n\ \exists k\ (\sum_{j=0}^{n-1}(2j+1)^3 = (4k)^2)$

$\forall n\ \exists k\ (\sum_{j=1}^{n}(2j-1)^3 = (4k)^2)$

$\forall n \in \mathbb{N}\ \exists k \in \mathbb{N}\ (\sum_{j=0}^{n-1}(2j+1)^3 = (4k)^2)$

$\forall n\ (n \in \mathbb{N} \to \exists k\ (k \in \mathbb{N} \wedge \sum_{j=0}^{n-1}(2j+1)^3 = (4k)^2)$

49 Formalitzeu, mitjançant una fórmula del llenguatge de predicats:

"L'equació $x^4+3x^2+5=0$ té solucions reals"

"L'equació $x^4+3x^2+5=0$ admet solucions reals"

"L'equació $x^4+3x^2+5=0$ té alguna solució real"

"Hi ha un nombre real que és solució de l'equació $x^4+3x^2+5=0$"

"Existeix alguna solució real de l'equació $x^4+3x^2+5=0$"

"Existeixen solucions reals de l'equació $x^4+3x^2+5=0$"

49* *Resposta:* Totes les afirmacions diuen el mateix (no importa si l'enunciat és cert o fals).

$\exists x(x \in \mathbb{R} \wedge x^4+3x^2+5=0)$

$\exists x \in \mathbb{R}(x^4+3x^2+5=0)$ (no estàndard)

Seria una possible formulació. O bé, si queda sobreentès que el conjunt universal és el dels nombres reals:

$\exists x(x^4+3x^2+5=0)$

50 Considereu la fórmula de predicats (versió estil informal o semiformalitzat):
$\forall x \in B\ P(x)$
Indiqueu quines de les següents són (equivalents a) la negació de la fórmula i les que ho siguin, per què:

a) $\forall x \in B\ \neg P(x)$
b) $\exists x \in B\ P(\neg x)$
c) $\exists x \in B\ P(x)$
d) $\exists x \in B\ \neg P(x)$
e) $\exists x \notin B\ P(x)$
f) $\exists x \notin B\ \neg P(x)$
g) $\forall x \notin B\ \neg P(x)$
h) $\forall x \notin B\ P(x)$

50* *Resposta:* L'única correcta és (d): $\exists x \in B\ \neg P(x)$.

Per veure-ho, hem de reformalitzar-la de forma estàndard:

$\forall x \in B\ P(x)$

$\forall x(x \in B \to P(x))$

La negació serà:

$\neg(\forall x(x \in B \to P(x)))$

$\exists x \neg(x \in B \to P(x))$

$\exists x(x \in B \wedge \neg P(x))$ (per $\neg(p \to q) \equiv p \wedge \neg q$),

que reescrivim informalment com:

$\exists x \in B(\neg P(x))$

$\exists x \in B \neg P(x)$

51 Indiqueu quina és la propietat que permet escriure:

$\forall a \forall a'((a \in A \wedge a' \in A \wedge a \neq a') \to f(a) \neq f(a'))$

en comptes de:

$\forall a \forall a'(((a \in A \wedge a' \in A) \wedge a \neq a') \to f(a) \neq f(a'))$

o de:

$\forall a \forall a'((a \in A \wedge (a' \in A \wedge a \neq a')) \to f(a) \neq f(a'))$

51* *Resposta:* L'associativitat de la conjunció.

52 Definint els predicats adequats, traduïu a una fórmula de predicats: "Si tot és matèria, aleshores no existeixen esperits".

52* *Resposta:* Si M és "ser matèria" i E és "ser esperit":

$\forall x M(x) \to \neg \exists y E(x)$

53 Considereu la frase: "cap home és un insecte". Estudieu si alguna de les fórmules de predicat següents, amb la notació òbvia H (ser home), I (ser insecte), n'és la traducció.

a) $\forall x(H(x) \to \neg I(x))$
b) $\neg \forall x(H(x) \to I(x))$
c) $\exists x(H(x) \wedge \neg I(x))$
d) $\neg \exists x(H(x) \wedge I(x))$

53* *Resposta:*

a) Correcte
b) Incorrecte. Equivalent a (3). No impedeix que algun home pugui ser insecte.
c) Incorrecte. Equivalent a (2). No impedeix que algun home pugui ser insecte.

d) Correcte. Equivalent a (1). Es veu pel significat i també formalment, derivant-la de (1), a través d'una seqüència d'equivalències:

$\forall x(H(x) \to \neg I(x))$

$\neg\neg\forall x(H(x) \to \neg I(x))$

$\neg\exists x\neg(H(x) \to \neg I(x))$

$\neg\exists x(H(x) \wedge \neg\neg I(x))$

$\neg\exists x(H(x) \wedge I(x))$

54 Definiu un nou quantificador existencial $\exists!!$, on $\exists!!xP(x)$ significa que "existeixen exactament dos x tals que $P(x)$". S'ha de definir en termes dels quantificadors ordinaris $\forall, \exists$ o un d'ells.

54* *Resposta:* Hi ha diverses solucions possibles. N'indiquem una solució bàsica:

$$\exists x\exists y(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z(P(z) \to (z = x \vee z = y)))$$

Les següents es poden obtenir a partir de la bàsica, per aplicació de diverses equivalències (De Morgan, contrarecíproc, etc.):

$$\exists x\exists y(P(x) \wedge P(y) \wedge x \neq y \wedge \neg\exists z(P(z) \wedge z \neq x \wedge z \neq y))$$

$$\exists x\exists y(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z((z \neq x \wedge z \neq y) \to \neg P(z)))$$

$$\exists x\exists y(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z((P(z) \wedge z \neq x) \to z = y))$$

$$\exists x\exists y(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z((P(z) \wedge z \neq y) \to z = x))$$

També, incorporant llenguatge de conjunts:

$$\exists x\exists y(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z(P(z) \to z \in \{x,y\}))$$

I, naturalment, canviant d'ordre els quantificadors existencials:

$$\exists y\exists x(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z(P(z) \to (z = x \vee z = y)))$$

Qüestió. Analitzeu si seria correcte escriure:

$$\exists xP(x) \wedge \exists yP(y) \wedge x \neq y \wedge \forall z(P(z) \to (z = x \vee z = y))$$

55 Considereu les fórmules de predicat següents i indiqueu quines són negacions de les altres, si és el cas.

a) $\forall x(A(x) \to B(x))$
b) $\forall x(A(x) \to \neg B(x))$
c) $\exists x(A(x) \wedge B(x))$
d) $\exists x(A(x) \wedge \neg B(x))$

55* *Resposta:*

(d) és negació de (a) (de fet, són negacions l'una de l'altra) i

(b) és negació de (c) (de fet, són negacions l'una de l'altra).

56 Considereu l'afirmació: "De cada 5 nombres enters consecutius, exactament un és múltiple de 5". Formalitzeu-la.

56* *Resposta:* Es pot simbolitzar de diverses maneres. En primer lloc, suposem que els nombres consecutius tenen la forma $n, n+1, n+2, n+3, n+4$ (equivalent a altres formulacions, com per exemple $n-4, n-3, n-2, n-1, n, n+k, n+k+1, \ldots$. Podem expressar la variació $0 \leq i \leq 4$ de diverses formes, com ara $i \in \{0,1,2,3,4\}$ o $i = 0 \vee i = 1 \vee i = 2 \vee i = 3 \vee i = 4$.

Versió 1. $\forall n(n \in \mathbb{Z} \to \exists i(i \in \mathbb{N} \wedge 0 \leq i \leq 4 \wedge 5|n+i \wedge \forall j((j \in \mathbb{N} \wedge 0 \leq j \leq 4 \wedge 5|n+j) \to j = i)))$

Versió 2. $\forall n(n \in \mathbb{Z} \to \exists i(i \in \mathbb{N} \wedge 0 \leq i \leq 4 \wedge 5|n+i) \wedge \forall j \forall k((j \in \mathbb{N} \wedge k \in \mathbb{N} \wedge 0 \leq j \leq 4 \wedge 0 \leq k \leq 4 \wedge 5|n+j \wedge 5|n+k) \to j = k)))$

Observació: Aquí només es formalitza, no es demostra.

57 Traduïu a llenguatge natural les fórmules de predicat següents:

a) $\forall x((M(x) \wedge \forall y \neg A(x,y)) \to I(x))$, si $M(x)$ és "x és un home", $I(x)$ és "x és infeliç", $A(x,y$ és "x és amic de y".

b) $\neg \exists x(E(x) \wedge \forall y(E(y) \to M(y,x)))$, si $E(x)$ és "x és enter" i $M(x,y)$ és "$x \leq y$"

c) Si $P(x)$ és "x és una persona" i $H(x,y)$ és "x odia a y":

i) $\exists x(P(x) \wedge \forall y(P(y) \to H(x,y)))$
ii) $\forall x(P(x) \to \forall y(P(y) \to H(x,y)))$
iii) $\forall x(P(x) \to \forall y(P(y) \to H(y,x)))$
iv) $\forall x(P(x) \to \exists y(P(y) \to H(x,y)))$
v) $\exists x(P(x) \wedge \forall y(P(y) \to (H(x,y) \leftrightarrow H(y,y))))$

58 Si A és un conjunt, considerem la fórmula de predicats:

$\forall x \forall y((x \in A \wedge x \in A) \to x = y)$

La fórmula diu:

a) que el conjunt A té elements.
b) no diu ni tan sols que hi hagi algun element a A.
c) que, si hi ha elements, com a màxim n'hi ha un.
d) que el conjunt A pot ser buit o tenir un element.

e) $|A| \leq 1$
f) $A = \emptyset$ o $|A| = 1$
g) $A = \emptyset$ o $\exists x(A = \{x\})$
h) $\forall x(x \notin A) \vee \exists x(A = \{x\})$
i) $\neg\exists x\exists y(x \in A \wedge y \in A \wedge x \neq y)$
j) $\forall x\forall y(x \neq y \rightarrow (x \notin A \vee y \notin A))$
k) $\forall x\forall y((x \neq y \wedge x \in A) \rightarrow y \notin A)$
l) $\forall x\forall y((x \neq y \wedge y \in A) \rightarrow x \notin A)$
m) $\exists x\exists y(x \in A \wedge y \in A \wedge x \neq y)$

58* *Resposta:*

a) Fals.
b) Cert.
c) Cert.
d) Cert.
e) Cert.
f) Cert.
g) Cert.
h) Cert.
i) Cert.
j) Cert.
k) Cert.
l) Cert.
m) Fals.

59 Expresseu amb una fórmula de predicats: “Algunes persones escolten a tothom”.

59* *Resposta:* Considerem els predicats:

$P(x)$:= “x és una persona”

$E(x,y)$:=“x escolta a y ”

Versió 1. Considerem que “una persona no s’escolta a si mateixa”.

Una solució possible:

$\exists x(P(x) \wedge \forall t((P(t) \wedge t \neq x) \rightarrow E(x,y)))$

Versió 2. Sense la condició “una persona no s’escolta a si mateixa”, aleshores seria:

$\exists x(P(x) \wedge \forall t(P(t) \rightarrow E(x,y)))$

Exercicis proposats

60 Si P, Q són predicats, indiqueu si són certs:

a) $\neg\forall xP(x) \equiv \exists xP(x)$.
b) $\forall xP(x) \equiv \neg\exists x\neg P(x)$.
c) $\forall xP(x) \equiv \neg\exists y\neg P(y)$.
d) $\forall x\neg P(x) \equiv \neg\exists xP(x)$
e) $\neg\exists xP(x) \equiv \forall xP(x)$
f) $\neg\forall x\neg P(x) \equiv \exists xP(x)$
g) $\exists xP(x) \equiv \neg\forall x\neg P(x)$
h) $\forall x(P(x) \wedge \neg Q(x)) \equiv \neg\exists x(P(x) \rightarrow Q(x))$
i) $\forall x(P(x) \rightarrow Q(x)) \equiv \forall x\neg(P(x) \wedge \neg Q(x))$
j) $\forall x(P(x) \rightarrow Q(x)) \equiv \forall x(\neg Q(x) \rightarrow \neg P(x))$

60* *Resposta:* Vegem només l’apartat (h): $\forall x(P(x) \wedge \neg Q(x)) \equiv \neg\exists x(P(x) \rightarrow Q(x))$.

Per doble negació, podem escriure la fórmula equivalent a l’anterior (esquerra):

$\forall x\neg\neg(P(x) \wedge \neg Q(x))$

Ara “desplacem” una d’aquestes negacions cap a l’esquerra i l’altra cap a la dreta i n’obtenim una seqüència d’equivalències:

$\neg\exists x \neg(P(x) \wedge \neg Q(x))$

$\neg\exists x(\neg P(x) \vee \neg\neg Q(x))$ (per De Morgan)

$\neg\exists x(\neg P(x) \vee Q(x))$ (per doble negació)

$\neg\exists x(P(x) \rightarrow Q(x))$ $(\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta)$

Per tant és cert: $\forall x(P(x) \wedge \neg Q(x)) \equiv \neg\exists x(P(x) \rightarrow Q(x))$.

61 Considereu la frase “els mirtils i les cireres són rics en antioxidants”. Estudieu quines de les fórmules de predicat següents serien bones traduccions de l’enunciat, amb els significats: M (ser mirtil), C (ser cirera), A (ser ric en antioxidants).

a) $\forall x((M(x) \wedge C(x)) \rightarrow A(x))$

b) $\forall x((M(x) \vee C(x)) \rightarrow A(x))$

c) $\forall x((M(x) \rightarrow A(x)) \vee (C(x) \rightarrow A(x)))$

d) $\forall x(M(x) \rightarrow A(x)) \vee \forall x(C(x) \rightarrow A(x))$

e) $\forall x((M(x) \rightarrow A(x)) \wedge (C(x) \rightarrow A(x)))$

f) $\forall x(M(x) \rightarrow A(x)) \wedge \forall x(C(x) \rightarrow A(x))$

62 En l’intent d’expressar: “hi ha, com a mínim, tres elements”, s’escriuen les fórmules següents. Estudieu quines relacions hi ha entre les diverses fórmules i quines corresponen a la frase.

a) $\exists x\exists y\exists z(x \neq y \wedge x \neq z \wedge y \neq z)$

b) $\exists x\exists y\exists z(\neg x = y \wedge \neg x = z \wedge \neg y = z)$

c) $\exists x\exists y\exists z\neg(x = y \vee x = z \vee y = z)$

d) $\neg\forall x\forall y\forall z(x = y \vee x = z \vee y = z)$

e) $\exists x\exists y\exists z\neg((x \neq y \wedge x \neq z) \rightarrow y = z)$

f) $\neg\forall x\forall y\forall z((x \neq y \wedge x \neq z) \rightarrow y = z)$

g) $\exists x\exists y\exists z\neg(y \neq z \rightarrow (x = y \vee x = z))$

h) $\exists x\exists y\exists z\neg(y \neq z \wedge x \neq y) \rightarrow x = z)$

i) $\exists x\exists y\exists z\neg(y \neq z \rightarrow (x \neq y \rightarrow x = z))$

63 Es tracta d’expressar amb una fórmula de predicats: “Algunes persones escolten a tothom”. Hi ha diverses formulacions equivalents, com “algú escolta a tothom”, per exemple.

Considereu els predicats:

$P(x)$:= "x és una persona"

$E(x,y)$:="x escolta a y"

i suposeu que "una persona no s'escolta a si mateixa".

Analitzeu les fórmules següents i indiqueu quines són la solució i quines no ho són.

a) $\exists x(P(x) \wedge \forall t((P(t) \wedge t \neq x) \rightarrow E(x,y)))$
b) $\exists x P(x) \wedge \forall t((P(t) \wedge t \neq x) \rightarrow E(x,y))$
c) $\exists x(P(x) \wedge \forall t(P(t) \rightarrow (t \neq x \rightarrow E(x,y))))$
d) $\exists x(P(x) \wedge \forall t(P(t) \rightarrow (\neg E(x,y) \rightarrow t = x)))$
e) $\exists x(P(x) \wedge \forall t(t \neq x \rightarrow (P(t) \rightarrow E(x,y))))$
f) $\exists x P(x) \wedge \forall t(t \neq x \rightarrow (P(t) \rightarrow E(x,y)))$.

→ 6

Mètodes de demostració

En alguns capítols anteriors, s'han vist diverses tècniques de demostració d'enunciats. En aquest capítol, s'exposen de manera més *sistemàtica* diverses *metodologies de demostració*, llevat de la inducció, a la qual es dedica un capítol exclusiu. Encara que algunes demostracions facin servir una barreja de mètodes, podem dir que els mètodes més habituals són els següents:

a) Demostració directa.

b) Demostració pel contrarecíproc (mètode del contrarecíproc).

c) Demostració per reducció a l'absurd (mètode de reducció a l'absurd).

d) Demostració per casos.

e) Demostració per inducció, en diverses modalitats (capítol específic).

Encara que cada tipologia es descriu per separat, si convé presentem demostracions amb la barreja de mètodes que calgui, encara que es descriguin monogràficament en seccions posteriors, dintre del mateix capítol.

Alguns dels mètodes es basen o estan relacionats amb equivalències lògiques, que ja s'han tractat en el capítol de llenguatge de proposicions. N'enumerem les principals:

a) $A \to B \equiv \neg A \vee B$ (condicional en termes de negació i disjunció).

b) $\neg(A \to B) \equiv A \wedge \neg B$ (negació del condicional).

c) $(A \to B) \equiv (\neg B \to \neg A)$ (contrarecíproc).

d) $(A \vee B) \to C \equiv (A \to C) \wedge (B \to C)$ (per casos)
(disjunció a l'antecedent; enunciat per a disjunció de dos casos, ampliable a més).

e) $A \to (B \vee C) \equiv (A \wedge \neg B) \to C \equiv (A \wedge \neg C) \to B$ (disjunció al conseqüent)
(enunciat per a disjunció de dos, ampliable a més).

f) $A \vee B \equiv \neg B \to A \equiv \neg A \to B$ (disjunció en termes de condicional) (enunciat per a dos casos, ampliable per associativitat).

g) $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$.

També s'utilitzen altres equivalències lògiques, com per exemple les de De Morgan.

Com a la resta de l'obra, molts exercicis són de poca dificultat tècnica, per tal de poder veure fàcilment el mecanisme de demostració, de manera que no quedi enfosquit per un cúmul de tecnicismes. D'aquesta manera, destaca el mecanisme, la metodologia de prova.

6.1. La implicació

6.1.1. La implicació (⇒)

Considerem el **condicional** $p \to q$. Vegem-ne un exemple, suposant que n és un nombre enter, en diverses formes:

"si n és senar, aleshores n^2 és senar",
"si n és senar, n^2 és senar",
"$2 \nmid n \to 2 \nmid n^2$",
on $p := 2 \nmid n$ i $q := 2 \nmid n^2$.

Es podria completar la fórmula anterior de dues maneres equivalents, introduint-hi el domini:

$(n \in \mathbb{Z} \wedge 2 \nmid n) \to 2 \nmid n^2$
$n \in \mathbb{Z} \to (2 \nmid n \to 2 \nmid n^2)$

En principi, $2 \nmid n \to 2 \nmid n^2$ és una simple fórmula, i res més, del llenguatge de predicats. Amb l'enunciat no afirmem res sobre la fórmula (a la pràctica moltes vegades se sobreentén una manifestació implícita de veracitat, només d'escriure-la). El pas següent és fer l'afirmació explícita de veracitat, si és el cas:

Què vol dir que *A* implica *B*? (***A*** $\boldsymbol{\Rightarrow}$ ***B***). Sobre aquesta fórmula, podem fer les afirmacions següents:

"$2 \nmid n \to 2 \nmid n^2$ **és cert**"
"El condicional $2 \nmid n \to 2 \nmid n^2$ **és cert**"
"**És cert** el condicional $2 \nmid n \to 2 \nmid n^2$",

on s'afirma la veracitat del condicional.

És el mateix que dir: $2 \nmid n \Rightarrow 2 \nmid n^2$, que es llegeix "$2 \nmid n$ **implica** $2 \nmid n^2$"

Per tant, i amb el símbol $\Rightarrow$,

$A \Rightarrow B$ (A implica B) si, i només si, $A \to B$ és cert .

De fet, A implica B si, i només si, “si A és cert, aleshores B és cert”.

Per tant, si afirmem “$2 \nmid n \Rightarrow 2 \nmid n^2$”, estem afirmant: “$2 \nmid n \to 2 \nmid n^2$ és cert”.

Observacions diverses

Observació 1 (de quin llenguatge és $\Rightarrow$?): $A \Rightarrow B$ no és una fórmula del llenguatge de predicats. És una afirmació externa, sobre una fórmula del llenguatge, concretament $A \to B$ (tècnicament, seria d’un “metallenguatge”).

Observació 2 (vegem-ne el rerafons lògic): En alguns textos s’afirma que “A implica B” si $A \to B$ és una tautologia.
És correcte i equivalent. En efecte, si observem la taula de veritat del condicional:

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

resulta que, en els casos $F \to F$ $(0 \to 0)$, $F \to V$ $(0 \to 1)$, ja està garantida la certesa, formalment, sense provar res. De fet, són casos sense interès per a aquest capítol sobre demostració. De manera que hem de veure que es produeix el cas $V \to V$ $(1 \to 1)$, és a dir, que no es produeix el cas $V \to F$ $(1 \to 0)$ o, dit d’una altra manera, que no pot ser que A sigui cert i B no ho sigui.

El cas $V \to V$ $(1 \to 1)$ (per a $A \to B$) normalment, és a dir, en enunciats d’interès, cal establir-lo. En aquest cas, sol ser necessari un “esforç”, una argumentació que estableixi la veracitat de B utilitzant la veracitat suposada de A. Els casos interessants seran aquells en què d’alguna forma existeixi alguna relació entre A i B, com per exemple, amb l’afirmació $2|n \Rightarrow 2|n^3$. Altres casos de condicional formalment cert no tenen cap interès pel que fa al que ens ocupa com per exemple $2 > 0 \to 4 < 5$.
Ens interessen, doncs, aquelles situacions en què es produeix un resultat realment nou, que cal establir, és a dir, demostrar.

Observació 3 (prevenim el lector). En alguns textos, no es fa aquesta distinció notacional i conceptual entre $\to$ i $\Rightarrow$.

Observació 4 (algunes redundàncies). També es diu:

“$A \Rightarrow B$ és cert” (és redundant)
“Demostrem $A \to B$” (es vol dir: “Demostrem que $A \to B$ és cert”).
O bé: “Hem de demostrar $A \to B$”.

Observació 5 (abús notacional). De vegades, es fa un abús del llenguatge. Per exemple, si s’escriu $(A \Rightarrow B) \wedge (A \Rightarrow C)$, s’està fent una barreja, ja que formalment el símbol $\Rightarrow$ no forma part de llenguatge de proposicions. Seria millor escriure $A \Rightarrow B$ i $A \Rightarrow C$. Aquest “problema” menor també es podria solucionar ampliant el llenguatge de predicats amb els símbols nous $\Rightarrow$ i $\Leftrightarrow$, amb les ampliacions gramaticals corresponents.

Un exemple més: la negació de la implicació "no ($A \Rightarrow B$)" ($A \to B$ no és cert), de vegades s'escriu abusivament com $\neg(A \Rightarrow B)$ i s'escriu que és $A \wedge \neg B$, quan en realitat s'ha d'escriure "A i no B".

Vulgui el lector disculpar que, de vegades, també nosaltres cometem aquest abús notacional.

Hipòtesi-tesi. En el context d'una implicació $A \Rightarrow B$, ampliem les denominacions per al cas del condicional dels dos components de la fórmula (A, B) (vegeu el capítol sobre el llenguatge de proposicions):

A és la **hipòtesi** (o la **premissa** o l'**antecedent**),
B és la **tesi** (o la **conclusió** o el **conseqüent o conseqüència**).

Condició necessària, condició suficient. També tenen el mateix ús que en el cas del condicional (vegeu el capítol sobre el llenguatge de proposicions) les expressions **condició necessària** i **condició suficient**: així, si $A \Rightarrow B$:

A és condició suficient per a B,
B és condició necessària per a A.

Això es pot reexpressar en una sèrie de frases equivalents totalment paral·leles que s'han vist al capítol dedicat al llenguatge de proposicions. Per exemple:

"si A és cert, necessàriament B és cert",
"és necessari que B sigui cert perquè ho sigui A",
"és suficient que A sigui cert per tal que també ho sigui B",
i moltes altres.

Vegem un exemple de **demostració**.

Exemple 6.1 Suposem que n és un nombre enter.

Demostrem $2 \nmid n \Rightarrow 2 \nmid n^3$.

És a dir, n és senar $\Rightarrow n^3$ és senar.

Hipòtesi: $2 \nmid n$ (amb n nombre enter)
Tesi: $2 \nmid n$ (amb n nombre enter)

Una altra formulació: $(n \in \mathbb{Z} \wedge 2 \nmid n) \Rightarrow 2 \nmid n^3$

Idea de la demostració. És convenient tenir una idea de la demostració. Es tracta d'encadenar arguments correctes, que produeixin una seqüència (finita) d'afirmacions, cada una conseqüència de l'anterior, que acabin en la conclusió (tesi) i s'utilitzi la hipòtesi (premissa). No existeixen regles en aquest sentit, tot depèn del problema. La idea en aquest exemple: és expressar que n és senar amb alguna fórmula equivalent, que puguem manipular, escrivint que n és de la forma $2k+1$ (amb k enter convenient) i intentant arribar a que n^3 també és de la mateixa forma, és a dir, $n^3 = 2k' + 1$ (amb k' enter convenient); aquesta idea és la que guia el curs o flux de la demostració. Cal recordar com s'expressa la paritat, és a dir, la propietat de ser parell o senar, per a un nombre enter (vegeu el capítol de preliminars).

Demostració. En una sèrie de passos, en què cada línia és conseqüència de l'anterior:

$2 \nmid n \Rightarrow$ (**hipòtesi**, n senar), d'on
existeix $k \in \mathbb{Z}$ tal que $n = 2k+1 \Rightarrow$ (ara elevant al cub)
existeix $k \in \mathbb{Z}$ tal que $n^3 = (2k+1)^3 \Rightarrow$ (calculant)
existeix $k \in \mathbb{Z}$ tal que $n^3 = 8k^3 + 12k^2 + 6k + 1 \Rightarrow$
existeix $k \in \mathbb{Z}$ tal que $n^3 = 2(4k^3 + 6k^2 + 3k) + 1 \Rightarrow$
existeix $k' \in \mathbb{Z}$ tal que $n^3 = 2k' + 1 \Rightarrow$ (prenem $k' = 4k^3 + 6k^2 + 3k \in \mathbb{Z}$)
$2 \nmid n^3$ (**tesi**).

Atenció: Cada una de les afirmacions anteriors és conseqüència de la immediatament anterior.

El curs argumental es pot distribuir també així:

$2 \nmid n$ (n senar)
$\Downarrow$
existeix $k \in \mathbb{Z}$ tal que $n = 2k+1$ (ara elevant al cub)
$\Downarrow$
existeix $k \in \mathbb{Z}$ tal que $n^3 = (2k+1)^3$ (calculant)
$\Downarrow$
existeix $k \in \mathbb{Z}$ tal que $n^3 = 8k^3 + 12k^2 + 6k + 1$
$\Downarrow$
existeix $k \in \mathbb{Z}$ tal que $n^3 = 2(4k^3 + 6k^2 + 3k) + 1$
$\Downarrow$
existeix $k' \in \mathbb{Z}$ tal que $n^3 = 2k' + 1$ (prenent $k' = 4k^3 + 6k^2 + 3k$)
$\Downarrow$
$2 \nmid n^3$ (n^3 senar)

Repetim l'anterior per a veure'n l'esquema:

$P_1 : 2 \nmid n$
P_2 : existeix $k \in \mathbb{Z}$ tal que $n = 2k+1$ (ara elevant al cub)
P_3 : existeix $k \in \mathbb{Z}$ tal que $n^3 = (2k+1)^3$ (calculant)
P_4 : existeix $k \in \mathbb{Z}$ tal que $n^3 = 8k^3 + 12k^2 + 6k + 1$
P_5 : existeix $k \in \mathbb{Z}$ tal que $n^3 = 2(4k^3 + 6k^2 + 3k) + 1$
P_6 : existeix $k' \in \mathbb{Z}$ tal que $n^3 = 2k' + 1$ (prenem $k' = 4k^3 + 6k^2 + 3k$) $P_7 : 2 \nmid n^3$

Hem provat un encadenament argumental, que és el que significa aquesta seqüència d'implicacions:

$P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow P_4 \Rightarrow P_5 \Rightarrow P_6 \Rightarrow P_7$

que és simplement:

$P_1 \Rightarrow P_2$ i $P_2 \Rightarrow P_3$ i $P_3 \Rightarrow P_4$ i $P_4 \Rightarrow P_5$ i $P_5 \Rightarrow P_6$ i $P_6 \Rightarrow P_7$

d'on resulta finalment $P_1 \Rightarrow P_7$, que és el que calia.

Estil expositiu alternatiu. També es pot exposar la demostració en un estil menys formalitzat, més verbal o més conversacional, igualment correcte. Vegem-ho:

1. Sigui n senar. Aleshores es pot expressar com $n = 2k+1$, per a algun k enter adequat. Atès que hem d'arribar a una afirmació sobre la paritat de n^3, calculem n^3 tenint en compte l'expressió anterior. És a dir, substituint, és $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k+1$. Ara el problema radica a expressar n^3 en la forma típica d'un nombre senar, és a dir, $2k'+1$, per a algun enter k'. Vegem si podem reescriure l'expressió $8k^3+12k^2+6k+1$ en aquesta forma. En efecte, $n^3 = 8k^3+12k^2+6k+1 = 2(4k^3+6k^2+3k)+1$, cosa que suggereix quin ha de ser k': prenem $k' = 4k^3+6k^2+3k \in \mathbb{Z}$ i finalment $n^3 = 2k'+1$, amb $k' \in \mathbb{Z}$ convenient.

   L'estil expositiu anterior encara està impregnat del que va pensant qui l'escriu, de quina és la seva guia o estratègia per a la resolució. En un estil més neutre es tindria:

2. Sigui n senar. Aleshores $n = 2k+1$, per a algun k enter adequat. Per tant, és $n^3 = (2k+1)^3 = 8k^3+12k^2+6k+1$. En conseqüència, $n^3 = 8k^3+12k^2+6k+1 = 2(4k^3+6k^2+3k)+1 = 2k'+1$, si prenem $k' = 4k^3+6k^2+3k \in \mathbb{Z}$. Finalment $n^3 = 2k'+1$, amb $k' \in \mathbb{Z}$ convenient. Per tant, n^3 és senar. ■

Si $A \Rightarrow B$ és cert, podem afirmar que B és cert? Demostrar $A \Rightarrow B$ no vol dir que B sigui cert! Per exemple, $1 = 0 \Rightarrow 2 = 4$ és cert perquè és un cas $F \to F$ $(0 \to 0)$, tot i que també podem aportar una demostració en el sentit d'una seqüència argumental:
$2 = 2+0 \overset{0=1}{=} 2+1 = 3 = 3+0 \overset{0=1}{=} 3+1 = 4$,
aplicant repetidament la hipòtesi $1 = 0$.

Una regla d'inferència (*Modus Ponens*). Hi ha la regla de MP (*Modus Ponens*):

A
$A \Rightarrow B$
——————
B

Aleshores es pot deduir B, es pot afirmar la veracitat de B. En efecte, tenint en compte la taula de veritat del condicional, si A és cert (valor veritatiu 1) i $A \to B$ és cert (valor veritatiu 1), és el cas en què B ha de ser cert (valor veritatiu 1).

Com podem obtenir $A \Rightarrow C$ de $A \Rightarrow B$ i de $B \Rightarrow C$?

$$\left.\begin{array}{c} A \Rightarrow B \\ B \Rightarrow C \end{array}\right\} \Rightarrow (A \Rightarrow C)$$

(Observació: S'ha d'entendre aquesta notació com "i" (conjunció):

$$\left.\begin{array}{c} A \Rightarrow B \\ \text{i} \\ B \Rightarrow C \end{array}\right\} \Rightarrow (A \Rightarrow C)$$

Preguntat d'una altra manera:

"Si $A \rightarrow B$ i $B \rightarrow C$ són certs, podem afirmar que $A \rightarrow C$ és cert?"
Sí, efectivament:

Vegem $A \Rightarrow C$. Suposem que A és cert. Vegem que C és cert.

De la suposició que A és cert i que $A \rightarrow B$ és cert, resulta B cert (taula de veritat).

De B cert i de $B \rightarrow C$ cert, resulta C cert.

Per tant, $A \rightarrow C$ és cert i, en conseqüència, $A \Rightarrow C$.

$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$

6.1.2. La doble implicació ($\Leftrightarrow$) o "equivalència"

Què vol dir que són equivalents A i B?

Demostrar el bicondicional $A \leftrightarrow B$ (és a dir, que $A \leftrightarrow B$ és cert).

$A \leftrightarrow B$ és cert

si, i només si, $(A \rightarrow B) \wedge (B \rightarrow A)$ és cert

si, i només si, $A \rightarrow B$ és cert i $B \rightarrow A$ és cert

si, i només si, $A \Rightarrow B$ i $B \Rightarrow A$

Per tant, demostrar que $A \leftrightarrow B$ és cert és el mateix que demostrar les dues implicacions:

$A \Rightarrow B$ i $B \Rightarrow A$

I això s'escriu:

$A \Leftrightarrow B$

Exemple 6.2 Sigui n enter.

$2|n \Leftrightarrow 2|n^2$ ($2|n \leftrightarrow 2|n^2$ és cert),
$5|n \Leftrightarrow 5|n^2$,
$2 \nmid n \Leftrightarrow 2 \nmid n^2$,
$2|n^2 \Leftrightarrow 2|n^5$,
$2 \nmid n^2 \Leftrightarrow 2 \nmid n^5$. ■

Per exemple, per a provar $2|n^2 \Leftrightarrow 2|n^5$, hem de demostrar

$2|n^2 \Rightarrow 2|n^5$ i $2|n^5 \Rightarrow 2|n^2$.

És útil tenir present que $A \Leftrightarrow B$ equival a $\neg A \Leftrightarrow \neg B$.

Així, demostrar $3 \nmid n \Leftrightarrow 3 \nmid n^5$ demostra automàticament $3|n \Leftrightarrow 3|n^5$, i viceversa.

Què vol dir que són equivalents (a), (b) i (c)? Un enunciat típic en relació amb la pregunta és:

> "Demostreu que són equivalents:
>
> (a) Afirmació 1.
>
> (b) Afirmació 2.
>
> (c) Afirmació 3."

Vol dir que $(a) \leftrightarrow (b)$ és cert, o sigui, $(a) \Leftrightarrow (b)$ (és a dir, $(a) \Rightarrow (b)$ i $(b) \Rightarrow (a)$)

Vol dir que $(a) \leftrightarrow (c)$ és cert, o sigui, $(a) \Leftrightarrow (c)$ (és a dir, $(a) \Rightarrow (c)$ i $(c) \Rightarrow (a)$)

Vol dir que $(b) \leftrightarrow (c)$ és cert, o sigui, $(b) \Leftrightarrow (c)$ (és a dir, $(b) \Rightarrow (c)$ i $(c) \Rightarrow (b)$)

És a dir, que qualsevol de les afirmacions implica qualsevol altra afirmació.

En aquests casos, es pot intentar efectuar una demostració "circular" o "cíclica", amb el consegüent estalvi d'implicacions a demostrar (poden ser possibles rutes diferents, que triarem segons si sabem fer les demostracions corresponents o no):

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$$

$$(a) \Rightarrow (c) \Rightarrow (b) \Rightarrow (a)$$

Tot això es pot generalitzar a més de tres afirmacions.

En veurem exemples en una secció específica d'aquest mateix capítol.

En algunes ocasions, aconseguim anar "arrossegant" l'equivalència "des de A fins a B", i no cal procedir demostrant dues implicacions separades. En un capítol posterior, dedicat als conjunts, veurem exemples il·lustrant aquesta situació.

No totes les afirmacions que es volen demostrar s'expressen com a implicació o condicional, tot i que més d'un tipus s'hi pot reduir. Per exemple:

$A \vee B$ (A o B)

$A \wedge B$ (A i B)

Aquestes tipologies es tracten en seccions posteriors dintre del capítol.

6.2. Demostracions: mètode directe

Descripció del mètode

Si hem de demostrar $A \Rightarrow B$, la demostració consistirà a produir una seqüència encadenada d'argumentacions que ens portin de la hipòtesi (suposició de la veracitat de A) a la tesi (veracitat de B).

Es pot donar aquest esquema:

$$A \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow B$$

i així resulta $A \Rightarrow B$

En altres casos, no començarem per A sinó per algun altre resultat cert; A s'aplicarà en algun pas intermedi, i s'arribarà finalment a B.

$$A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow B$$

Als efectes formals, afegim A_1 a la hipòtesi (encara que A al principi no s'aplica):

$$(A \wedge A_1) \Rightarrow (A \wedge A_2) \Rightarrow \cdots (A \wedge A_{k-1}) \Rightarrow A_k \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow B$$

També es pot expressar així, que és el que passa realment:

$$\left.\begin{array}{r} A \\ A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_{k-1} \end{array}\right\} \Rightarrow A_k \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow B$$

També es podria descriure el procés com:

$$A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_{k-2} \Rightarrow (A \wedge A_{k-1}) \Rightarrow A_k \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow B,$$

encara que no sigui molt intuïtiu.

Exemples

Exemple 6.3 Vegem diversos exemples que es podrien demostrar directament (a, b són enters).

$2|a \Rightarrow 2|a^2$,

$2 \nmid a \Rightarrow 2 \nmid a^2$,

$3|a \Rightarrow 3|a^2$,

$3|a \Rightarrow 3|a^3$ ("el cub d'un enter múltiple de 3 és múltiple de 3"),

$3 \nmid a \Rightarrow 3 \nmid a^2$,

$13|a \Rightarrow 13|a^7$,

$(2|a \wedge 2|b) \Rightarrow 2|a-b$,

$(2 \nmid a \wedge 2 \nmid b) \Rightarrow 2|a-b$,

$(2 \nmid a \wedge 2|b) \Rightarrow 2 \nmid a-b$,

$(7|a \wedge 7|b) \Rightarrow 7|a+b$,

$(3|a \wedge 3|b) \Rightarrow 3|a+b$. ■

Vegem diversos exemples de demostració per un mètode directe.

Exemple 6.4 Vegem que

"el quadrat d'un nombre enter senar és senar"

Formalitzat (suposant n nombre enter), $2 \nmid n \Rightarrow 2 \nmid n^2$.

La hipòtesi és $2 \nmid n$.

La tesi és $2 \nmid n^2$.

Demostració. Per hipòtesi, i tenint en compte quina és l'expressió d'un nombre senar, existeix un enter k tal que $n = 2k+1$. Vegem que n^2 és del mateix tipus. Aplicant l'expressió anterior, $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ i, per tant, existeix k' enter tal que $n^2 = 2k'$, parell. És suficient prendre $k' = 2k^+2k$.

$2|n \Rightarrow 2|n^2$: Resulta fàcil seguir el mateix esquema per a demostrar $2|n \Rightarrow 2|n^2$. Per hipòtesi, i tenint en compte quina és l'expressió d'un nombre parell, existeix un enter k tal que $n = 2k$. Vegem que n^2 és del mateix tipus. Aplicant l'expressió anterior, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ i, per tant, existeix k' enter tal que $n^2 = 2k'$, parell. És suficient prendre $k' = 2k^2$.

Per arguments similars, es poden demostrar "directament" resultats com:

$3|a \Rightarrow 3|a^2$,

$3|a \Rightarrow 3|a^3$ ("el cub d'un enter múltiple de 3 és múltiple de 3"). ■

Exemple 6.5 Vegem que

"la suma de dos nombres enters senars és un nombre parell" .

Vegem, com a pràctica de simbolització, que aquest enunciat es pot formalitzar en diferents graus i de diferents maneres:

"Si a i b són nombres enters senars, aleshores $a+b$ és senar"

"Suposant a,b nombres enters: (a és senar $\wedge$ b és senar) $\rightarrow$ $a+b$ és parell"

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 2 \nmid a \wedge 2 \nmid b) \rightarrow 2|(a+b)$

$(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \rightarrow ((2 \nmid a \wedge 2 \nmid b) \rightarrow 2|(a+b))$

Siguin a,b nombres enters. Vegem que $(2 \nmid a \wedge 2 \nmid b) \rightarrow 2|(a+b)$, que és el nucli del que s'ha de demostrar.

Demostració

$2 \nmid a \Rightarrow a = 2k+1$ per a algun k enter

$2 \nmid b \Rightarrow b = 2k'+1$ per a algun k' enter

Per tant:

$a+b = (2k+1)+(2k'+1) = 2k+2k'+2 = 2(k+k'+1) = 2k''$, si $k'' = k+k'+1 \in \mathbb{Z}$.

En conseqüència, $a+b$ és un nombre parell.

Vegem-ne un redactat alternatiu, més verbalitzat.

Com que a,b són nombres enters senars, existeixen enters k,k' tals que $a = 2k+1$ i $b = 2k'+1$. Tenint en compte que els nombres parells són els múltiples de 2, hem de veure que existeix k'' enter tal que $a+b = 2k''$. En efecte, $a+b = (2k+1)+(2k'+1) = 2(k+k'+1) = 2k''$, amb $k'' = k+k'+1$.

Molts resultats anàlegs es poden *demostrar* semblantment.

Per exemple, $(3|a \wedge 3|b) \Rightarrow 3|a+b$ ("la suma de dos múltiples de 3 és múltiple de 3"). En efecte, per hipòtesi, existeixen enters k,k' tals que $a = 3k$ i $b = 3k$. En conseqüència, $a+b = 3k+3k' = 3(k+k') = 3k''$, amb $k'' = k+k'$ enter. Així, $3|a+b$. ■

Exemple 6.6 Considerem l'enunciat següent.

Siguin x,y nombres reals. Proveu que $(x-y)^2 = x^2-2xy+y^2$

La suposició que x,y són nombres reals permet utilitzar totes les propietats de la suma i del producte en els reals. L'estructura és d'un condicional; vegem-ne un possible enunciat alternatiu:

"Demostreu que, si x,y són nombres reals, aleshores $(x-y)^2 = x^2-2xy+y^2$".

x,y són nombres reals $\rightarrow (x-y)^2 = x^2-2xy+y^2$,

$(x \in \mathbb{R} \wedge y \in \mathbb{R}) \rightarrow (x-y)^2 = x^2-2xy+y^2$.

Demostració. Es fa servir que $a(-b) = -ab$, $a-b = a+(-b)$, $-(a+b) = -a-b$, entre altres propietats.

$(x-y)^2 = (x-y)(x-y)$
$= (x-y)x-(x-y)y$ (per la propietat distributiva del producte respecte de la suma),
$= (x^2-yx)-(xy-y^2)$ (per la propietat distributiva del producte respecte de la suma),
$= x^+(-yx-xy)+y^2$ (per la propietat associativa de la suma),
$= x^2-2xy+y^2$ (per la propietat commutativa de la suma).

El lector pot demostrar similarment resultats com:

Per a tot nombre real x, y, $(x+y)^2 = x^2+2xy+y^2 \Rightarrow xy = yx$.
Per a tot nombre real x, y, $(x+y)^3 = x^3+3x^2y+3xy^2+y^3$. ■

PROBLEMA 6.1

Sigui n un nombre enter. Proveu que, si $5|n$*, aleshores* $5|n^9$.

Solució. Hem de veure $5|n \Rightarrow 5|n^9$.

Per definició de divisibilitat, existeix un enter k tal que $n = 5k$. En conseqüència, $n^9 = (5k)^9$. Ara hem de veure que n^9 es pot expressar en la forma típica d'un múltiple de 5, és a dir, com a $n^9 = 5k'$ per a un k' enter convenient. En efecte, $n^9 = 5^9k^9 = 5 \cdot 5^8k^9 = 5k'$, múltiple de 5, amb $k' = 5^8k^9 \in \mathbb{Z}$.

Reescriptura expositiva:

$5|n$
$\Rightarrow \exists k(k \in \mathbb{Z} \wedge n = 5k)$
$\Rightarrow \exists k(k \in \mathbb{Z} \wedge n^9 = (5k)^9)$
$\Rightarrow \exists k(k \in \mathbb{Z} \wedge n^9 = 5 \cdot 5^8k^9)$
$\Rightarrow \exists k'(k' \in \mathbb{Z} \wedge n^9 = 5k')$ (amb $k' = 5^8k^9$)
$\Rightarrow 5|n^9$.

PROBLEMA 6.2

Demostreu que, per a tot $x, y \in \mathbb{R}$, $(x+y)(x-y) = x^2-y^2$.

Solució. Escrivim un enunciat complet, completament formalitzat:

$\forall x \forall y((x \in \mathbb{R} \wedge x \in \mathbb{R}) \rightarrow (x+y)(x-y) = x^2-y^2)$

Siguin x, y nombres reals arbitraris (però fixos per a la demostració). Cal veure $(x+y)(x-y) = x^2-y^2$.

De fet, si prescindim dels quantificadors, fixades x, y, cal demostrar:

$(x \in \mathbb{R} \wedge x \in \mathbb{R}) \Rightarrow (x+y)(x-y) = x^2-y^2$.

Així que tenim:

Hipòtesi: $x \in \mathbb{R} \wedge x \in \mathbb{R}$

Tesi: $(x+y)(x-y) = x^2 - y^2$.

La hipòtesi ens permet aplicar totes les propietats de les operacions de suma i producte en els nombres reals. També el detall de què s'aplica exactament, on i quan, ens permet veure a què és aplicable i que, per exemple, per a matrius quadrades, la demsotració no es pot mimetitzar, atès que no hi ha garantida la commutativitat del producte.

P1] $(x+y)(x-y) = (x+y)x + (x+y)(-y))$ (per distributivitat del producte respecte de la suma) i $x - y = x + (-y)$,

$\Downarrow$ (per distributivitat del producte respecte de la suma, dues vegades)

P2] $(x+y)(x-y) = (xx+yx) + (x(-y) + y(-y))$

$\Downarrow$ (per notació i altres propietats bàsiques)

P3] $(x+y)(x-y) = (x^2+yx) + (-xy - y^2)$

$\Downarrow$ (per associativitat de la suma, amb unes quantes maniobres)

P4] $(x+y)(x-y) = x^2 + (yx - xy) - y^2$

$\Downarrow$ (per commutativitat del producte)

P5] $(x+y)(x-y) = x^2 + 0 - y^2$

$\Downarrow$

P6] $(x+y)(x-y) = x^2 - y^2$.

Així, hem provat: $P1 \Rightarrow P2$, $P2 \Rightarrow P3, \ldots, P5 \Rightarrow P6$.

En resum: $P1 \Rightarrow P6$.

PROBLEMA 6.3

Proveu que, per a tot enter senar n, $4 | 13n^2 - 9$.

Solució. *Anàlisi de l'enunciat*. Formalment, l'enunciat complet és:

$\forall n(n \in \mathbb{Z} \rightarrow (2 \nmid n \rightarrow 4 | 13n^2 - 9))$ o bé:

$\forall n((n \in \mathbb{Z} \wedge 2 \nmid n) \rightarrow 4 | 13n^2 - 9))$ o bé:

$\forall n(2 \nmid n \rightarrow 4 | 13n^2 - 9)$ (suposant n enter)

Demostració. Per a la demostració, sigui n un enter fixat (tot i que arbitrari). Per a aquest enter, demostrarem:

$2 \nmid n \Rightarrow 4 | 13n^2 - 9$

Hipòtesi: $2 \nmid n$ (és a dir, n és senar, a més de ser enter)

Tesi: $4|13n^2-9$.

Essent n senar, $n=2k+1$ per a algun k enter (hipòtesi). Volem veure que existeix k' enter tal que $13n^2-9=4k'$ (tesi).

Idea de la demostració. Formalment:

$\exists k(n=2k+1) \rightarrow \exists k'(13n^2-9=4k')$

Substituint, resulta: $13n^2-9=13(2k+1)^2-9=13(4k^2+4k+1)-9=4(13k^2+13k)+(13-9)=4(13k^2+13k)+4=4(13k^2+13k+1)$. És suficient prendre $k'=13k^2+13k+1 \in \mathbb{Z}$ i en resulta $13n^2-9=4k'$, múltiple de 4.

Això prova l'enunciat.

A la secció següent, se'n veuen exemples addicionals, presentats conjuntament amb les demostracions dels contrarecíprocs respectius.

6.3. Prova d'enunciats del tipus $A \rightarrow B$. Mètode del contrarecíproc (indirecte)

Contrarecíproc per a proposicions. Equivalència lògica. Què és el contrarecíproc?

Ja hem vist anteriorment enunciats amb estructura de condicional, és a dir, $A \rightarrow B$, que hem demostrat per mètodes directes o per altres mètodes. Ara considerem el **mètode de demostració pel contrarecíproc**, que consisteix a demostrar la fórmula contrarecíproca equivalent.

El contrarecíproc de $A \rightarrow B$ és la fórmula o enunciat: $\neg B \rightarrow \neg A$

La relació entre un enunciat i el seu contrarecíproc és l'equivalència lògica, demostrada per a proposicions i, en general, fórmules proposicionals:

$$A \rightarrow B \equiv \neg B \rightarrow \neg A\ .$$

A, B poden ser enunciats complexos, amb negacions internes, condicionals, conjuncions o altres estructures.

Exemple 6.7 Quin és contrarecíproc de: $A \rightarrow \neg B$, $\neg A \rightarrow B$, $\neg A \rightarrow \neg B$, $\neg B \rightarrow A$?

Respectivament:

$\neg\neg B \rightarrow \neg A$, que equival a $B \rightarrow \neg A$,

$\neg B \rightarrow \neg\neg A$, que equival a $\neg B \rightarrow A$,

$\neg\neg B \to \neg\neg A$, que equival a $B \to A$,

$\neg A \to \neg\neg B$, que equival a $\neg A \to B$. ■

El concepte de contrarecíproc es pot estendre a fórmules de predicat que tinguin la mateixa estructura de condicional. Vegem-ne un exemple:

Exemple 6.8 Suposant $n \in \mathbb{Z}$, considerem l'enunciat

$2|n^2 \to 2|n$

El contrarecíproc és

$\neg(2|n) \to \neg(2|n^2)$, que, en aquest cas, es pot reescriure com

$2 \nmid n \to 2 \nmid n^2$

Les fórmules $2|n^2 \to 2|n$ i $2 \nmid n \to 2 \nmid n^2$ són equivalents (es pot veure per substitució o simplement pensant que n és fix).

Per tant, demostrar la certesa de qualsevol de les dues equival a demostrar la certesa de l'altra, és a dir:

$2|n^2 \to 2|n$ és cert si, i només si, $2 \nmid n \to 2 \nmid n^2$ és cert.

En termes d'implicació:

$2|n^2 \Rightarrow 2|n$ si, i només si, $2 \nmid n \Rightarrow 2 \nmid n^2$.

Observació: També es podria resoldre directament, sense demostració pel contrarecíproc. Vegem-ne algunes possibilitats:

Una possibilitat seria utilitzar el lema d'Euclides. Una altra, mitjançant una demostració directa: en efecte, de $n^2 = 2k+1$, podem escriure $n^2 - 1 = 2k$, és a dir, $n^2 - 1^2 = 2k$, d'on $2k = (n-1)(n+1)$. Així, $2|(n-1)(n+1)$. Per tant, 2 ha de dividir algun dels factors (de fet, els dos, ja que la diferència entre els factors és 2 $(n+1-(n-1)=2)$ i, per tant, si un d'ells és parell, l'altre també). Suposem, doncs, que $2|n-1$. Per definició de divisibilitat, existeix k' enter tal que $n-1 = 2k'$, d'on $n = 2k'+1$, senar, com havíem de veure. ■

Observació. L'equivalència del contrarecíproc es pot utilitzar a l'interior d'una fórmula, en subfórmules amb estructura de condicional, obtenint una nova fórmula lògicament equivalent a la inicial. Així, són lògicament equivalents:

$r \to (p \to q) \equiv (r \to (\neg q \to \neg p))$.

Vegem-ne un altre exemple:

$\forall x(P(x) \to Q(x))$ equival a $\forall x(\neg Q(x) \to \neg P(x))$

$\forall n(5|n^7 \to 5|n)$ equival a $\forall n(5 \nmid n \to 5 \nmid n^7)$.

En què consisteix el mètode

L'equivalència del contrarecíproc és la base del mètode de demostració del mateix nom. Normalment, s'utilitza s'ha de demostrar $A \Rightarrow B$ i resulta difícil o no se sap com abordar la demostració. Si, en canvi, resulta fàcil demostrar $\neg B \Rightarrow \neg A$, demostrant $\neg B \Rightarrow \neg A$ resulta provat $A \Rightarrow B$.

Per tant, demostrar una de les implicacions equival a demostrar l'altra, és a dir:

$A \Rightarrow B$ si, i només si, $\neg B \Rightarrow \neg A$.

Aquest és l'interès de l'equivalència, de la qual deriva un mètode de demostració, el de les demostracions pel contrarecíproc:

DESCRIPCIÓ DEL MÈTODE:

- "Demostrar $A \Rightarrow B$ pel contrarecíproc o pel mètode del contrarecíproc és demostrar (equivalentment) $\neg B \Rightarrow \neg A$".
- "Demostrar que $A \to B$ *és cert* pel contrarecíproc o pel mètode del contrarecíproc és demostrar (equivalentment) que $\neg B \to \neg A$ *és cert*".
- "Demostrar que, *si A és cert, aleshores B és cert* pel contrarecíproc o pel mètode del contrarecíproc és demostrar (equivalentment) que, *si ¬B és cert, aleshores ¬A és cert*".

Exemple 6.9 Sigui n un nombre enter.

Demostrar $2|n^{13} \Rightarrow 2|n$ ("difícil") pel contrarecíproc és demostrar $2 \nmid n \Rightarrow 2 \nmid n^{13}$ ("fàcil").

Observació. El mètode és un exemple de **reducció d'un problema a un altre**, ja resolt o que es preveu saber resoldre o que resulta més fàcil de resoldre.

Observació. El contrarecíproc d'un enunciat pot provar-se pels mètodes que ens semblin possibles o convenients: demostració directa, directa per casos, per reducció a l'absurd o altres. La prova del contrarecíproc és un nou problema, que podem abordar independentment de l'origen.

Observació: *Contrarecíproc del contrarecíproc*. El contrarecíproc del contrarecíproc és l'enunciat original. Vegem-ho:

Enunciat original: $p \to q$

Contrarecíproc: $\neg q \to \neg p$

Contrarecíproc del contrarecíproc:

$\neg(\neg p) \to \neg(\neg q)$, que és equivalent a

$p \to q$.

Així doncs, a efectes de demostració, no guanyem res considerant el contrarecíproc del contrarecíproc, ja que recuperem l'enunciat inicial; no té cap utilitat pràctica.

Exemples de parelles "enunciat–contrarecíproc"

Abans de presentar exemples de demostració per aquest mètode, vegem exemples d'enunciats i del seu contrarecíproc. Suposem que totes les variables que hi apareixen són nombres enters (de $U = \mathbb{Z}$):

a) "Si plou i no sóc a aixopluc, em mullo",
Contrarecíproc: "Si no em mullo, aleshores o bé no plou o bé estic a aixopluc" (hem fer servir De Morgan i doble negació).

b) "Si ja són les 12 del matí, ja sóc esmorzat",
Contrarecíproc: "Si no sóc esmorzat, encara no són les 12 del matí".

c) "Si és festa, en Josep va al cinema",
Contrarecíproc: "Si en Josep no va al cinema, aleshores no és festa".

d) "Si els víkings no han atacat el convent, Ermessenda conrea el jardí de plantes medicinals",
Contrarecíproc: "Si Ermessenda no conrea el jardí de plantes medicinals, aleshores els víkings han atacat el convent" (hem fet servir doble negació).

e) "Si n és parell, aleshores n^2 és parell",
Contrarecíproc: "si n^2 no és parell, aleshores n no és parell", o bé:
"si n^2 és senar, aleshores n és senar".

f) "Si $n < 2$, aleshores n no és primer",
Contrarecíproc: "Si n és primer, aleshores $n \geq 2$".

g) $2|n^2 \to 2|n$ (si n^2 és parell, aleshores n és parell),
Contrarecíproc: $\neg(2|n) \to \neg(2|n^2)$ (si n no és parell, aleshores n^2 no és parell).
$2 \nmid n \to 2 \nmid n^2$ (si n és senar, aleshores n^2 és senar).

h) $2|n^7 \to 2|n$ (si n^7 és parell, aleshores n és parell),
Contrarecíproc: $2 \nmid n \to 2 \nmid n^7$.

i) $2|n^3 \to 2|n$,
Contrarecíproc: $2 \nmid n \to 2 \nmid n^3$.

j) $2 \nmid n^2 \to 2 \nmid n$ (si n^2 és senar, aleshores n és senar),
Contrarecíproc: $2|n \to 2|n^2$ (si n és parell, aleshores n^2 és parell).

k) $2|ab \to (2|a \vee 2|b)$ (si el producte de dos nombres naturals és parell, aleshores algun dels factors també ho és),
Contrarecíproc: $\neg(2|a \vee 2|b) \to 2 \nmid ab$.
El contrarecíproc es pot modificar en un enunciat equivalent utilitzant De Morgan:
$(\neg 2|a \wedge \neg 2|b) \to 2 \nmid ab$
$(2 \nmid a \wedge 2 \nmid b) \to 2 \nmid ab$ ("el producte de dos enters senars és senar", o bé "si dos enters són senars, aleshores el producte és senar").

Exemples d'aplicació del mètode

Exemple 6.10 Sigui $n \in \mathbb{Z}$. Proveu que $2 \nmid n^2 \Rightarrow 2 \nmid n$ ("Si n^2 és un nombre senar, n és també un nombre senar").

Si partim de la hipòtesi, podem escriure $n^2 = 2k+1$, per a un enter k convenient. Però suposem que aquí quedem encallats i imaginem que no es veu clar com continuar, ja que hem de deduir una expressió del mateix tipus però per a n.

Formulem el contrarecíproc: $\neg(2 \nmid n) \to \neg(2 \nmid n^2)$, és a dir, $2|n \to 2|n^2$, que hem de demostrar que és cert. És a dir, hem de provar $2|n \Rightarrow 2|n^2$. És abordable sense gaires dificultats, cosa que fem a continuació:

Demostració (ara directa! del contrarecíproc) de $2|n \Rightarrow 2|n^2$.

Sigui n enter parell.

Aleshores existeix un k enter tal que $n = 2k$.

Calculem n^2 substituint n per l'expressió anterior: $n^2 = (2k)^2 = 4k^2$.

És $n^2 = 4k^2 = 2(2k^2) = 2k'$, escollint $k' = 2k^2 \in \mathbb{Z}$.

Per tant, existeix un k' enter tal que $n^2 = 2k'$ i, en conseqüència:

n^2 és parell.

Observació. Podem demostrar de la mateixa manera resultats similars, com per exemple $3 \nmid n^2 \Rightarrow 3 \nmid n$, $2 \nmid n^7 \Rightarrow 2 \nmid n$, $5 \nmid n^8 \Rightarrow 5 \nmid n$. ■

Exemple 6.11 Sigui $n \in \mathbb{Z}$. Proveu que $2|n^2 \Rightarrow 2|n$ ("Si n^2 és un nombre parell, n és també un nombre parell").

Partir de $n^2 = 2k$ no sembla prometedor per a arribar a $n = 2k'$ (encallats, tot i que es pot justificar pel lema d'Euclides). Ho provem amb el contrarecíproc:

$2 \nmid n \to 2 \nmid n^2$

Demostració (ara directa del contrarecíproc) de $2 \nmid n \Rightarrow 2 \nmid n^2$.

Sigui n un enter senar.

Aleshores, existeix un k enter tal que $n = 2k+1$.

Calculem n^2 substituint n per l'expressió anterior: $n^2 = (2k+1)^2 = 4k^2+4k+1$.

Observem que $n^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ (en un intent d'expressar n^2 en la forma típica d'un nombre senar).

Escollint $k' = 2k^2+2k \in \mathbb{Z}$, resulta $n^2 = 2(2k^2+2k)+1 = 2k'+1$.

Per tant, existeix k' enter tal que $n^2 = 2k'+1$ i, en conseqüència:

n^2 és senar. ■

Exemple 6.12 Siguin $a, b \in \mathbb{Z}$. Demostreu que $2|ab \Rightarrow (2|a \vee 2|b)$ $(2|ab \Rightarrow (2|a \text{ o } 2|b))$.

Escriure $2|ab$ com "existeix un enter k tal que $ab = 2k$" no sembla que ens permeti avançar en la resolució del problema (tot i que es podria aplicar el lema d'Euclides). Vegem si la situació millora considerant l'equivalent contrarecíproc (que esperem poder demostrar i resoldre així el problema). El contrarecíproc és

$$\neg(2|a \vee 2|b) \rightarrow \neg 2|ab$$

$$\neg(2|a \vee 2|b) \rightarrow 2 \nmid ab$$

Per poder treballar, considerem l'equivalent derivat de l'aplicació de De Morgan:

$$(\neg(2|a) \wedge \neg(2|b)) \rightarrow 2 \nmid ab$$

$$(2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab$$

Equival a dir que el producte de dos enters senars és un nombre senar. Suposant que no disposem d'una demostració ja feta d'aquest resultat anteriorment, resulta fàcil fer-la ara:

$2 \nmid a \Rightarrow$ existeix $k \in \mathbb{Z}$ tal que $a = 2k+1$

$2 \nmid b \Rightarrow$ existeix $k' \in \mathbb{Z}$ tal que $b = 2k'+1$

Per tant (existeixen k, k' enters tals que):

$$ab = (2k+1)(2k'+1) = 4kk' + 2k + 2k' + 1$$

Vegem com el podem escriure en forma senar:

$ab = 4kk' + 2k + 2k' + 1 = 2(2kk' + k + k') + 1 = 2k'' + 1$, escollint $k'' = 2kk' + k + k'$ enter.

Per tant, existeix k'' enter tal que $ab = 2k' + 1$.

En conseqüència, ab és senar.

Una altra versió més formalitzada, que podem escriure després del desenvolupament anterior:

$(2 \nmid a \wedge 2 \nmid b) \Rightarrow$

$\Rightarrow \exists k \exists k' (k \in \mathbb{Z} \wedge k' \in \mathbb{Z} \wedge a = 2k+1 \wedge b = 2k'+1)$

$\Rightarrow \exists k \exists k' (k \in \mathbb{Z} \wedge k' \in \mathbb{Z} \wedge ab = 2(2kk' + k + k') + 1)$

$\Rightarrow \exists k'' (k'' \in \mathbb{Z} \wedge ab = 2k'' + 1)$ (amb $k'' = 2kk' + k + k'$)

$\Rightarrow 2 \nmid ab$. ■

Exemple 6.13 Sigui n un nombre enter.

Proveu pel mètode del contrarecíproc: $3n+7$ senar $\Rightarrow n+4$ parell.

Formulem el contrarecíproc: $n+4$ senar $\Rightarrow 3n+7$ parell.

Fem una demostració “directa” del contrarecíproc:

Per hipòtesi, existeix un enter k tal que $n+4=2k+1$. D’aquí resulta $n=2k+1-4=2k-3$. Substituint, tindrem $3n+7=3(2k-3)+7=6k-9+7=6k-2=2(3k-1)=2k'$, parell (amb $k'=3k-1$). ■

Exemple 6.14 Sigui n un nombre enter.

Proveu pel mètode del contrarecíproc: $7n+1$ senar $\Rightarrow n+1$ senar.

Formulem el contrarecíproc: $n+1$ parell $\Rightarrow 7n+1$ parell.

Fem una demostració “directa” del contrarecíproc:

Per hipòtesi, existeix un enter k tal que $n+1=2k$. D’aquí resulta $n=2k-1$. Substituint, tindrem $7n+1=7(2k-1)+1=14k-7+1=14k-6=2(7k-3)=2k'$, parell (amb $k'=7k-3$). ■

6.4. Demostració per casos

En què consisteix el mètode?

De vegades, la demostració de propietats pot no ser fàcil de fer per la variació de possibilitats, que no es poden tractar totes alhora, barrejades, d’un sol cop, globalment.

En aquestes situacions, la idea és descompondre el problema en una col·lecció de subproblemes, corresponents a condicions, que es resoldran separadament. Se suposa que cada problema és més fàcil de resoldre que el global complet, ja que només hem de tractar amb una condició. És una simplificació en la resolució, ja que esperem que cada cas sigui més tractable o més abordable o més fàcil que el general; destriem les situacions diferents que es poden donar i les resolem cada una separadament, cas per cas, una per una. Cada cas, un subproblema.

Quins poden ser els casos? De quina tipologia? No es pot afirmar res en general. Com a exemple, sovint resulta còmode fer una distinció de casos segons la paritat d’un paràmetre, sobretot si el resultat que es vol demostrar és sobre la paritat d’alguna expressió.

Els casos normalment no vénen explicitats a l’enunciat; no s’especifica quins serien els casos convenients per considerar, ni la condició o propietat en què es basen els diversos casos. De manera que és feina creativa de qui resol el problema buscar, intuir i proposar els casos possibles, lligats al problema, de manera que es vegi factible la demostració per a cada un d’ells.

Exemple 6.15 Vegem-ne un exemple molt senzill:

“*donats dos enters consecutius, exactament un és parell*” (i, en conseqüència, el seu producte és parell).

Resolució. Siguin $n, n+1$ dos enters consecutius (anàlogament seria per a parelles tals com $n-1, n$ o altres variants).

Efectuarem una demostració *per casos*, casos segons la paritat de n, és a dir, segons si és parell o senar.

Cas 1. Si n és parell, ja està.

Cas 2. Si n és senar, aleshores $n+1$ és parell, per ser la suma de dos senars (o també: $n = 2k+1$ per a un cert enter k, d'on $n+1 = (2k+1)+1 = 2k+2 = 2(k+1) = 2k'$, parell, amb $k' = k+1 \in \mathbb{Z}$). ■

En una altra situació, sobretot si ens trobem davant d'un resultat de divisibilitat, podem intentar fer una distinció segons els valors dels residu d'una divisió entera, com podem veure a l'exemple següent (tot i que l'anterior distinció de paritat és, de fet, sobre divisibilitat per 2).

Exemple 6.16 *Exemple senzill*. Considerem la propietat:

D: "*D'entre cada tres enters consecutius hi ha exactament un múltiple de 3*".

Resolució. Podem suposar, *sense pèrdua de generalitat*, que els nombres enters consecutius són $n, n+1, n+2$. També seria possible considerar ternes com $n-1, n, n+1$ o $n-2, n-1, n$.

Considerem la divisió entera de n per 3: existeixen enters q, r únics que satisfan

$n = 3q + r$, $0 \leq r < 3$ (que equival a $0 \leq r \leq 2$, ja que r és enter).

És a dir, que $r = 0$ o $r = 1$ o $r = 2$. I aquests són els casos sobre els quals construirem la demostració. Observeu que es cobreixen totes les possibilitats.

Cas 1 ($r = 0$). Suposem que $r = 0$. Aleshores $n = 3q$, $n+1 = 3q+1$, $n+2 = 3q+2$ (l'únic múltiple de 3 és n, en aquest cas).

Cas 2 ($r = 1$). Suposem que $r = 1$. Aleshores $n = 3q+1$, $n+1 = 3q+2$, $n+2 = 3q+3 = 3(q+1)$ (l'únic múltiple de 3 és $n+3$, en aquest cas).

Cas 3 ($r = 2$). Suposem que $r = 2$. Aleshores $n = 3q+2$, $n+1 = 3q+3 = 3(q+1)$, $n+2 = 3q+4 = 3(q+1)+1$ (l'únic múltiple de 3 és $n+2$, en aquest cas).

Observeu que **cada cas separadament, tot sol, implica la conclusió**.

Veurem el mateix enunciat resolt posteriorment per reducció a l'absurd.

Vegeu-ne un resultat relacionat:

'Tot nombre enter és o bé múltiple de 3, o bé múltiple de 3 més 1, o bé múltiple de 3 menys 1." ■

Anàlisi de l'estructura demostrativa de l'exemple anterior

Denotem per C_1 la propietat $r = 0$, per C_2 la propietat $r = 1$ i per C_3 la propietat $r = 3$.

Formalment, si denotem els casos per C_1... (són les propietats diverses a què corresponen o que defineixen els casos), considerem $C_1 \vee C_2 \vee C_3$ i hem de demostrar

$$(C_1 \vee C_2 \vee C_2) \Rightarrow D,$$

és a dir:

$$(r = 0 \vee r = 1 \vee r = 2) \Rightarrow D.$$

Cada cas ha d'implicar la conclusió, separadament dels altres. És a dir:

$C_1 \Rightarrow D \quad (r = 0 \Rightarrow D)$

$C_2 \Rightarrow D \quad (r = 1 \Rightarrow D)$

$C_3 \Rightarrow D \quad (r = 2 \Rightarrow D)$

És a dir, es compleix

$$(C_1 \to D) \wedge (C_2 \to D) \wedge (C_3 \to D).$$

L'esquema demostratiu es basa formalment en les equivalències:

$(C_1 \vee C_2) \to D \equiv (C_1 \to D) \wedge (C_2 \to D)$ (2 casos).

$(C_1 \vee C_2 \vee C_3) \to D \equiv (C_1 \to D) \wedge (C_2 \to D) \wedge (C_3 \to D)$ (3 casos).

$(C_1 \vee \cdots \vee C_n) \to D \equiv (C_1 \to D) \wedge \cdots \wedge (C_n \to D)$ (n casos).

Vegem la deducció de l'equivalència (més formalment, s'hauria de veure per inducció):

$(C_1 \vee \cdots \vee C_n) \to D$

$\equiv \neg(C_1 \vee \cdots \vee C_n) \vee D$ (per l'equivalència $A \to B \equiv \neg A \vee B$)

$\equiv (\neg C_1 \wedge \cdots \wedge \neg C_n) \vee D$ (per De Morgan generalitzat)

$\equiv (\neg C_1 \vee D) \wedge \cdots \wedge (\neg C_n \vee D)$ (per distributivitat generalitzada de $\vee$ respecte de $\wedge$)

$\equiv (C_1 \to D) \wedge \cdots \wedge (C_n \to D)$ (per l'equivalència $A \to B \equiv \neg A \vee B$)

Recordeu que els casos que es considerin han de cobrir totes les possibilitats

Resumint:

Suposem que hem de demostrar $C \Rightarrow Q$.

a) Es descompon C en una disjunció de condicions, $C \equiv C_1 \vee \cdots \vee C_n$.
b) Cada C_i correspon a un cas possible.
c) El conjunt de casos $C_1, \cdots, C_n$ ha de cobrir totes les possibilitats.
d) Cal provar totes les implicacions següents (és a dir, una conjunció d'implicacions):

$$C_1 \Rightarrow Q$$
$$\vdots$$
$$C_n \Rightarrow Q$$

Si l'enunciat es formula només com a "demostreu Q"

(per exemple, $3|n(n+1)(n+2)$ per a n enter),

aleshores hem de buscar els casos $C_1, \cdots, C_n$ convenients i provar

$$C_1 \Rightarrow Q$$
$$\vdots$$
$$C_n \Rightarrow Q$$

Això deixarà demostrat: $(C_1 \vee \cdots \vee C_n) \Rightarrow Q$.

L'exemple anterior és d'aquest tipus. Vegem un exemple addicional d'aquesta idea:

Exemple 6.17 Suposem que es tracta de demostrar $2|n(n+1)$ per a n enter. Es pot reformular com $n \in \mathbb{Z} \Rightarrow 2|n(n+1)$. Atès que $n \in \mathbb{Z} \equiv (2|n \vee 2 \nmid n)$, el resultat equival a $(2|n \vee 2 \nmid n) \Rightarrow 2|n(n+1)$, que equival a $(2|n \Rightarrow 2|n(n+1)) \wedge (2 \nmid n \Rightarrow 2|n(n+1))$. Cal demostrar separadament:

$2|n \Rightarrow 2|n(n+1)$ (Cas 1: $2|n$)

$2 \nmid n \Rightarrow 2|n(n+1)$ (Cas 2: $2 \nmid n$)

Formalment:

$C = n \in \mathbb{Z}$

$C_1 = 2|n$

$C_2 = 2 \nmid n$

$C = C_1 \vee C_2$

Cal veure $C \Rightarrow 2|n(n+1)$, és a dir:

$C_1 \vee C_2 \Rightarrow 2|n(n+1)$

Cal provar:

$(C_1 \to 2|n(n+1)) \wedge (C_2 \to 2|n(n+1))$ és cert.

$C_1 \Rightarrow 2|n(n+1)$ i $(C_2 \Rightarrow 2|n(n+1)$. ■

Exemples

Mostrarem la idea del mètode amb diversos exemples.

Exemple 6.18 Proveu que, si x, y són nombres reals, aleshores $\text{màx}(x,y)+\text{mín}(x,y) = x+y$.

Resolució. Si intentem resoldre directament el problema, la dificultat és que no podem atribuir cap valor a $\text{màx}(x,y)$ ni $\text{mín}(x,y)$, ja que depèn de quin sigui el més gran dels dos: això ens dóna la clau de considerar casos, i ens diu quins i respecte de què.

Cas 1 ($x \geq y$). Si $x \geq y$, és $\text{màx}(x,y) = x$ i $\text{mín}(x,y) = y$, d'on

$\text{màx}(x,y)+\text{mín}(x,y) = x+y$.

Altres presentacions expositives:

$$x \geq y \Rightarrow \left\{ \begin{array}{l} \text{màx}(x,y) = x \\ \text{mín}(x,y) = y) \end{array} \right\} \Rightarrow \text{màx}(x,y)+\text{mín}(x,y) = x+y$$

Cas 2 ($x < y$). Si $x < y$, és $\text{màx}(x,y) = y$ i $\text{mín}(x,y) = x$, d'on

$\text{màx}(x,y)+\text{mín}(x,y) = y+x = x+y$.

Estructura demostrativa. Tenim:

$x \geq y \Rightarrow \text{màx}(x,y)+\text{mín}(x,y) = x+y$
$x < y \Rightarrow \text{màx}(x,y)+\text{mín}(x,y) = x+y$

O sigui:

$(x \geq y \vee x < y) \Rightarrow \text{màx}(x,y)+\text{mín}(x,y) = x+y$

$(x \in \mathbb{R} \wedge y \in \mathbb{R}) \Rightarrow (x \geq y \vee x < y) \Rightarrow \text{màx}(x,y)+\text{mín}(x,y) = x+y$

És a dir, si denotem per

$C_1 = (x \geq y)$
$C_2 = (x < y)$

$D = (\text{màx}(x,y) + \text{mín}(x,y) = x + y)$, aleshores hem provat:

$(C_1 \vee C_2) \Rightarrow D$, ja que hem provat

$(C_1 \to D) \wedge (C_2 \to D)$

Recordem l'equivalència:

$(C_1 \vee C_2) \to D \equiv (C_1 \to D) \wedge (C_2 \to D)$.

Són possibles altres formulacions:

1. $x \leq y, x \nleq y$ $(x > y)$ (2 casos)
2. $x < y, x = y, x > y$ (3 casos). ■

Diversos problemes

PROBLEMA 6.4

Sigui n un nombre enter. Provem que $2|5n^2 - 3n + 4$ *fent una demostració per casos.*

Solució. *Idea per a la resolució*. Es pot reexpressar dient que $5n^2 - 3n + 4$ és parell.

Casos respecte de quin criteri? Un possible criteri pot ser el de la paritat de n, atesa la tipologia del resultat, de la conclusió. Per tant, considerarem la possibilitat que n sigui parell o que sigui senar.

S'ha resolt anteriorment un enunciat similar, per casos, escrivint $n = 2k$ (cas de n parell) i $n = 2k + 1$ (cas de n senar), amb substitució posterior a la fórmula. Aquí adoptem una altra idea, en què fem servir resultats ben coneguts de paritat, d'altra banda justificats als capítols preliminars.

Cas 1 (n és parell). Si n és parell, en una demostració independent s'ha provat que n^2 també és parell. També és deduïble que n^2 és parell expressant-lo com a producte $n^2 = n \cdot n$ i aplicant que el producte de dos parells és parell.

El sumand $5n^2$ és parell per ser producte amb un parell (n^2).

El producte $3n$ és parell per ser producte amb un factor parell.

Així, tenim que $5n^2 - 3n + 4$ és suma de tres nombres parells i, per tant, és parell.

Cas 2 (n és senar). Anteriorment, i independentment, s'ha provat $2 \nmid n \Rightarrow 2 \nmid n^2$, de manera que, essent n senar, resulta n^2 senar i, per tant, $5n^2$ és senar, com a producte de dos senars (alternativament, també resulta senar si es veu com a producte de tres senars: $5 \cdot n \cdot n$).

Com a producte de dos senars, $3n$ és senar.

La diferència de dos senars és parell i, per tant, $5n^2 - 3n$ és parell.

Finalment, $5n^2 - 3n + 4 = (5n^2 - 3n) + 4$, suma de dos parells, és parell.

En tots els casos possibles, el nombre és parell.

PROBLEMA 6.5

Sigui n un nombre enter. Demostreu que $2|n^2 + 3n + 4$.

Solució. Demostrarem el resultat per casos segons la paritat de n.

Cas 1 $2|n$ (n és parell). Aleshores existeix $k \in \mathbb{Z}$ tal que $n = 2k$. Substituint a la fórmula, resulta $n^2 + 3n + 4 = (2k)^2 + 3(2k) + 4 = 4k^2 + 2(3k) + 4 = 2(2k^2 + 3k + 2) = 2k'$, amb $k' = 2k^2 + 3k + 2 \in \mathbb{Z}$. Així $n^2 + 3n + 4$ és parell.

Hem provat $2|n \Rightarrow 2|n^2 + 3n + 4$

Cas 2 $2 \nmid n$ (n és senar). Aleshores existeix $k \in \mathbb{Z}$ tal que $n = 2k + 1$. Substituint a la fórmula, s'obté $n^2+3n+4 = (2k+1)^2+3(2k+1)+4 = (4k^2+4k+1)+(6k+3)+4 = 2(2k^2 + 5k + 4) = 2k'$, amb $k' = 2k^2 + 5k + 4 \in \mathbb{Z}$. Així, $n^2 + 3n + 4$ és parell.

Hem provat $2 \nmid n \Rightarrow 2|n^2 + 3n + 4$.

No hi ha més casos.

Observació. La distinció segons paritat es pot situar amb més generalitat, de manera que el mètode sigui aplicable a casos més complicats, com el següent, en què s'ha de provar $3|a^3 - a$. La paritat de m es pot formular segons els valors del residu de la divisió entera $m = 2q + r$, $0 \le r < 2$, és a dir, $0 \le r \le 1$. Així:

m és parell si, i només si $r = 0$

m és senar si, i només si $r = 1$

És, doncs, un cas particular de distinció de casos per al residu de la divisió entera per 2.

Altres variants argumentals

Variant 1. Escrivim $n^2 + 3n + 4 = n(n+3) + 4$.

Si n és parell, també ho és $n(n+3)$ i, per tant, també $n(n+3)+4$, perquè és suma de parells.

Si n és senar, $n+3$ és parell, per ser suma de dos senars. El producte $n(n+3)$ és parell, i també $n(n+3)+4$, per ser suma de parells.

Variant 2. $n^2 + 3n + 4 = n(n+3) + 4 = n((n+1)+2) + 4 = n(n+1) + 2n + 4$. Els nombres n, $n+1$ són consecutius. Per tant, un dels dos és parell, de manera que $n(n+1)$ és parell. D'altra banda, $2n$ i 4 són parells. Atès que la suma de parells és un nombre parell, és $n^2 + 3n + 4$ parell. No s'ha resolt per casos, llevat que es vulgui demostrar per casos que "$n(n+1)$ és parell" (segons paritat de n).

PROBLEMA 6.6

Sigui a un nombre enter. Demostreu que $3|a^3-a$.

Solució. No sembla que una distinció segons paritat de a porti enlloc (per exemple, es pot comprovar en el cas a parell). Fem una distinció de casos lligada a la divisibilitat o no-divisibilitat per 3; la no divisibilitat dóna lloc a considerar diversos casos.

Considerem la divisió entera de a per 3: $a = 3q+r$, on $0 \leq r < 3$, és a dir, $0 \leq r \leq 2$. Fem una demostració per distinció de casos segons els possibles valors del residu r de la divisió entera.

Cas 1 ($r=0$). $r=0 \Rightarrow a=3q \Rightarrow a^3-a=(3q)^3-(3q)=3(3^2q^3-q)=3q'$, múltiple de 3.

Cas 2 ($r=1$). En aquest cas, $a=3q+1$ i, per tant, $a^3-a=(3q+1)^3-(3q+1)=(3q)^3+3(3q)^2+3(3q)+1-(3q+1)=3(3^2q^3+3^2q^2+6q)=3q'$, múltiple de 3.

Cas 3 ($r=2$). En aquest cas, $a=3q+2$ i, per tant, $a^3-a=(3q+2)^3-(3q+2)=3q'+6=3(q'+2)=3q''$, múltiple de 3.

Així, en *cada cas* resulta $3|a^3-a$ i, per tant, la propietat queda demostrada.

Observació: El resultat també es pot demostrar directament tenint en compte

$$a^3-a=a(a^2-1)=a(a^2-1^2=a(a+1)(a-1))=(a-1)a(a+1),$$

expressat com a producte de tres enters consecutius. Ara bé, donats tres enters consecutius, exactament un és múltiple de 3 i, per tant, el producte és múltiple de 3 (com s'ha demostrat al principi de la secció).

PROBLEMA 6.7

"La suma de dos nombres enters de la mateixa paritat és parell"
Suposant a,b enters:

$$((2|a \wedge 2|b) \vee ((2\nmid a \wedge 2\nmid b)) \rightarrow 2|(a+b)$$

Solució. En aquesta última forma, ja s'estan explicitant els casos que s'han de considerar. Cada cas dóna lloc a un (sub)problema separat, que resoldrem separadament. Observeu que es cobreixen totes les possibilitats.

Cas 1. La paritat comuna dels dos nombres és parell ("els dos nombres són parells").

Cas 2. La paritat comuna dels dos nombres és senar ("els dos nombres són senars").

Concretem i resolem separadament cas per cas:

Cas 1. S'ha de demostrar $(2|a \wedge 2|b) \Rightarrow 2|(a+b)$.

En efecte, essent a i b parells, podem escriure $a=2k$ i $b=2k'$, per a nombres enters k,k' adequats, d'on resulta $a+b=2k+2k'=2(k+k')=2k''$, parell (amb $k''=k+k' \in \mathbb{Z}$).

Cas 2. S'ha de demostrar $(2 \nmid a \wedge 2 \nmid b) \Rightarrow 2|(a+b)$.

En efecte, essent a i b senars, podem escriure $a = 2k+1$ i $b = 2k'+1$, per a nombres enters k, k' adequats, d'on resulta $a+b = (2k+1)+(2k'+1) = 2k+2k'+2 = 2(k+k'+1) = 2k''$, parell (amb $k'' = k+k'+1 \in \mathbb{Z}$).

Estructura-estratègia demostrativa. Noteu que el que hem demostrat és que són certes:

$(2|a \wedge 2|b) \rightarrow 2|(a+b)$ i

$(2 \nmid a \wedge 2 \nmid b) \rightarrow 2|(a+b)$,

és a dir, que és cert

$((2|a \wedge 2|b) \rightarrow 2|(a+b)) \wedge ((2 \nmid a \wedge 2 \nmid b) \rightarrow 2|(a+b))$,

quan havíem de demostrar la disjunció

$((2|a \wedge 2|b) \vee ((2 \nmid a \wedge 2 \nmid b)) \rightarrow 2|(a+b)$. Ara bé, això no és contradictori per l'equivalència lògica que es comenta a continuació.

A la demostració per casos, demostrem (per exemple, per a 2, però generalitzable a n):

$C_1 \rightarrow W$
$C_2 \rightarrow W$

és a dir:

$(C_1 \rightarrow W) \wedge (C_2 \rightarrow W)$

Considerant una de les equivalències lògiques:

$(C_1 \vee C_2) \rightarrow W \equiv (C_1 \rightarrow W) \wedge (C_2 \rightarrow W)$,

la demostració de $(C_1 \rightarrow W) \wedge (C_2 \rightarrow W)$ equival a la demostració de

$(C_1 \vee C_2) \rightarrow W$.

PROBLEMA 6.8

Siguin a, b nombres reals.
Aleshores:

a) $\text{màx}(a,b) = \dfrac{a+b+|a-b|}{2}$

b) $\text{mín}(a,b) = \dfrac{a+b-|a-b|}{2}$

Solució

a) Fem una distinció de casos de resultes de la comparació entre a i b. Vegem que en cada cas coincideixen els valors dels membres de l'esquerra i de la dreta de la igualtat.

Cas 1. $a \geq b$. Aleshores, per una banda, és $\text{màx}(a,b) = a$ i, per l'altra, tenim

$a \geq b \Rightarrow a - b \geq 0 \Rightarrow |a-b| = a - b \Rightarrow \frac{a+b+|a-b|}{2} = \frac{a+b+(a-b)}{2} = \frac{2a}{2} = a$, coincidents.

Cas 2. $a < b$. Aleshores, per una banda, és $\text{màx}(a,b) = b$ i, per l'altra, tenim

$a < b \Rightarrow a - b < 0 \Rightarrow |a-b| = -(a-b) = b - a \Rightarrow \frac{a+b+|a-b|}{2} = \frac{a+b+(b-a)}{2} = \frac{2b}{2} = b$, coincidents.

Estructura-anàlisi de la demostració. En el cas 1, hem provat

$a \geq b \Rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2}$,

és a dir, que

$a \geq b \rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2}$ és cert.

En el cas 2, hem provat $a < b \Rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2}$, és a dir, que

$a < b \rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2}$ és cert.

En conjunt, hem provat que és cert:

$(a \geq b \rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2}) \wedge (a < b \rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2})$.

És a dir

$(a \geq b \vee a < b) \rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2}$, és a dir,

$(a \in \mathbb{R} \wedge b \in \mathbb{R}) \rightarrow \text{màx}(a,b) = \frac{a+b+|a-b|}{2}$.

b) Es demostra anàlogament a l'apartat anterior:

Cas 1. $a \geq b$. Aleshores, per una banda, és $\text{mín}(a,b) = b$ i, per l'altra, tenim

$a \geq b \Rightarrow a - b \geq 0 \Rightarrow |a-b| = a - b \Rightarrow \frac{a+b-|a-b|}{2} = \frac{a+b-(a-b)}{2} = \frac{2b}{2} = b$, coincidents.

Cas 2. $a < b$. Aleshores, per una banda, és $\text{mín}(a,b) = a$ i, per l'altra, tenim

$a < b \Rightarrow a - b < 0 \Rightarrow |a-b| = -(a-b) = b - a \Rightarrow \frac{a+b-|a-b|}{2} = \frac{a+b-(b-a)}{2} = \frac{2a}{2} = a$, coincidents.

De vegades, és necessari distingir entre diversos casos possibles. Hi ha situacions en què les línies argumentals són similars a cada cas. En algunes situacions, ens hi veiem obligats perquè hem de seguir línies argumentals diferents. Això es pot veure en els dos exemples que segueixen.

Exemple 6.19 (ja s'ha vist anteriorment) Proveu que

$\forall x \in \mathbb{R} \forall y \in \mathbb{R}(\text{màx}(x,y) + \text{mín}(x,y) = x + y)$.

En distingirem dos casos:

Cas 1: $x \geq y$. Aleshores és $\text{màx}(x,y) = x$, $\text{mín}(x,y) = y$, d'on la igualtat.

Cas 2: $x < y$. Aleshores és $\text{màx}(x,y) = y$, $\text{mín}(x,y) = x$, d'on la igualtat. ■

Exemple 6.20 Càlcul de la suma dels primers nombres naturals $1+2+\cdots+n$ (una demostració més d'un resultat ja conegut, però es tracta d'il·lustrar un nou mètode!). La *idea* ara, en aquesta variant argumental, es basa en les agrupacions següents: el primer sumand amb l'últim, el segon amb el penúltim, i així successivament, ja que aquestes associacions sumen el mateix, $(n+1)$: $1+n = 2+(n-1) = 3+(n-2) = \cdots$. L'associació anterior es pot fer en grups de dos si n és parell; en canvi, si n és senar, queda un sumand central, $\frac{n+1}{2}$ que no es pot aparellar amb cap, i aleshores hem d'argumentar i comptar de maneres diferents segons la paritat. Per això, es fa necessària la distinció per casos segons la paritat de n:

Cas 1: n és parell. Aleshores reescrivim la suma com

$1+2+3+\cdots+\frac{n}{2}+(\frac{n}{2}+1)+\cdots+(n-1)+n$. Reagrupant tal com hem dit,

$$\begin{aligned}
&1+2+3+\cdots+\tfrac{n}{2}+(\tfrac{n}{2}+1)+\cdots+(n-1)+n = \\
&(1+n)+(2+(n-1))+(3+(n-2))+(4+(n-3))+\cdots+\tfrac{n}{2}+(\tfrac{n}{2}+1),
\end{aligned}$$

resulten $\frac{n}{2}$ agrupacions, de suma $n+1$. Per tant, la suma és $\frac{n}{2}(n+1)$, que és la fórmula buscada.

Cas 2: n és senar. Aleshores la llista L de sumands es descompon en un element central, $\frac{n+1}{2}$, i dues subllistes, L_1, L_2, del mateix nombre d'elements, concretament

$$L_1 = \{1,2,3,\cdots,\frac{n+1}{2}-1\}, L_2 = \{\frac{n+1}{2}+1,\cdots,n-2,n-1,n\};$$

també es pot reescriure

$$\frac{n+1}{2}-1 = \frac{n-1}{2}, \frac{n+1}{2}+1 = \frac{n+3}{2}.$$

El nombre d'elements de L_1 és $\dfrac{n+1}{2}-1$, i aquest és el nombre d'agrupacions que es formen. Atès que cada agrupació suma $n+1$, en resulta la fórmula:

$$1+2+3+\cdots+\frac{n-1}{2}+\frac{n+1}{2}+\frac{n+3}{2}+\cdots+(n-1)+n=$$
$$(1+n)+(2+(n-1))+\cdots+(\frac{n-1}{2}+\frac{n+3}{2})+\frac{n+1}{2}=$$
$$(1+n)\frac{n-1}{2}+\frac{n+1}{2}=\frac{n(n+1)}{2}. \qquad \blacksquare$$

Una observació final és que no cal que els casos en una demostració per casos siguin mútuament excloents. En aquest sentit un exemple és cas de la reunió de conjunts, que no són necessàriament disjunts. Així, $x \in A \cup B$ si, i només si, $x \in A$ o $x \in B$. Si convingués, com així passa en més d'una ocasió (vegeu el capítol dedicat a conjunts), es podria fer una demostració per casos segons l'esquema:

Cas 1. $x \in A$. ...

Cas 2. $x \in B$. ...

per a $x \in A \cup B$.

El que sí que cal és que es cobreixin totes les situacions; en cas contrari, el resultat només quedarà demostrat per als casos que s'hagin considerat.

Vegem un exemple addicional sobre aquesta qüestió.

Exemple 6.21 Per a a,b nombres enters, $(3|a \vee 3|b) \Rightarrow 3|ab$.

En efecte, els casos $3|a$ i $3|b$ no són mútuament excloents.

Cas $3|a$. $3|a \overset{\exists k\in\mathbb{Z}}{\Rightarrow} a=3k \overset{\exists k\in\mathbb{Z}}{\Rightarrow} ab=(3k)b=3(kb) \overset{\exists k'\in\mathbb{Z}\ (k'=kb)}{\Rightarrow} ab=3k' \Rightarrow 3|ab$.

Cas $3|b$. $3|b \Rightarrow \exists k \in \mathbb{Z}(b=3k) \Rightarrow \exists k \in \mathbb{Z}\ (ab=a(3k)=3(ka)) \Rightarrow \exists k' \in \mathbb{Z}\ (ab=3k') \Rightarrow 3|ab$ (amb $k'=ka$).

L'afirmació equival a $(3|a \to 3|ab) \wedge (3|b \to 3|ab)$, com a cas particular de

$(A \vee B) \to C \equiv (A \to C) \wedge (B \to C)$.

Anàlogament:

$(2|a \vee 2|b) \Rightarrow 2|ab$

$(5|a \vee 5|b) \Rightarrow 5|ab$

$(15|a \vee 10|b) \Rightarrow 5|ab$ $\blacksquare$

Exercicis addicionals

S'han de resoldre per distinció de casos.

1. $2|n^3+5n+232$, per a tot n enter
2. $3|n^3+2n$, n nombre natural
3. $6|n^3-n$, per a tot nombre natural n
4. $2|n^3+n$, n nombre enter
5. $2|n^2+n-2$, per a tot nombre enter n
6. $2|n^3+n+6$, per a tot enter n

6.5. Demostracions per reducció a l'absurd

Sobre el mètode de demostració per reducció a l'absurd

Suposem que hem de demostrar l'enunciat $\mathscr{A}$ per reducció a l'absurd.

El mètode consisteix a:
- suposar que $\mathscr{A}$ no és cert (o sigui, $\mathscr{A}$ és fals), és a dir, que $\neg\mathscr{A}$ és cert.
- a partir d'aquesta suposició, s'arriba a alguna **contradicció**.
- es conclou que $\neg\mathscr{A}$ és fals.
- per tant, es conclou que és cert $\neg\neg\mathscr{A}$, o sigui $\mathscr{A}$.

És un mètode indirecte de demostració.

La contradicció pot acabar tenint formes variades, però essencialment s'arriba a $G\wedge\neg G$ cert, en què és cert G i la seva negació. Pot produir-se una contradicció amb afirmacions que s'han fet en el curs de la demostració o bé amb resultats generals de la matemàtica.

Com poden ser els enunciats? L'enunciat $\mathscr{A}$ pot ser molt complex. Per exemple:

$\mathscr{A} = (F_1\wedge F_2\wedge\neg(F_2\to\neg F_4))\vee F_5$.

L'enunciat $\mathscr{A}$ pot tenir qualsevol forma, com per exemple:

$A\to B$ (és a dir, $\mathscr{A} = A\to B$)

$A\wedge B$

$A\vee B$

$\forall x P(x)$

$\forall x(P(x)\to Q(x))$

I altres:

$\forall x(P(x) \rightarrow \neg Q(x))$

$A \vee \neg(B \rightarrow \neg C)$

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

Així:

a) En el cas $A \rightarrow B$, suposem certa la negació, és a dir, suposem cert $A \wedge \neg B$ i arribem a una contradicció.
b) En el cas $A \wedge B$, suposem certa la negació, és a dir, $\neg(A \wedge B)$, o bé, per De Morgan, suposem cert $\neg A \vee \neg B$ i arribem a una contradicció.
c) En el cas $A \vee B$, suposem certa la negació, és a dir, $\neg(A \vee B)$, o bé, per De Morgan, suposem cert $\neg A \wedge \neg B$ i arribem a una contradicció.
d) En el cas $\forall x P(x)$, suposem certa la negació, és a dir $\neg \forall x P(x)$, que equival a dir $\exists x \neg P(x)$ cert, i arribem a una contradicció.
e) De manera semblant, si tenim l'estructura $\forall x(P(x) \rightarrow Q(x))$, suposem cert $\neg \forall x(P(x) \rightarrow Q(x))$, és a dir, $\exists x(P(x) \wedge \neg Q(x))$ cert i arribem a una contradicció.

Amb implicació, és el mateix: si hem de demostrar $A \Rightarrow B$, hem de demostrar que $\mathscr{A} = A \rightarrow B$ és certa, de manera que suposem que és certa la negació, és a dir, $A \wedge \neg B$ és cert (o bé A i no B certs).

Exemples 6.22 Vegem alguns exemples en què s'indica la idea demostrativa, però no se'n fa la demostració.

Exemple 1. Si hem de demostrar per reducció a l'absurd que $2|n \Rightarrow 2|n^3$, hem de partir de la suposició que $2|n \wedge 2 \nmid n^3$ és cert. De fet, la formulació (per a enters) $\forall n(2|n \rightarrow 2|n^3)$ és la correcta i aleshores partim de la suposició que, per a algun n enter, es compleix que $2|n \wedge 2 \nmid n^3$ és cert, i arribem a una contradicció.

Naturalment, en aquest exemple seria més fàcil una demostració directa.■

Exemple 2. Si hem de demostrar per reducció a l'absurd que

$(2|a \wedge 2|b) \rightarrow 2|(a+b)$, partirem de la suposició que $2|a \wedge 2|b \wedge 2 \nmid (a+b)$ és certa (de fet per a alguns a,b).

Amb quantificadors, $\forall a \forall b((2|a \wedge 2|b) \rightarrow 2|(a+b))$. ■

Exemple 3. Si hem de demostrar que $\sqrt{2}$ és irracional, aleshores $\mathscr{A}$ es pot expressar de diverses maneres:

$\mathscr{A} :=$ "$\sqrt{2}$ és irracional"

$\mathscr{A} :=$ "$\sqrt{2} \notin \mathbb{Q}$"

O fins i tot en termes de condicional:

$(x \in \mathbb{R} \wedge x > 0 \wedge x^2 = 2) \rightarrow x \notin \mathbb{Q}$

Aquest últim enunciat és el complet; l'enunciat "$\sqrt{2}$ és irracional" és, de fet, incomplet, ja que no ens diu què és $\sqrt{2}$.

En la primera versió, diríem:

"suposem que $\sqrt{2}$ és racional" o bé
"suposem que $\sqrt{2} \in \mathbb{Q}$"

A l'última versió, diríem:
"suposem que $x \in \mathbb{R} \wedge x > 0 \wedge x^2 = 2 \wedge x \in \mathbb{Q}$ per a algun x". ■

Vegem un primer exemple de demostració per reducció a l'absurd:

Exemple 6.23 Considerem els conjunts:

$A = \{3r+2 | r \in \mathbb{Z}\}$
$B = \{6s-5 | s \in \mathbb{Z}\}$

Volem provar que $A \cap B = \emptyset$.

Demostrem-ho **per reducció a l'absurd**. Suposem que $A \cap B \neq \emptyset$ i arribem a alguna contradicció.

Si $A \cap B \neq \emptyset$, aleshores existeix algun $x \in A \cap B$, és a dir, algun x tal que $x \in A$ i $x \in B$. Per ser $x \in A$, $x = 3r+2$ per a algun enter r. Per ser $x \in B$, $x = 6s-5$ per a un cert enter s. Així, existeixen enters r, s tals que $3r+2 = 6s-5$. D'on $3(r-2s) = -5-2 = -7$. Donat que $3|3(r-2s)$, resulta $3|-7$, absurd.

Per tant, $A \cap B = \emptyset$. ■

Exemples diversos d'aplicació del mètode

Presentem, en primer lloc, l'exemple més emblemàtic per a mostrar el mètode: "l'arrel quadrada de 2 és irracional".

Demostració de "$\sqrt{2} \notin \mathbb{Q}$" pel mètode de reducció a l'absurd

Exemple 6.24 Suposem que $\sqrt{2} \notin \mathbb{Q}$ és fals.

És a dir, que $\sqrt{2} \in \mathbb{Q}$.

Per tant, existeixen $a, b \in \mathbb{Z}$, amb $b \neq 0$ tals que $\sqrt{2} = \frac{a}{b}$.

Podem suposar que la fracció $\frac{a}{b}$ és irreductible, és a dir, que l'únic divisor comú positiu de a i b és la unitat. Si no fos així, sempre podríem reduir-la a aquest cas, dividint a i b pel màxim comú divisor $\mathrm{mcd}(a,b)$.

Suposem, doncs, que a i b no tenen cap divisor comú positiu llevat de 1.

Elevant al quadrat:

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

Òbviament, $2|2b^2$. Per l'última igualtat, és $2|a^2$

Resolem un subproblema:

Vegem que $2|a$, és a dir, $2|a^2 \Rightarrow 2|a$, o que $2|a^2 \rightarrow 2|a$ és cert. Es pot provar de diverses maneres:

Mètode 1. Si el lector coneix el lema d'Euclides (vegeu el capítol de preliminars), que afirma, per a nombres enters c,d:

$(p \text{ primer} \wedge p|cd) \rightarrow (p|c \vee p|d)$,

aleshores es pot aplicar amb $p = 2$, $c = a$ i $d = a$ i es conclou que $2|a$.

Mètode 2. Podem demostrar $2|a^2 \rightarrow 2|a$ pel *contrarrecíproc*, és a dir:

$2 \nmid a \rightarrow 2 \nmid a^2$.

En efecte, si $2 \nmid a$, aleshores a és senar i s'expressa com $a = 2k+1$, per a un k enter convenient. Per tant, $a^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1 = 2k'+1$, amb $k' = 2k^2+2k \in \mathbb{Z}$, d'on a^2 és senar, és a dir, $2 \nmid a^2$, demostrat.

Mètode 3. També es pot demostrar *per reducció a l'absurd*, és a dir, resoldre aquest subproblema per reducció a l'absurd, suposant que, per a algun a enter, és $2|a^2 \wedge 2 \nmid a$ i arribant a contradicció.

Variant. També es pot demostrar per casos segons la paritat de a. Si $2|a$, hem acabat; si $2 \nmid a$, aleshores és un cas impossible, seguint l'argument del contrarecíproc.

Fi del subproblema

Continuem amb l'argumentació. Tenim, doncs, $2|a$. Per tant, existeix k nombre enter tal que $a = 2k$. Ara podem substituir $a = 2k$ a l'anterior $2b^2 = a^2$. Així resulta $2b^2 = (2k)^2 = 4k^2$, d'on, simplificant, $b^2 = 2k^2$.

Fem una argumentació similar a la d'abans de resoldre el subproblema:

Com que $2|2k^2$, per la igualtat anterior, resulta $2|b^2$ i ara, per qualsevol dels mètodes abans exposats, resulta $2|b$.

Resumint, hem arribat a:

$2|a$ i $2|b$, **contradicció**,

ja que a, b no tenen divisors comuns positius diferents d'1.

Per tant, $\sqrt{2} \in \mathbb{Q}$ és fals. És a dir, $\sqrt{2} \notin \mathbb{Q}$ és cert. ■

Exemples addicionals de demostració per reducció a l'absurd

Exemple 6.25 Demostreu que $\frac{1+\sqrt{2}}{2}$ és un nombre irracional.

La propietat és $\mathscr{A}$:="$\frac{1+\sqrt{2}}{2}$ és un nombre irracional"

Apliquem el mètode de reducció a l'absurd i suposem que $\neg\mathscr{A}$ és cert, és a dir, que "$\frac{1+\sqrt{2}}{2}$ és un nombre racional".

Mètode 1. Si $\frac{1+\sqrt{2}}{2}$ és racional, aleshores existeixen enters a, b, amb $b \neq 0$, tals que

$\frac{1+\sqrt{2}}{2} = \frac{a}{b}$. D'on $1+\sqrt{2} = \frac{2a}{b}$. Per tant,

$\sqrt{2} = \frac{2a}{b} - 1 = \frac{2a-b}{b}$.

Ara bé, $\frac{2a-b}{b} \in \mathbb{Q}$. I així resulta $\sqrt{2} \in \mathbb{Q}$, que es contradiu amb $\sqrt{2} \notin \mathbb{Q}$.

Mètode 2. És una variant de l'anterior. Suposem que $\frac{1+\sqrt{2}}{2} \in \mathbb{Q}$. El producte de dos nombres racionals és racional i, per tant, $2 \cdot \frac{1+\sqrt{2}}{2} \in \mathbb{Q}$, d'on $1+\sqrt{2} \in \mathbb{Q}$. Atès que la suma (diferència) de dos nombres racionals és racional, és $(1+\sqrt{2}) - 1 \in \mathbb{Q}$, d'on $\sqrt{2} \in \mathbb{Q}$, cosa que entra en contradicció amb un resultat prèviament demostrat. ■

Vegem un exemple addicional en què s'aplica el mètode de reducció a l'absurd per a enunciats del tipus $A \to B$.

S'ha de demostrar que $A \to B$ és cert, és a dir, $A \Rightarrow B$. Així, $\mathscr{A} = A \to B$ és l'enunciat que volem provar per reducció a l'absurd. Procedim de la manera següent:

1. Negació de $\mathscr{A}$. Suposem que $\mathscr{A}$ és fals, és a dir, que $\neg\mathscr{A}$ és cert. En el nostre cas, és $\neg(A \to B)$. Ara bé, és $\neg(A \to B) \equiv A \wedge \neg B$. Així, suposem cert $A \wedge \neg B$.
2. S'arriba a alguna contradicció.
3. Es conclou que $\mathscr{A}$ és cert.

Exemple 6.26 Propietat que es vol demostrar:

"La suma d'un nombre racional i d'un nombre irracional és irracional"

"Si x és un nombre racional i y és un nombre irracional, aleshores $x+y$ és un nombre irracional"

Formalitzadament:

"(x és un nombre racional i y és un nombre irracional) $\to x+y$ és un nombre irracional"

$(x \in \mathbb{Q} \wedge y \notin \mathbb{Q}) \to x+y \notin \mathbb{Q}$

$(x \in \mathbb{Q} \wedge y \notin \mathbb{Q}) \Rightarrow x+y \notin \mathbb{Q}$

Demostració per reducció a l'absurd.

Suposem cert: $x \in \mathbb{Q} \wedge y \notin \mathbb{Q} \wedge x+y \in \mathbb{Q}$

L'argumentació depèn del que considerem sabut sobre els nombres racionals.

Mètode 1. Si es considera sabut, i acceptat, que la suma (i diferència) de dos nombres racionals és racional, aleshores podem escriure:

Sigui $z = x+y \in \mathbb{Q}$. Essent $x \in \mathbb{Q}$, pel que acabem de dir és $z-x \in \mathbb{Q}$. Però $z-x=y$, d'on $y \in \mathbb{Q}$, contradicció, i en resulta el que havíem de demostrar.

Mètode 2. Si no es fa servir el resultat esmentat al mètode 1, aleshores s'ha d'utilitzar la forma dels nombres racionals. I podem escriure:

$x \in \mathbb{Q} \Rightarrow x = \dfrac{a}{b}$, per a a i b enters convenients, amb $b \neq 0$. Anàlogament:

$x+y \in \mathbb{Q} \Rightarrow x+y = \frac{c}{d}$, per a c i d enters convenients, amb $d \neq 0$.

Per tant:

$y = (x+y)-x = \dfrac{c}{d} - \dfrac{a}{b} = \dfrac{cb-ad}{db} \in \mathbb{Q}$, ja que $cb-ad \in \mathbb{Z}$, $db \in \mathbb{Z}$ i $db \neq 0$.

És a dir, que hem arribat a una contradicció: $y \notin \mathbb{Q}$ i $y \in \mathbb{Q}$.

Per tant, $(x \in \mathbb{Q} \wedge y \notin \mathbb{Q}) \Rightarrow x+y \notin \mathbb{Q}$.

Formalment, de manera més completa, l'afirmació és

$\forall x \forall y((x \in \mathbb{Q} \wedge y \notin \mathbb{Q}) \to x+y \notin \mathbb{Q})$ i la negació és

$\exists x \exists y((x \in \mathbb{Q} \wedge y \notin \mathbb{Q}) \wedge x+y \in \mathbb{Q})$, punt de partida de la demostració per reducció a l'absurd. ■

Recuperem algun dels enunciats inicials, que resolem aquí.

Exemple 6.27 Provem per reducció a l'absurd que, per a n enter, es compleix:

$2|n^2 \Rightarrow 2|n$.

De fet, és $\forall n(2|n^2 \to 2|n)$. La negació de l'enunciat és $\exists n(2|n^2 \wedge 2 \nmid n)$, és a dir que, per a algun enter n, és $2|n^2 \wedge 2 \nmid n$ cert.

Suposem que l'afirmació no és certa, és a dir, que és certa la negació $\neg(2|n^2 \to 2|n)$, és a dir, que és cert: $2|n^2 \wedge 2 \nmid n$, per a algun n. Per tant:

$2|n^2 \Rightarrow$ existeix k enter tal que $n^2 = 2k$.

$2 \nmid n \Rightarrow$ existeix t enter tal que $n = 2t+1$.

Per tant, $n^2 = (2t+1)^2 = 4t^2+4t+1$. Igualant, $2k = n^2 = 4t^2+4t+1$, d'on $2k = 4t^2+4t+1$. Per tant, $2k-(4t^2+4t) = 1$, d'on $2(k-2t^2-2t) = 1$, contradicció, perquè concloem que el nombre senar 1 és parell.

Variant argumental de la part final. O també: $2|2(k-2t^2-2t)$ i, per la igualtat, $2|1$, absurd. ■

PROBLEMA 6.9

Proveu que, per a tot nombre real x, és $x - \sqrt{x^2+1} \neq 0$.

Solució. Per veure que l'expressió $x - \sqrt{x^2+1}$ no s'anul·la per a cap nombre real, en fem una demostració *per reducció a l'absurd*.

Amb quantificadors, la fórmula de predicats que expressa l'afirmació és

$\forall x(x \in \mathbb{R} \to x - \sqrt{x^2+1} \neq 0)$

Neguem l'afirmació i arribem a una contradicció:

$\neg\forall x(x \in \mathbb{R} \to x - \sqrt{x^2+1} \neq 0)$

$\exists x\neg(x \in \mathbb{R} \to x - \sqrt{x^2+1} \neq 0)$

$\exists x(x \in \mathbb{R} \wedge \neg(x - \sqrt{x^2+1} \neq 0))$

$\exists x(x \in \mathbb{R} \wedge x - \sqrt{x^2+1} = 0)$

Ara, si $x - \sqrt{x^2+1} = 0$ per a algun x real, és $x = \sqrt{x^2+1}$. Elevant al quadrat ambdós membres de la igualtat, $x^2 = x^2+1$, d'on $0 = 1$, cosa absurda.

PROBLEMA 6.10

Sigui $b \notin \mathbb{Z}$. *Proveu que* $b-3 \notin \mathbb{Z}$.

Solució. Seria reformulable com $b \notin \mathbb{Z} \Rightarrow b-3 \notin \mathbb{Z}$.

Aplicant el mètode de *reducció a l'absurd*, neguem l'afirmació anterior i suposem cert: $b \notin \mathbb{Z}$ i $b-3 \in \mathbb{Z}$. Sigui $m = b-3 \in \mathbb{Z}$. Aleshores, per les propietats de la suma d'enters, és $m+3 \in \mathbb{Z}$. Però $m+3 = (b-3)+3 = b$, i així tenim que $b = m+3 \in \mathbb{Z}$, contradicció amb $b \notin \mathbb{Z}$.

Observació. També es podria formular com una demostració pel *contrarecíproc*, demostrant equivalentment $b-3 \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}$. És immediat: $b = (b-3)+3$, suma d'enters i, per tant, enter.

PROBLEMA 6.11

Demostreu, per reducció a l'absurd, que, per a tot enter n, es compleix $2|n(n+1)$*, és a dir, que el producte de dos enters consecutius qualssevol és un nombre parell.*

Observació. *Tenim un enunciat similar per a* $2|(n-1)n$.

Solució. L'afirmació és

$\mathscr{A} : \forall n(n \in \mathbb{Z} \to 2|n(n+1))$. Equivalentment, si suposem $\Omega = \mathbb{Z}$,

$\mathscr{A} : \forall n(2|n(n+1))$.

La negació és $\neg\mathscr{A}$: (equival a qualsevol de les fórmules posteriors)

$\neg\forall n(n \in \mathbb{Z} \to 2|n(n+1))$
$\exists n\neg(n \in \mathbb{Z} \to 2|n(n+1))$
$\exists n(n \in \mathbb{Z} \wedge \neg 2|n(n+1))$
$\exists n(n \in \mathbb{Z} \wedge 2 \nmid n(n+1))$ (adoptem aquesta)

Suposem $\neg\mathscr{A}$ cert i arribem a alguna contradicció.

És a dir, suposem certa l'afirmació $\exists n(n \in \mathbb{Z} \wedge 2 \nmid n(n+1))$. Sigui, doncs, n_0 un enter tal que $n_0(n_0+1)$ no és parell i, per tant, és senar.

Vegem que n_0 no és parell. En efecte, si ho fos, aleshores seria $n_0 = 2k$ per a un cert k enter, d'on $n_0(n_0+1) = 2k(n_0+1)$ i és, per tant, parell.

Alternativament, el que fem és demostrar el contrarecíproc de $2 \nmid n_0(n_0+1) \Rightarrow 2 \nmid n_0$, és a dir, $2|n_0 2 \Rightarrow 2|n_0(n_0+1)$.

Per tant, ha de ser n_0 senar. Però, aleshores, n_0+1 és parell, és a dir, $n_0+1 = 2k'$ per a un k' enter convenient. En conseqüència, $n_0(n_0+1) = 2k'n_0$, parell.

Hem arribat a una contradicció i, per tant, queda demostrat $\mathscr{A}$.

Reformulació expositiva. Es podria plantejar per casos segons la paritat de n_0:

Cas 1 (n_0 és parell). Aleshores seria $n_0 = 2k$ per a un cert k enter, d'on $n_0(n_0+1) = 2k(n_0+1)$ i és, per tant, parell. Contradicció.

Cas 2 (n_0 és senar). Aleshores tenim:

n_0 és senar $\Rightarrow n_0+1$ és parell $\Rightarrow \exists k'(k' \in \mathbb{Z} \wedge n_0+1 = 2k') \Rightarrow \exists k'(k' \in \mathbb{Z} \wedge n_0(n_0+1) = 2k'n_0) \Rightarrow n_0(n_0+1)$ és parell.

Com a conclusió, $n_0(n_0+1)$ és parell . Contradicció.

No hi ha més casos, per la dicotomia parell-senar.

En tots els casos, arribem a una contradicció. Per tant, l'enunciat és cert.

PROBLEMA 6.12

Demostreu que 203 *és senar pel mètode de reducció a l'absurd. Observació: és obvi; és un exercici essencialment per a exposar el mètode.*

Solució. L'afirmació és "203 és senar".

Per efectuar la demostració per reducció a l'absurd, suposem que l'enunciat és fals, és a dir, suposem que "203 no és senar" és cert. Això és equivalent a dir "203 és parell". És a dir, que "203 és parell" és cert.

Vegem que arribem a una conclusió falsa, a un absurd.

Si 203 és parell, aleshores és divisible per 2, és a dir, existeix un enter k tal que $203 = 2k$. D'altra banda, podem escriure (divisió entera) $203 = 2 \cdot 101 + 1$. Així, $2k = 2 \cdot 101 + 1$, d'on $2(k - 101) = 1$. Atès que $2|2(k - 101)$, tenim que $2|1$, que és absurd.

Alternativament, no cal efectuar la divisió entera ja que, amb altres expressions, també arribem a una contradicció. Per exemple, si $203 = 2 \cdot 100 + 3$, aleshores és $2k = 2 \cdot 100 + 3$, d'on $2(k - 100) = 3$, d'on $2|3$, que és absurd.

PROBLEMA 6.13

Demostreu per reducció a l'absurd que "306 és múltiple de 3". Observació: és obvi, ja que $306 = 3 \cdot 102$*, però aquí es tracta d'exposar el mètode de demostració per reducció a l'absurd.*

Solució. Afirmació $\mathscr{A}$: "306 és múltiple de 3".

Negació de l'afirmació: $\neg\mathscr{A}$: "306 no és múltiple de 3".

Es tracta d'arribar a una contradicció.

El primer problema és: De quines maneres pot un nombre enter a no ser múltiple de 3?

Si efectuem la divisió entera $a = 3q + r$, amb $0 \leq r \leq 3 - 1 = 2$, hem de descartar el cas $r = 0$, perquè a no és múltiple de 3 i, per tant, resten dues possibilitats: $r = 1$ o $r = 2$. Tenim, doncs, dos casos possibles:

Cas 1. $a = 3q + 1$.

Cas 2. $a = 3q + 2$.

Vegem, separadament, que en cada cas arribem a contradicció.

Cas 1. Suposem que existeix un enter q tal que $306 = 3q + 1$, d'on $3q = 306 - 1 = 305$. En resulta $3|305$, que és fals.

Cas 2. Suposem que existeix un enter q tal que $306 = 3q + 2$, d'on $3q = 306 - 2 = 304$. En resulta $3|304$, que és fals ($304 = 2^4 \times 19$).

PROBLEMA 6.14

Hem de demostrar que, per a tot $x \neq 7$ real, és $\frac{5x}{x-7} \neq 5$. És a dir, més formalitzadament, $\forall x(x \neq 7 \rightarrow \frac{5x}{x-7} \neq 5)$. Apliqueu el mètode de reducció a l'absurd.

Solució. Es tracta de negar:

$\forall x(x \neq 7 \rightarrow \frac{5x}{x-7} \neq 5)$

i arribar a alguna contradicció.

$\neg\forall x(x \neq 7 \rightarrow \frac{5x}{x-7} \neq 5)$

$\exists x \neg(x \neq 7 \rightarrow \frac{5x}{x-7} \neq 5)$

$\exists x(x \neq 7 \wedge \neg(\frac{5x}{x-7} \neq 5))$

$\exists x(x \neq 7 \wedge \frac{5x}{x-7} = 5)$

Ara bé, $\frac{5x}{x-7} = 5 \Rightarrow 5x = 5(x-7) \Rightarrow 5x = 5x - 37 \Rightarrow 0 = -35$, que és absurd. Per tant, és certa l'afirmació original.

PROBLEMA 6.15

Si existeix el límit d'una funció en un punt, aleshores és únic.

Sigui $f : \mathbb{R} \rightarrow \mathbb{R}$ una funció; sigui $a \in \mathbb{R}$, i suposem que existeix el límit $\lim_{x \to a} f(x)$. Vegeu que és únic.

Solució. Demostrem el resultat per reducció a l'absurd.

Suposem que l'afirmació no és certa i siguin L_1, L_2 dos límits diferents ($L_1 \neq L_2$). És a dir:

$\lim_{x \to a} f(x) = L_1$

$\lim_{x \to a} f(x) = L_2$, amb $L_1 \neq L_2$.

Per definició de límit, per a *cada* nombre real $\epsilon > 0$:

- existeix un nombre real $\delta_1 > 0$ tal que $|f(x) - L_1| < \epsilon$ per a cada real x tal que $0 < |x-a| < \delta_1$,

- existeix un nombre real $\delta_2 > 0$ tal que $|f(x) - L_2| < \epsilon$ per a cada real x tal que $0 < |x-a| < \delta_2$

Unificant, per a $\delta = \text{mín}(\delta_1, \delta_2)$, podem afirmar:

$|f(x) - L_1| < \epsilon$ per a cada real x tal que $0 < |x-a| < \delta$ (ja que $0 < |x-a| < \delta \leq \delta_1$),

$|f(x) - L_2| < \epsilon$ per a cada real x tal que $0 < |x-a| < \delta$ (ja que $0 < |x-a| < \delta \leq \delta_2$), i, per tant, tindrem:

$0 < |L_1 - L_2| = |(L_1 - f(x)) + (f(x) - L_2)| \leq |L_1 - f(x)| + |f(x) - L_2| = |f(x) - L_1| + |f(x) - L_2| < \epsilon + \epsilon = 2\epsilon$

Arribem a un absurd si prenem $0 < \epsilon < \frac{1}{2}(|L_1 - L_2|)$, ja que resultaria, amb aquesta elecció de ϵ:

$0 < |L_1 - L_2| < 2\epsilon < 2\frac{1}{2}(|L_1 - L_2|) = |L_1 - L_2|$, és a dir, $|L_1 - L_2| < |L_1 - L_2|$.

Barreja de mètodes de demostració

No sempre apliquem el mètode "en estat pur", sinó que ens podem veure forçats a utilitzar-lo en combinació amb altres mètodes. En ocasions, cal fer una combinació de tècniques demostratives. Aquesta situació s'il·lustra a l'exemple següent i en alguns altres que ja hem vist o que seguiran.

En algunes situacions, demostrem un resultat per un mètode, però internament se'n poden fer servir d'altres. I així es veuen barreges de "reducció a l'absurd", "per casos", "pel contrarecíproc"; de vegades, es veuen petites demostracions per reducció a l'absurd a l'interior de la demostració d'un cas. Algunes demostracions per reducció a l'absurd d'implicacions poden compartir argumentacions amb demostracions del mateix resultat pel contrarecíproc.

Vegem, per exemple, la demostració de $\sqrt{3} \notin \mathbb{Q}$, inspirada en la demostració de la irracionalitat de $\sqrt{2}$ per reducció a l'absurd. Utilitzem, a més, distinció de casos.

Exemple 6.28 *Enunciat*: Demostreu $\sqrt{3} \notin \mathbb{Q}$

Solució. L'*estratègia general* és demostrar $\sqrt{3} \notin \mathbb{Q}$ pel *mètode de reducció a l'absurd*. En un cert punt de la demostració, se'ns presentarà la necessitat o la conveniència de demostrar el resultat auxiliar $3|a^2 \Rightarrow 3|a$. Aquest és un subproblema, o problema apart, que resoldrem per una altra metodologia, la demostració equivalent del *contrarecíproc*, és a dir, de $3 \nmid a \Rightarrow 3 \nmid a^2$. Ara bé, la consideració de $3 \nmid a$ ens farà plantejar de quines maneres pot un nombre no ser múltiple de 3. Això ens porta a considerar els residus de la divisió entera de a per 3, i fer encara un *estudi per casos* segons els valors possibles dels residus. Són, doncs, tres metodologies en un sol problema.

Resolució: Suposem que $\sqrt{3} \notin \mathbb{Q}$ no és cert, és a dir, que $\sqrt{3} \in \mathbb{Q}$ és cert. Aleshores existeixen a, b nombres enters, amb $b \neq 0$ tals que $\sqrt{3} = \frac{a}{b}$ i, sense pèrdua de generalitat, podem suposar que és una fracció irreductible, de manera que a i b no tenen divisors comuns llevat de ± 1.

Aleshores tenim $3 = (\frac{a}{b})^2 = \frac{a^2}{b^2}$, d'on $3b^2 = a^2$. Atès que $3b^2$ és múltiple de 3, resulta, per la igualtat, que a^2 és múltiple de 3. Vegem que a és múltiple de 3.

Subproblema. Hem de demostrar $3|a^2 \Rightarrow 3|a$. Demostrarem equivalentment el *contrarecíproc*, és a dir, $3 \nmid a \Rightarrow 3 \nmid a^2$. Com expressar que a no és múltiple de 3? Escrivim la divisió entera $a = 3q + r$, on $0 \le r < 3$ (és a dir, $0 \le r \le 2$). Que $3 \nmid a$ equival a $r \neq 0$, de manera que és $1 \le r \le 2$, que equival a dos casos possibles: $r = 1$ o $r = 2$.

Fem un estudi *per casos*, els indicats pels valors que pot prendre r.

Cas 1 ($r = 1$). Aleshores: $r = 1 \Rightarrow a = 3q + 1 \Rightarrow a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$, no múltiple de 3. Es pot veure de dues maneres: per la unicitat de quocient i residu a la divisió entera, l'anterior $a^2 = 3q' + r'$ ho és i, per tant, a^2 no és múltiple de 3, ja que el residu és $r' = 1 \neq 0$. D'una altra manera, si fos 3 divisor de a^2, aleshores $3|(a^2 - 3(3q^2 + 2q)) = 1$, d'on $3|1$, impossible. Per tant, $r = 1 \Rightarrow 3 \nmid a^2$.

Cas 2 ($r = 2$). Aleshores: $r = 2 \Rightarrow a = 3q + 2 \Rightarrow a^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q) + 4$, no múltiple de 3. Es pot veure de dues maneres: per la unicitat de quocient i residu a la divisió entera, l'anterior $a^2 = 3q' + r'$ ho és i, per tant, a^2 no és múltiple de 3, ja que el residu és $r' = 4 \neq 0$. Altrament, si fos 3 divisor de a^2, aleshores $3|(a^2 - 3(3q^2 + 4q)) = 4$, d'on $3|4$, cosa impossible. Per tant, $r = 2 \Rightarrow 3 \nmid a^2$.

Així doncs, hem vist que es compleix $(r = 1 \to 3 \nmid a^2) \wedge (r = 2 \to 3 \nmid a^2)$, és a dir,

$((r = 1 \vee r = 2) \to 3 \nmid a^2)$ és cert.

Per tant, $3 \nmid a \Rightarrow 3 \nmid a^2$. *Fi del subproblema.*

Ara podem continuar amb l'argumentació.

Tenim, doncs, que a és múltiple de 3, és a dir $a = 3t$ per a un cert enter t. Substituint a $3b^2 = a^2$, resulta $3b^2 = (3t)^2 = 3^3t^2$, d'on $b^2 = 3t^2$. Ara farem una argumentació similar a l'anterior: atès que $3t^2$ és múltiple de 3, també ho és b^2. Vegem que $3|b^2 \Rightarrow 3|b$. L'argumentació és la mateixa que en el "subproblema", de manera que obtenim $3|b$.

Així, hem arribat a la conclusió $3|a$ i $3|b$, que és absurda, ja que la fracció $\frac{a}{b}$ és irreductible. On és l'origen de la contradicció? En la suposició $\sqrt{3} \in \mathbb{Q}$. Per tant, $\sqrt{3} \notin \mathbb{Q}$, com havíem de veure. ■

PROBLEMA 6.16

Sigui n un nombre enter qualsevol. Proveu que $3|(n-1)n(n+1)$.

Formalització: $\forall n(n \in \mathbb{Z} \to 3|(n-1)n(n+1))$

De fet, l'enunciat seria equivalent a qualsevol variant com les següents:

$3|n(n+1)(n+2)$

$3|(n-2)(n-1)n$

$3|(n+13)(n+14)(n+15)$

El producte de tres enters consecutius és múltiple de 3. *De fet, a cada tres enters consecutius hi ha exactament un múltiple de* 3.

Solució. Un possible mètode de demostració és *per casos*. Quins són els casos possibles? Respecte de quin criteri considerem casos? Atès el tipus de resultat, podem considerar la divisió entera de n per 3 i com a casos, els diferents valors possibles del residu r corresponent. Existeixen enters q, r únics que satisfan $n = 3q + r$, amb $0 \leq r \leq 2$. Per tant, $r = 0$ o $r = 1$ o $r = 2$ (o $r \in \{0, 1, 2\}$).

Cas 1 ($r = 0$). Aleshores $n = 3q$, múltiple de 3.

Cas 2 ($r = 1$). Aleshores $n = 3q + 1$. Per tant, $n - 1 = (3q + 1) - 1 = 3q$, múltiple de 3.

Cas 3 ($r = 2$). Aleshores $n = 3q + 2$. Per tant, $n + 1 = (3q + 2) + 1 = 3q + 3 = 3q'$, múltiple de 3.

Observació. Com es podria demostrar l'altra variant $3|(n+13)(n+14)(n+15)$? Anàlogament per casos: per exemple, si $n = 3q + 1$, aleshores $n + 13 = 3q + 1 + 13 = 3q + 4 \times 3 + 1 + 1 = 3(q + 4) + 2 = 3q' + 2$, $n + 14 = 3q' + 3 = 3q''$ (múltiple de 3), etc.

Es podria demostrar per reducció a l'absurd? Vegem-ho.

Suposem que, per a algun enter n, no es compleix l'afirmació, és a dir:

$3 \nmid (n-1)n(n+1)$.

Això implica que 3 no divideix cap dels factors, ja que, en cas contrari, dividiria el producte. Així, $3 \nmid n - 1$, $3 \nmid n$ i $3 \nmid n + 1$. En termes de la divisió entera per 3, això significa (equival a) que els residus corresponents són no nuls, és a dir, que existeixen q_i, r_i únics tals que

α]: $n - 1 = 3q_1 + r_1$, amb $1 \leq r_1 \leq 2$ ($r_1 \neq 0$)
β]: $n = 3q_2 + r_2$, amb $1 \leq r_2 \leq 2$ ($r_2 \neq 0$)
γ]: $n + 1 = 3q_3 + r_3$, amb $1 \leq r_3 \leq 2$ ($r_3 \neq 0$)

Hem de combinar el mètode general de demostració per reducció a l'absurd amb el mètode de demostració per casos i arribar a un absurd o una contradicció en cada cas.

Vegem-ne una possibilitat, per exemple, segons els valors possibles per a r_3 (hi ha altres possibilitats); és $r_3 = 1 \vee r_3 = 2$.

Cas 1 ($r_3 = 1$). Aleshores $n + 1 = 3q_3 + 1$, d'on $n = 3q_3 + 0$, satisfent les condicions de divisió entera. Per unicitat, tenint en compte [β], és $q_2 = q_3$ i $r_2 = 0$, absurd.

Cas 2 ($r_3 = 2$). Aleshores $n + 1 = 3q_3 + 2$, d'on $n = 3q_3 + 1$ i, per tant, $n - 1 = 3q_3 = 3q_3 + 0$, divisió entera. Per unicitat, tenint en compte [α], és $q_1 = q_3$ i $r_1 = 0$, absurd.

En ambdós casos, s'arriba a una contradicció. Queda demostrada la propietat per reducció a l'absurd.

Variant argumental. Vegem una altra possibilitat d'argumentació, encara que de tipus similar a l'anterior, considerant els valors possibles per a r_2 com a base de l'anàlisi per casos.

Cas 1 ($r_2 = 1$). Aleshores $n = 3q_2 + 1$, d'on $n - 1 = 3q_2 = 3q_2 + 0$, divisió entera. Però [α] també és una divisió entera: per unicitat resulta $q_1 = q_2$ (irrellevant per a la demostració) i $r_1 = 0$, absurd.

Cas 2 ($r_2 = 2$). Aleshores $n = 3q_2 + 2$, d'on $n + 1 = 3q_2 + 3 = 3(q_2 + 1) + 0 = 3q_2' + 0$, divisió entera. Però [$\gamma$] també és una divisió entera: per unicitat resulta $q_2' = q_3$ i $r_3 = 0$, absurd.

En ambdós casos s'arriba a contradicció. Queda demostrada la propietat per reducció a l'absurd.

Una altra variant argumental similar al desenvolupament anterior consistiria a considerar r_1 com a valor base per als diversos casos.

PROBLEMA 6.17

Sigui n un nombre enter. Proveu que $16n + 5$ no és un quadrat perfecte. És a dir, no es pot expressar com a quadrat d'algun enter.

Solució. Resolem el problema per *reducció a l'absurd*.

Suposem que existeix $\alpha \in \mathbb{Z}$ tal que $16n + 5 = \alpha^2$.

Considerarem una distinció *de casos* segons la paritat de α:

Cas 1 (α parell). Aleshores és $\alpha = 2\beta$, per a un cert β enter. Per tant, $16n + 5 = (2\beta)^2 = 4\beta^2$, d'on $16n - 4\beta^2 = 5$. El membre de l'esquerra és múltiple de 2 i, en canvi, el de la dreta no. Per tant, α no pot ser parell. Això és una contradicció.

Cas 2 (α senar). Aleshores és $\alpha = 2\beta + 1$, per a un cert β enter. Per tant, $16n + 5 = (2\beta + 1)^2 = 4\beta^2 + 4\beta + 1$, d'on $4n + 1 = \beta^2 + \beta$. Ara bé, $4n + 1$ és senar perquè és la suma d'un nombre parell i un senar; en canvi, $\beta^2 + \beta = \beta(\beta + 1)$ és producte de dos enters consecutius, un dels quals ha de ser parell, és a dir, múltiple de 2 (donats dos enters consecutius, exactament un és parell i l'altre, senar). Per tant, $\beta(\beta + 1)$ és parell, i així hem arribat a una contradicció. Per tant, α no pot ser senar.

Això esgota els casos possibles. En cada cas, s'arriba a una contradicció. Per tant, $16n + 5$ no és quadrat de cap nombre enter.

Encara que sigui repetitiu, vegeu-ne un altre exemple. Cal resoldre subproblemes per casos segons els valors del residu d'una divisió entera.

PROBLEMA 6.18

Demostreu que $\sqrt{5}$ és irracional.

Solució. Demostrem el resultat pel mètode de reducció a l'absurd.

Adaptem la demostració que s'ha fet per a provar $\sqrt{2} \notin \mathbb{Q}$.

Suposem que $\sqrt{5} \notin \mathbb{Q}$ és fals, en aplicació del mètode de demostració per reducció a l'absurd.

És a dir, que $\sqrt{5} \in \mathbb{Q}$.

Per tant, existeixen $a,b \in \mathbb{Z}$, amb $b \neq 0$ tals que $\sqrt{5} = \frac{a}{b}$.

Podem suposar que la fracció $\frac{a}{b}$ és irreductible, és a dir, que l'únic divisor comú positiu de a i b és la unitat. Si no fos així d'entrada, sempre podríem reduir-la a aquesta expressió, dividint a i b pel màxim comú divisor $d = \text{mcd}(a,b)$. En efecte, seria $a = a'd$, $b = b'd$ i $\frac{a}{b} = \frac{a'd}{a'd} = \frac{a'}{b'}$, irreductible.

Suposem, doncs, que a i b no tenen cap divisor comú positiu llevat de 1. Ja avancem que la contradicció a què arribarem és justament que a,b tenen divisors comuns positius diferents de 1.

Elevant al quadrat:

$\sqrt{5} = \frac{a}{b} \Rightarrow 5 = (\sqrt{5})^2 = (\frac{a}{b})^2 = \frac{a^2}{b^2} \Rightarrow 5b^2 = a^2$

Òbviament, $5|5b^2$; per l'última igualtat, és $5|a^2$.

Fem un parèntesi per a resoldre el subproblema següent, intern a l'argumentació general.

Subproblema: Vegem que, en conseqüència, $5|a$, és a dir, $5|a^2 \Rightarrow 5|a$, o que $5|a^2 \rightarrow 5|a$ és cert. Es pot provar de diverses maneres:

Mètode 1. Es pot demostrar $5|a^2 \Rightarrow 5|a$ pel mètode del *contrarecíproc*. Hem de demostrar equivalentment que $\neg 5|a \Rightarrow \neg 5|a^2$, és a dir:

$5 \nmid a \Rightarrow 5 \nmid a^2$.

Sigui, doncs, $5 \nmid a$. Si considerem la divisió entera de a per 5, tenim $a = 5q + r$, $0 \leq r < 5$, és a dir, $0 \leq r \leq 4$. Per la condició $5 \nmid a$, és $r \neq 0$. Per tant, les possibilitats per a r són $1 \leq r \leq 4$, o bé $r = 1 \vee r = 2 \vee r = 3 \vee r = 4$.

Hem de fer un estudi per casos segons els possibles valors de r. En cada cas, hem de calcular a^2 i veure que no és múltiple de 5. És $a^2 = (5q+r)^2 = 25q^2 + 10rq + r^2 = 5(5q^2 + 2rq) + r^2$.

► *Cas 1* ($r = 1$). És $a^2 = 5(5q^2 + 2q) + 1$. Aquesta expressió és la divisió entera de a^2 entre 5, per la unicitat del quocient i el residu satisfent $a^2 = 5c + r'$, $0 \leq r' < 5$ (en aquest cas, $r' = 1$). Per tant, atès que $r' = 1 \neq 0$, és $5 \nmid a^2$.

Argument alternatiu (per reducció a l'absurd): si fos $5|a^2$, seria $5|(a^2 - (5(5q^2 + 2q))) = 1$, d'on $5|1$, que no és cert.

► *Cas 2* ($r = 2$). És $a^2 = 5(5q^2 + 4q) + 4$. Aquesta expressió és la divisió entera de a^2 entre 5, per la unicitat del quocient i el residu que satisfan $a^2 = 5c + r'$, $0 \leq r' < 5$ ((en aquest cas, $r' = 4$). Per tant, atès que $r' = 4 \neq 0$, és $5 \nmid a^2$.

Argument alternatiu (per reducció a l'absurd): Si fos $5|a^2$, seria $5|(a^2-(5(5q^2+4q)))=4$, d'on $5|4$, que no és cert.

► *Cas 3* ($r=3$). És $a^2=5(5q^2+6q)+9=5(5q^2+6q+1)+4$. Aquesta expressió és la divisió entera de a^2 entre 5, per la unicitat del quocient i el residu satisfent $a^2=5c+r'$, $0\leq r'<5$ (en aquest cas, $r'=4$). Per tant, atès que $r'=4\neq 0$, és $5\nmid a^2$.

Argument alternatiu (per reducció a l'absurd): Si fos $5|a^2$, seria $5|(a^2-(5(5q^2+6q+1)))=4$, d'on $5|4$, que no és cert.

► *Cas 4* ($r=4$). És $a^2=5(5q^2+8q)+16=5(5q^2+8q+3)+1$. Aquesta expressió és la divisió entera de a^2 entre 5, per la unicitat del quocient i el residu satisfent $a^2=5c+r'$, $0\leq r'<5$ ((en aquest cas, $r'=1$). Per tant, atès que $r'=1\neq 0$, és $5\nmid a^2$.

Argument alternatiu (per reducció a l'absurd): Si fos $5|a^2$, seria $5|(a^2-(5(5q^2+8q+3)))=1$, d'on $5|1$, que no és cert.

Observació. S'hauria pogut compactar aquest estudi per casos, ja que $r\in\{1,2,3,4\}$ (una manera de dir que $5\nmid a$) equival a $r^2\in\{1,4,9,16\}$. També de $a^2=(5q+r)^2=25q^2+10rq+r^2=5(5q^2+2rq)+r^2$ podem escriure

$a^2-5(5q^2+2rq)=r^2$. Si fos $5|a^2$, seria $5|(a^2-5(5q^2+2rq))$, és a dir, $5|r^2$, que no es compleix en cap dels casos, ja que $r^2\in\{1,4,9,16\}$ ($5\nmid 1\wedge 5\nmid 4\wedge 5\nmid 9\wedge 5\nmid 16$).

Mètode 2. Si el lector coneix el lema d'Euclides (vegeu el capítol preliminar), que afirma, per a nombres enters c,d:

$(p \text{ primer} \wedge p|cd)\rightarrow(p|c\vee p|d)$,

aleshores es pot aplicar amb $p=5$, $c=a$ i $d=a$, i es conclou que $5|a$.

Mètode 3. Per reducció a l'absurd. Suposem, com a punt de partida, que $5|a^2\wedge 5\nmid a$ és cert. S'haurien de fer argumentacions similars a les del mètode 1.

Resolt el subproblema, continuem amb l'argumentació. Tenim, doncs, $5|a$. Per tant, existeix un k nombre enter tal que $a=5k$. Ara podem substituir $a=5k$ a l'anterior $5b^2=a^2$. Així, resulta $5b^2=(5k)^2=5^2k^2$, d'on, simplificant, $b^2=5k^2$.

Fem una argumentació similar a la d'abans, del principi:

Com que $5|5k^2$, per la igualtat anterior, resulta $5|b^2$ i ara, per qualsevol dels mètodes abans exposats, resulta $5|b$.

Resumint, hem arribat a: $5|a$ i $5|b$, la qual cosa és una **contradicció**, ja que a,b no tenen divisors comuns positius diferents de 1.

Per tant, $\sqrt{5}\in\mathbb{Q}$ és fals. És a dir, $\sqrt{5}\notin\mathbb{Q}$ és cert.

PROBLEMA 6.19

Proveu que $\sqrt{6} \notin \mathbb{Q}$

Solució. Per reducció a l'absurd: Suposem que $\sqrt{6} \in \mathbb{Q}$, és a dir, que podem expressar $\sqrt{6}$ com a fracció racional irreductible, $\sqrt{6} = \dfrac{a}{b}$. Aleshores:

$$\sqrt{6} = \frac{a}{b} \Rightarrow 6 = \frac{a^2}{b^2} \Rightarrow a^2 = 6b^2 \overset{6|6b^2}{\Rightarrow} 6|a^2 \Rightarrow 2 \cdot 3|a^2 \Rightarrow (2|a^2 \wedge 3|a^2).$$

A partir d'aquí, hi ha diverses possibilitats:

- De $2|a^2$, se'n deriva $2|a$ per diversos mètodes: aplicació del lema d'Euclides (vegeu capítol de preliminars), o bé pel contrarecíproc, o bé per reducció a l'absurd. Així, $a = 2k$ per a algun enter k, d'on, substituint a $a^2 = 6b^2$, resulta $(2k)^2 = 6b^2$, d'on $2k^2 = 3b^2$. Així $2|3b^2$; pel lema d'Euclides és $2|3$ o $2|b^2$. Per tant, $2|b^2$. Novament, pel lema d'Euclides $2|b$, i així resulta que 2 divideix a i b, cosa que és una contradicció. Això conclou la demostració.
- Similarment a l'argumentació anterior, podem partir de $3|a^2$ i arribar a la contradicció que 3 és un divisor de a i de b, contradicció.

PROBLEMA 6.20

Proveu que $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$

Solució. Suposem que hem demostrat (per exemple, a l'exercici anterior) que $\sqrt{6}$ no és racional.

Resoldrem el problema *per reducció a l'absurd*.

En aplicació del mètode de demostració per reducció a l'absurd, suposem que $\sqrt{2} + \sqrt{3} \in \mathbb{Q}$. Aleshores és $\sqrt{2} + \sqrt{3} = \frac{a}{b}$, per a a, b enters convenients, amb $b \neq 0$. Elevant al quadrat, resulta: $2 + 2\sqrt{2}\sqrt{3} + 3 = \frac{a^2}{b^2}$, és a dir, $5 + \sqrt{6} = \frac{a^2}{b^2}$ $(b^2 \neq 0)$. Per tant, $\sqrt{6} = \frac{a^2}{b^2} - 5 = \frac{a^2 - 5b^2}{b^2} \in \mathbb{Q}$. Així, $\sqrt{6} \in \mathbb{Q}$ i, d'altra banda, $\sqrt{6} \notin \mathbb{Q}$, cosa que és una contradicció.

Per tant, $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

Enunciat addicional, que es pot resoldre a imitació dels anteriors en què es prova la irracionalitat de $\sqrt{2}$, $\sqrt{5}$, utilitzant el teorema d'Euclides ("si un nombre primer divideix un producte de dos factors, aleshores divideix algun dels factors"):

Proveu que, "si p és un nombre primer, aleshores $\sqrt{p}$ és irracional".

Ara podríem aplicar el mètode de demostració per reducció a l'absurd per a provar diverses implicacions, algunes ja demostrades per altres mètodes:

$2|n \Rightarrow 2|n^2$ (n enter)

$2 \nmid n \Rightarrow 2 \nmid n^2$ (n enter)

$2 \nmid n \Rightarrow 2 \nmid n^2$ (n enter)

$(2|a \wedge 2|b) \Rightarrow 2|(a+b)$ (a, b enters)

i molts altres de tipus similar. En realitat, s'han de quantificar i posteriorment negar la fórmula quantificada en aplicació del mètode. És a dir que, per exemple, en el primer, el mètode s'ha d'aplicar a:

$\forall n(2|n \rightarrow 2|n^2)$.

Hauríem de suposar que $\exists n(2|n \wedge 2 \nmid n^2)$ és cert i arribar a alguna contradicció.

En efecte, si $n = 2k$ per a algun k enter, resultaria $n^2 = (2k)^2 = 2(2k^2) = 2k'$, amb $k' = 2k^2$, enter. Així, n^2 seria parell, contradicció. O bé, ja que $n^2 = 2q+1$, amb q enter, resultaria $2q+1 = 2k'$, d'on $1 = 2(k'-q)$, múltiple de 2. Per tant, hem arribat a la contradicció: 1 és parell.

6.6. Demostració d'enunciats amb quantificació

Hi ha dues possibilitats:

- amb quantificador universal ($\forall$) i
- amb quantificador existencial ($\exists$).

6.6.1. Amb quantificador universal

Considerem el cas més senzill: $\forall x P(x)$, per exemple. Hi pot haver més d'un quantificador i l'estructura pot ser més complexa, com per exemple, a $\forall x \forall y P(x, y)$.

Si hem de demostrar $\forall x P(x)$, per exemple, podem procedir de la manera següent:

- Considerem x arbitrari, però fix per a la demostració.
- Per a l'objecte x anterior, es demostra $P(x)$.
- Finalment, es generalitza amb el quantificador universal, $\forall x P(x)$.

Exemple 6.29 Suposem que, en aquest exemple, el domini per a les variables és $\Omega = \mathbb{Z}$.

Com demostrar:

"Per tot nombre enter n, és $2|n \Rightarrow 2|n^2$"? O bé

$\forall n(2|n \rightarrow 2|n^2)$

$\forall n((n \in \mathbb{Z} \rightarrow (2|n \rightarrow 2|n^2))$

$\forall n((n \in \mathbb{Z} \wedge 2|n) \rightarrow 2|n^2)$.

Procedim de la manera següent:

a) Fixem n, d'altra banda arbitrari.
b) Per a aquest n, demostrem la propietat: $2|n \rightarrow 2|n^2$. Aquesta és la part tècnica de la demostració, la part que s'ha de resoldre; en el cas d'aquest exemple, s'ha fet en problemes anteriors. La tècnica demostrativa pot ser diversa (directa, pel contrarecíproc, per reducció a l'absurd, per casos o altres).
c) Un cop demostrat, es generalitza amb el quantificador universal:

$$\forall n(2|n \rightarrow 2|n^2).$$

Idea de la demostració (punt b anterior): si $2|n$, aleshores $n = 2k$ per a algun k enter. Per tant, $n^2 = (2k)^2 = 2(2k^2) = 2k'$, d'on $2|n^2$. ■

Exemple 6.30 "El producte de dos nombres enters senars qualssevol és senar"
"Per a tot a,b senars, és ab senar"
$\forall a \forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$ (a $\mathbb{Z}$).

a) Es consideren a i b enters qualssevol però fixos per a la demostració.
b) S'extreu la propietat de l'estructura de quantificació, és a dir:

$$(2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab.$$

c) Es demostra, per a aquests a,b fixos: $(2 \nmid a \wedge 2 \nmid b) \Rightarrow 2 \nmid ab$ (aquesta és la part tècnica, de dificultat variable depenent de l'enunciat).
d) Es quantifica finalment, generalitzant: $\forall a \forall b((2 \nmid a \wedge 2 \nmid b) \rightarrow 2 \nmid ab)$.

Idea de la demostració del punt c anterior: existeixen enters k,k' convenients tals que $a = 2k+1$ i $b = 2k'+1$, d'on $ab = (2k+1)(2k'+1) = 2(2kk'+k+k')+1$, senar. ■

Una altra possibilitat consisteix a demostrar $\forall x P(x)$ per **reducció a l'absurd**. Partim de suposar certa la negació de l'afirmació, és a dir, $\exists x \neg P(x)$, i cal arribar a una contradicció.

Per a estructures més complicades (per exemple, amb quantificadors universals a l'interior), com seria:

$$\forall x(P(x) \rightarrow \forall y(Q(y) \rightarrow R(x,y)))$$

ens podem inspirar en les situacions bàsiques descrites anteriorment.

6.6.2. Amb quantificador existencial

Vegem-ne un cas senzill estructuralment: $\exists x P(x)$. Els enunciats poden ser més complexos, amb la possibilitat de barreges dels dos quantificadors:

$\exists x \exists y P(x,y)\ldots$

$\exists x \forall y \exists z\ldots$

$\forall x \exists y\ldots$ (exemple, a la definició de límit)

"Existeixen infinits nombres primers".

Un bon nombre de resultats de càlcul són d'existència. Per exemple, el teorema de Bolzano (funcions contínues), el teorema de Rolle (derivació), el teorema del valor mitjà (derivació), el teorema de Weierstrass d'assoliment de valors extrems, en l'expressió del residu en el teorema de Taylor. Rarament s'obté una expressió explícita d'existència: la demostració pot ser *per reducció a l'absurd*. Per exemple, en el cas del teorema de Bolzano, per a una funció contínua $f : [a,b] \to \mathbb{R}$ amb $f(a)f(b) < 0$, es demostra l'existència d'algun $c \in (a,b)$ tal que $f(c) = 0$. El lector pot consultar [POZO2013].

Alguns d'aquests teoremes generals permeten obtenir resultats d'existència per a casos particulars:

Exemple 6.31 Vegem-ne un exemple senzill.

Existeix alguna solució real de $x^2 = 2$ a l'interval $(1,2)$; en efecte, considerem $f(x) = x^2 - 2$, funció contínua, amb $a = 1$ i $b = 2$. Aleshores existeix c, amb $1 < c < 2$ tal que $f(c) = 0$, és a dir, $c^2 - 2 = 0$, en aplicació del teorema de Bolzano. ■

En el cas $\exists x P(x)$ o, de manera més precisa i per a un domini Ω, per a demostrar l'enunciat, podem procedir:

- exhibint algun element x del domini per al qual $P(x)$ sigui cert.
- per reducció a l'absurd, suposant que $\exists x P(x)$ és fals (és a dir, que $\neg \exists x P(x)$ és cert o, equivalentment, que $\forall x \neg P(x)$ és cert), i arribant a una contradicció. Per exemple, en el cas de l'existència d'infinits nombres primers (però aleshores l'enunciat és formalment més complex).

Vegem el cas de les solucions de l'equació de segon grau $ax^2 + bx + c = 0$ a coeficients a,b,c reals, $a \neq 0$. És un cas de clara dependència del domini al qual puguin pertànyer les solucions.

Exemple 6.32 L'afirmació $\forall a \forall b \forall c (a \neq 0 \to \exists x(ax^2 + bx + c = 0))$ és certa en $\mathbb{C}$. Per a la seva demostració fixem $a \neq 0, b, c$ (d'altra banda, coeficients arbitraris) i aportem alguna solució. Es pot obtenir constructivament o bé es formula i ***es comprova***. Per exemple, si afirmem que les solucions són

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ i } x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

ens podem limitar a una comprovació: $ax_1^2 + bx_1 + c = 0$. En efecte:

$$ax_1^2 + bx_1 + c = a\left(\frac{-b + \sqrt{b^2 - 4ac}}{2a}\right)^2 + b\left(\frac{-b + \sqrt{b^2 - 4ac}}{2a}\right) + c = \cdots = 0.$$

Per demostrar l'existència d'alguna solució, amb la comprovació d'una que ho sigui, n'hi ha prou (x_1 o x_2).

L'afirmació no és certa en el conjunt dels nombres reals (per exemple, per a $a=1$, $b=1$, $c=1$); com és ben sabut, és certa quan $b^2-4ac \geq 0$. Així, doncs:

$\forall a \forall b \forall c((a \neq 0 \wedge b^2-4ac \geq 0) \rightarrow \exists x(ax^2+bx+c=0))$ és certa en $\mathbb{R}$.

Vegem un altre mètode per a demostrar l'existència de solucions: és un ***mètode constructiu***, en què s'obtenen deductivament, explícitament les solucions:

L'equació de segon grau $ax^2+bx+c=0$, amb $a>0$ (anàlogament, en el cas $a<0$), $a,b,c \in \mathbb{R}$ té dues solucions (en $\mathbb{C}$, conjunt del nombres complexos). La demostració és constructiva i aporta l'expressió explícita de les solucions (ja ben conegudes del lector). Considerem $F(x)=ax^2+bx+c=a(x^2+\frac{b}{a}x+\frac{c}{a})$. Completant quadrats a l'expressió $x^2+\frac{b}{a}x$, resulta $F(x)=a(((x+\frac{b}{2a})^2-\frac{b^2}{4a^2})+\frac{c}{a})$. També resulta $F(x)=0$ si, i només si, $(x+\frac{b}{2a})^2=\frac{b^2}{4a^2}-\frac{c}{a}$, si, i només si, $(x+\frac{b}{2a})^2=\frac{b^2-4ac}{4a^2}$.

En $\mathbb{C}$ (o bé en $\mathbb{R}$, si $b^2-4ac \geq 0$), podem escriure $x+\frac{b}{2a}=\pm\sqrt{\frac{b^2-4ac}{4a^2}}$, d'on

$x=-\frac{b}{2a}\pm\sqrt{\frac{b^2-4ac}{4a^2}}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$, la coneguda fórmula explícita per a les solucions de l'equació de segon grau. ■

I ara demostrem l'existència d'infinits nombres primers, un exemple més de la metodologia de demostració ***per reducció a l'absurd***:

Exemple 6.33 (de fet, és un teorema important) *Existència d'infinits nombres primers* (el resultat és interessant per si mateix, a part d'il·lustrar un aspecte de les tècniques demostratives). Es pot provar que existeixen infinits nombres primers. La demostració no és constructiva, en el sentit que no els enumera (impossible) ni aporta cap fórmula ni mètode per obtenir-los tots.

Demostració. Suposem que el nombre de primers és finit i siguin $p_1,\cdots,p_n$ tots els nombres primers ($p_i \geq 2$). Considerem $q=p_1\cdots p_n+1$. El nombre q no pot ser primer ja que, si ho fos, seria algun dels de la llista anterior, és a dir, $q=p_{i_0}$, per a algun $1 \leq i_0 \leq n$; aleshores tindríem $p_{i_0}=p_1\cdots p_{i_0}\cdots p_n+1>p_1\cdots p_{i_0}\cdots p_n$. Essent $p_i \geq 2$, $i=1,\cdots,p$, és $p_1\cdots p_{i_0}\cdots p_n \geq p_{i_0}$. Per tant, $p_{i_0}>p_{i_0}$, que és contradictori.

Si q és compost, té divisors primers. Sigui p_{i_0} un d'aquests divisors, que òbviament divideix també $p_1\cdots p_n$, ja que n'és un dels factors. Per tant, és divisor de la diferència $1=q-p_1\cdots p_n$, la qual cosa és una contradicció.

Per tant, el conjunt de nombres primers ha de ser infinit.

Observeu que aquest és, doncs, un exemple de demostració per reducció a l'absurd. Formalitzadament, l'enunciat és p: "existeixen infinits nombre primers"; suposem $\neg p$, és a dir, "el conjunt de nombres primers és finit". ■

I ara un exemple de resultat d'existència negatiu:

Exemple 6.34 "No existeixen solucions reals de l'equació $x^2+x+1=0$".

És a dir:

$\neg\exists x(x^2+x+1=0)$ (en $\mathbb{R}$), que equival a
$\forall x\neg(x^2+x+1=0)$, que equival a
$\forall x(x^2+x+1=0\neq 0)$.

En efecte, si existís alguna solució, completant quadrats podríem escriure

$x^2+x+1=(x^2+x)+1=(x+\frac{1}{2})^2-(\frac{1}{2})^2+1=(x+\frac{1}{2})^2+\frac{3}{4}>0.$ ■

6.7. Equivalències

Equivalències amb dos enunciats

Recordem l'equivalència lògica $A\leftrightarrow B\equiv(A\rightarrow B)\wedge(B\rightarrow A)$.

Quan escrivim $A\Leftrightarrow B$, volem dir $A\Rightarrow B$ i $B\Rightarrow A$, de manera que hem de demostrar dues implicacions si volem demostrar l'equivalència ($\Leftrightarrow$).

Exemple 6.35 Vegem diversos exemples d'equivalències, per a n enter:

$2|n\Leftrightarrow 2|n^2$,
$2\nmid n\Leftrightarrow 2\nmid n^2$,
$3|n\Leftrightarrow 3|n^2$,
$3|n\Leftrightarrow 3|n^7$. ■

Exemple 6.36 Si tenim l'equivalència, que s'enuncia per a nombres enters:

$3|n\Leftrightarrow 3|n^5$

(amb quantificació universal (un altre enunciat de fet) seria:

$\forall n(3|n\Leftrightarrow 3|n^5))$,

per a la demostració de $3|n\Leftrightarrow 3|n^5$ o del "nucli" de $\forall n(3|n\Leftrightarrow 3|n^5)$, cal demostrar separadament dues implicacions:

$3|n\Rightarrow 3|n^5$
$3|n^5\Rightarrow 3|n$

Es concretarà a l'exemple següent. ■

Observació: En algunes ocasions, s'aconsegueix encadenar una seqüència d'equivalències o afirmacions equivalents, i així queda demostrada l'original $P_1 \Leftrightarrow P_m$ per transitivitat: la seqüència $P_1 \Leftrightarrow P_2 \Leftrightarrow \cdots \Leftrightarrow P_{m-1} \Leftrightarrow P_m$ demostra $P_1 \Leftrightarrow P_m$. En aquests casos, no cal demostrar equivalències separadament.

Exemple 6.37 Per a n enter, demostreu les implicacions:

$3|n \Rightarrow 3|n^5$

$3|n^5 \Rightarrow 3|n$

Les demostrem separadament.

1. Aportem una demostració directa per a la primera: $3|n \Rightarrow 3|n^5$.

   Hipòtesi: $3|n$.

   Tesi: $3|n^5$.

   Per la hipòtesi, existeix un enter k tal que $n = 3k$. Ara substituïm a n^5 l'expressió anterior per a n: $n^5 = (3k)^5 = 3 \cdot (3^4k^5) = 3k'$, múltiple de 3, amb $k' = 3^4k^5$.

   No sembla factible (o no fàcil) demostrar aquesta implicació pel contrarecíproc, és a dir, demostrar $\neg 3|n^5 \Rightarrow \neg 3|n$.

2. Vegem una demostració de $3|n^5 \Rightarrow 3|n$.

Mètode 1 (directe). Apliquem el lema d'Euclides a la situació $3|n \cdot n \cdot n \cdot n \cdot n$ amb 3 de nombre primer: es conclou que $3|n \vee 3|n \vee 3|n \vee 3|n \vee 3|n$, és a dir, $3|n$.

Mètode 2 (pel contrarecíproc). Hem de veure que $\neg 3|n \Rightarrow \neg 3|n^5$, és a dir, $3 \nmid n \Rightarrow 3 \nmid n^5$. Considerant el residu de la divisió entera de n per 3, dos són els casos en què 3 no és divisor de n: $n = 3q + r$, amb $1 \leq r \leq 3 - 1 = 2$; els casos són $r = 1$, $r = 2$. Fem, doncs. una demostració per casos (utilitzarem la fórmula del binomi de Newton):

Cas 1 ($r = 1$, $n = 3q + 1$). Aleshores és $n^5 = (3q+1)^5 = \sum_{k=0}^{5} \binom{5}{k} (3q)^k 1^{5-k} = \sum_{k=0}^{5} \binom{5}{k} (3q)^k = 1 + \sum_{k=1}^{5} \binom{5}{k} (3q)^k = 1 + 3(\sum_{k=1}^{5} \binom{5}{k} 3^{k-1} q^k) = 1 + 3q'$, no múltiple de 3 (en efecte, si $1 + 3q'$ fos múltiple de 3, seria $1 + 3q' = 3w$, d'on $3(q' - w) = 1$ i seria $3|1$, absurd).

Cas 2 ($r = 2$, $n = 3q + 2$). Aleshores és $n^5 = (3q+2)^5 = \sum_{k=0}^{5} \binom{5}{k} (3q)^k 2^{5-k} = 2^5 + \sum_{k=1}^{5} \binom{5}{k} (3q)^k 2^{5-k} = 2^5 + 3(\sum_{k=1}^{5} \binom{5}{k} 3^{k-1} q^k 2^{5-k}) = 2^5 + 3q''$, no múltiple de 3 (en efecte, si $2^5 + 3q''$ fos múltiple de 3, seria $2^5 + 3q'' = 3t$, d'on $3(q'' - t) = 2^5$ i seria $3|2^5$, d'on $3|2$, absurd).

Mètode 3 (per reducció a l'absurd). Suposem $3|n^5 \wedge 3 \nmid n$. Hauríem de fer servir arguments similars als del mètode 2. ■

Observem també que si demostrem $A \Leftrightarrow B$, resulta demostrat $\neg A \Leftrightarrow \neg B$, que seria en el cas anterior $\neg 3|n \Leftrightarrow \neg 3|n^5$, és a dir, $3 \nmid n \Leftrightarrow 3| \nmid n^5$.

Enunciats com els anteriors de vegades també es presenten de la forma següent:

"Demostreu que són equivalents (2 enunciats o "afirmacions"):

a) Afirmació 1.
b) Afirmació 2."

Aleshores, com ja hem vist, cal demostrar $(a) \Leftrightarrow (b)$ o bé: $(a) \Rightarrow (b)$ i $(b) \Rightarrow (a)$.

Vegem un exemple concret d'aquesta formulació:

Exemple 6.38 Sigui n un nombre enter qualsevol. Proveu que són equivalents:

a) $n+1$ és senar.
b) $3n+1$ és senar.

Vegem-ne la demostració:

$(a) \Rightarrow (b)$: $n+1$ és senar $\Rightarrow$ $3n+1$ és senar.

Mètode 1. $3n+1 = (n+1)+2n$ és la suma d'un nombre senar ($n+1$, per hipòtesi) i el nombre parell $2n$. La suma d'un nombre senar i un nombre parell és senar i, per tant, $3n+1$ és senar.

Mètode 2. Si $n+1$ és senar, $n+1 = 2k+1$ per a algun enter k. Per tant, $n = (n+1)-1 = (2k+1)-1 = 2k$. Substituint, $3n+1 = 3(2k)+1 = 2(3k)+1 = 2k'+1$, senar.

Variant argumental: Si $n+1$ és senar, aleshores $n = (n+1)-1$ és parell, per ser la diferència de dos senars. Essent n parell, $3n$ és parell; $3n+1$ és senar, per ser la suma d'un parell i un senar. O també $3n+1 = n+(2n+1)$, suma de parell i senar i, per tant, senar.

Mètode 3 (pel contrarecíproc). Cal veure que, si $3n+1$ és parell, aleshores $n+1$ és parell.

En efecte, és $n+1 = (3n+1)-2n$, parell per ser la diferència de parells.

Variant argumental: $3n+1 = 2k$, amb k enter convenient. Per tant, $n = (3n+1)-2n = 2k-2n = 2(k-n)$, parell.

Mètode 4 (per reducció a l'absurd). Suposem que $n+1$ és senar i $3n+1$ és parell. És $3n+1 = (n+1)+(2n)$, senar, per ser la suma de parell i senar, contradicció.

L'altra implicació:

$(b) \Rightarrow (a)$: $3n+1$ és senar $\Rightarrow$ $n+1$ és senar.

Similarment a la demostració de la implicació anterior, per a aquesta també es poden formular diverses demostracions. En presentem només una (i el lector en pot aportar d'altres):

$n+1 = (3n+1)-2n$, que és senar per ser diferència d'un senar ($3n+1$, per hipòtesi) i un parell.

Equivalències amb més de dos enunciats

Considerem enunciats com els següents:

"Demostreu que són equivalents (3 enunciats o "afirmacions"):

a) Afirmació 1.

b) Afirmació 2.

c) Afirmació 3."

Estructura de la demostració: Hem de demostrar $(a) \Leftrightarrow (b)$, $(b) \Leftrightarrow (c)$; per transitivitat, queda demostrat $(a) \Leftrightarrow (c)$. També es pot procedir d'altres maneres, demostrant $(a) \Leftrightarrow (c)$, $(c) \Leftrightarrow (b)$, i queda demostrat $(a) \Leftrightarrow (b)$ per transitivitat. Demostrar una equivalència suposa normalment demostrar dues implicacions (llevat que s'aconsegueixi demostrar directament l'equivalència).

Altres possibilitats: cal demostrar totes les implicacions possibles entre (a), (b) i (c) ("totes amb totes"). Una demostració o esquema "triangular" pot alleugerir la feina: $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

Ara hem de demostrar separadament cadascuna d'aquestes implicacions:

$(a) \Rightarrow (b)$: "Afirmació 1" $\Rightarrow$ "Afirmació 2"

$(b) \Rightarrow (c)$: "Afirmació 2" $\Rightarrow$ "Afirmació 3"

$(c) \Rightarrow (a)$: "Afirmació 3" $\Rightarrow$ "Afirmació 1"

Es poden escollir altres ordres, com per exemple: $(c) \Rightarrow (b) \Rightarrow (a) \Rightarrow (c)$ o altres.

"Demostreu que són equivalents (4 enunciats o "afirmacions"):

a) Afirmació 1.

b) Afirmació 2.

c) Afirmació 3.

d) Afirmació 4."

Estructura de la demostració: Caldria provar les equivalències: $(a) \Leftrightarrow (b)$, $(b) \Leftrightarrow (c)$, $(c) \Leftrightarrow (d)$; per transitivitat, queda demostrat $(a) \Leftrightarrow (c)$. També es pot procedir en altres ordres: $(a) \Leftrightarrow (c)$, $(d) \Leftrightarrow (b)$, $(a) \Leftrightarrow (d)$; per transitivitat, resulta demostrat $(b) \Leftrightarrow (c)$; encara hi ha altres ordres possibles.

Dit d'una altra manera: cal demostrar que tota afirmació és equivalent a qualsevol altra, que és el mateix que dir que cal demostrar que tota afirmació implica qualsevol altra. Per transitivitat, pot quedar demostrat el mateix adoptant altres esquemes demostratius i provant menys implicacions. Una possibilitat és seguir un esquema circular de demostració:

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) \Rightarrow (a) \qquad \begin{array}{ccc} \text{(a)} & \Rightarrow & \text{(b)} \\ \Uparrow & & \Downarrow \\ \text{(d)} & \Leftarrow & \text{(c)} \end{array}$$

Ara hem de demostrar separadament cadascuna d'aquestes implicacions:

$(a) \Rightarrow (b)$: "Afirmació 1" $\Rightarrow$ "Afirmació 2"

$(b) \Rightarrow (c)$: "Afirmació 2" $\Rightarrow$ "Afirmació 3"

$(c) \Rightarrow (d)$: "Afirmació 3" $\Rightarrow$ "Afirmació 4"

$(d) \Rightarrow (a)$: "Afirmació 4" $\Rightarrow$ "Afirmació 1"

Altres esquemes demostratius. En teoria, és possible escollir altres ordres, suposant que no es presenten problemes tècnics, com per exemple:

$$(a) \Rightarrow (c) \Rightarrow (b) \Rightarrow (d) \Rightarrow (a) \qquad \begin{array}{ccc} \text{(a)} & \Rightarrow & \text{(c)} \\ \Uparrow & & \Downarrow \\ \text{(d)} & \Leftarrow & \text{(b)} \end{array}$$

O també, depenent de la dificultat tècnica per a fer una determinada demostració, podem triar altres esquemes: $(a) \Leftrightarrow (b)$ i un esquema circular: $(a) \Rightarrow (c) \Rightarrow (d) \Rightarrow (a)$.

Per a demostrar l'equivalència de **més** afirmacions que en els exemples anteriors, es procediria de manera similar.

Vegem els exercicis següents. Són de baixa dificultat tècnica per tal que se'n pugui mostrar més fàcilment l'estructura demostrativa.

PROBLEMA 6.21

Sigui n un enter. Proveu que són equivalents les afirmacions següents:

a) $n+2$ *és parell*

b) $n+3$ *és senar*

c) $5n+1$ *és senar*

d) $7n$ *és parell*

Solució. *Estructura de la demostració*: Cal demostrar que tota afirmació implica qualsevol altra. Per transitivitat, pot quedar demostrat el mateix adoptant altres esquemes demostratius i provant menys implicacions. Una possibilitat és provar:

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) \Rightarrow (a) \qquad \begin{array}{ccc} \text{(a)} & \Rightarrow & \text{(b)} \\ \Uparrow & & \Downarrow \\ \text{(d)} & \Leftarrow & \text{(c)} \end{array}$$

Ara hem de demostrar separadament cadascuna d'aquestes implicacions; demostrarem amb detall la primera:

$(a) \Rightarrow (b)$: $2|n+2 \Rightarrow 2 \nmid n+3$.

Mètode 1. Si $2|n+2$, existeix un enter k tal que $n+2=2k$, d'on $n=2k-2$. Substituint, $n+3=(2k-2)+3=2k+1$, senar.

Mètode 2. Tenim $n+3=(n+2)+1$. Per hipòtesi, $n+2$ és parell i, per tant, $n+3$ és la suma d'un parell i un senar. El resultat és senar.

Mètode 3. Pel contrarecíproc: cal provar $\neg 2 \nmid n+3 \Rightarrow \neg 2|n+2$, és a dir, $2|n+3 \Rightarrow 2 \nmid n+2$.

Variant argumental 1: $n+2=(n+3)-1$, la diferència d'un parell ($n+3$, per hipòtesi) i un senar; el resultat és senar.

Variant argumental 2: $n+3=2k+1$ per a un k enter convenient; per tant, $n+2=(n+3)-1=(2k+1)-1=2k$, parell.

Variant argumental 3: $n+3=2k+1$ per a un k enter convenient; per tant, $n=(2k+1)-3=2k-2$, d'on $n+2=(2k-2)+2=2k$, parell.

Mètode 4. Per reducció a l'absurd. Partim de $2|n+2 \wedge 2|n+3$ i arribem a un absurd, de diverses maneres possibles (que no es detallen).

$(b) \Rightarrow (c)$: $2 \nmid n+3 \Rightarrow 2 \nmid 5n+1$.

Tenim $5n+1=(n+3)-3+4n+1=(n+3)+(4n-2)=(n+3)+2(2n-1)$, suma d'un senar (per hipòtesi) i d'un parell: el resultat és senar.

Variant argumental 1. Per hipòtesi $n+3=2k+1$ per a un cert enter k, d'on $n=(2k+1)-3=2k-2=2(k-2)$. Així, n és parell i, per tant, $5n$ és parell. Ara bé, $5n+1$ és, doncs, la suma d'un parell més un senar, amb resultat de senar.

Variant argumental 2. Per hipòtesi, $n+3=2k+1$ per a un cert enter k, d'on $n=(2k+1)-3=2k-2=2(k-2)$. Per tant, $5n+1=(5\cdot 2(k-2)+1)=2\cdot 5(k-2)+1$, senar.

També es pot demostrar pel mètode del contrarecíproc i per reducció a l'absurd.

$(c) \Rightarrow (d)$: $2 \nmid 5n+1 \Rightarrow 2|7n$

Mètode 1. $7n=5n+2n=(5n+1)+(2n-1)$, suma de dos senars ($5n+1$ ho és per hipòtesi); per tant, $7n$ és parell.

Mètode 2. Per hipòtesi, $5n+1=2k+1$, per a un k enter. Per tant, $n=(2k+1)-4n-1=2(k-2n)$. Ara, substituint, $7n=7(2(k-2n))=2(7(k-2n))$, parell.

Mètode 3. Per hipòtesi, $5n+1=2k+1$, per a un k enter. Per tant, $5n=2k$; així $5n$ és parell. Per tant, n és parell (o bé aplicant el lema d'Euclides, o bé argumentant que, si n fos senar, aleshores també ho seria $5n$, cosa que és una contradicció. Per tant, $7n$ és parell.

Mètode 4 (contrarecíproc). Sigui $7n$ senar. Volem veure que $5n+1$ és parell. En efecte, $5n+1=7n-2n+1=7n-(2n-1)$, parell, per ser la suma de dos senars.

Variant argumental. Suposant $7n$ senar, és $7n = 2k+1$, d'on $5n+1 = 7n-2n+1 = 2k+1-2n-1 = 2(k-n)$, parell.

Variant argumental. Suposant $7n$ senar, és n senar (pel lema d'Euclides o perquè, si no ho fos, aleshores n seria parell i $7n$ seria parell). Per tant, $5n$ és senar, per ser el producte de senars; per tant, $5n+1$ és parell per ser la suma de dos senars.

$(d) \Rightarrow (a)$: $2|7n \Rightarrow 2|n+2$

Mètode 1. Essent $7n$ parell, n ha de ser parell, ja que, en cas contrari, $7n$ seria senar. Per tant, $n+2$ és suma de parells i, en conseqüència, és parell.

Mètode 2 (contrarecíproc). Suposem que $n+2$ és senar. Existeix un k enter tal que $n+2 = 2k+1$, d'on $n = (2k+1)-2 = 2k-1$. Substituint, $7n = 7(2k-1)$ és senar, per ser producte el de dos senars. També es pot veure així: $7n = 2(7k)-7$, suma d'un parell més un senar (la suma és senar); o bé: $7n = 2(7k)-7 = 2(7k)-2\cdot 3-1 = 2(7k-3)-1$, senar.

Altres esquemes demostratius. En teoria, és possible escollir altres ordres, suposant que no es presenten problemes tècnics per a provar les implicacions, com per exemple:

$(a) \Rightarrow (c) \Rightarrow (b) \Rightarrow (d) \Rightarrow (a)$

$$\begin{array}{ccc} \text{(a)} & \Rightarrow & \text{(c)} \\ \Uparrow & & \Downarrow \\ \text{(d)} & \Leftarrow & \text{(b)} \end{array}$$

PROBLEMA 6.22

Sigui n un enter. Proveu que són equivalents les afirmacions següents:

a) *n és senar.*

b) *$5n-2n^2$ és senar.*

c) *$n-5$ és parell.*

Solució. *Estructura de la demostració*: Cal demostrar que tota afirmació implica qualsevol altra. Per transitivitat, pot quedar demostrat el mateix adoptant altres esquemes demostratius i provant menys implicacions. Una possibilitat és provar:

$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$

Ara hem de demostrar separadament cadascuna d'aquestes implicacions:

$(a) \Rightarrow (b)$: Si n és senar, aleshores és de la forma $n = 2k+1$ per a algun $k \in \mathbb{Z}$. Provem que $5n-2n^2$ també és senar, és a dir, existeix $k' \in \mathbb{Z}$ tal que $5n-2n^2 = 2k'+1$. En efecte, utilitzant la hipòtesi, podem escriure: $5n-2n^2 = 5(2k+1)-2(2k+1)^2 = 10k+5-2(4k^2+4k+1) = -8k^2+2k+3 = 2(k-4k^2+1)+1 = 2k'+1$, amb $k' = k-4k^2+1$.

Argument alternatiu directe: si n és senar, també ho és $5n$, per ser el producte de dos senars; el producte $2n^2$ és parell. Ara, $5n-2n^2$ és la diferència d'un nombre senar i d'un nombre parell: el resultat és senar.

$(b) \Rightarrow (c)$: En primer lloc, un esquema *directe* de demostració: si $5n - 2n^2$ és senar, aleshores $5n - 2n^2 = 2k + 1$ per a algun $k \in \mathbb{Z}$. Amb la finalitat de fer aparèixer $n - 5$, sumem i restem aquesta expressió: $(n-5) + 4n + 5 - 2n^2 = 2k + 1$, d'on $n - 5 = 2k + 1 - 4n + 2n^2 - 5 = 2(k - 2n + n^2 - 2)$, múltiple de 2, és a dir, parell.

Podem veure un *altre argument per a una demostració directa*: suposem que $5n - 2n^2$ és senar. De la descomposició $5n - 2n^2 = n(5 - 2n)$, en deduïm que n no és parell, ja que, si ho fos, també ho seria $5n - 2n^2$. Per tant, n és senar i, en conseqüència, $n - 5$ és parell ($n - 5 = (2k + 1) - 5 = 2(k - 2)$).

Alternativament (contrarecíproc) podríem veure $\neg(c) \Rightarrow \neg(b)$. Suposem que $n - 5$ és senar; aleshores n és parell (en efecte, $n - 5 = 2k + 1$ i, per tant, $n = 2k + 1 + 5 = 2(k+3)$). Ara bé, $5n - 2n^2 = n(5 - 2n)$, que és parell perquè té el factor n parell (també es pot provar substituint $n = 2t$ en $5n - 2n^2$ i comprovant que té el factor 2).

Encara es podria considerar una *altra variant argumental (contrarecíproc)*. Si $n - 5$ és senar, n és parell, com hem vist a la variant anterior. Reescrivim $5n - 2n^2 = n + (4n - 2n^2) = n + 2(2n - n^2)$, parell, com a suma de dos parells.

Encara es podria formular d'una *altra manera (contrarecíproc)*. Si $n - 5$ és senar, es pot escriure, per a un adequat $k \in \mathbb{Z}$, $n - 5 = 2k + 1$, d'on $n = 2k + 6$; substituïm a l'expressió $5n - 2n^2$ i en resulta: $5n - 2n^2 = 5(2k+6) - 2(2k+6)^2 = (2k+6)(5 - 4k - 12) = 2(k+3)(-4k-7) = 2k'$, parell. És a dir, $\neg c \Rightarrow \neg b$.

$(c) \Rightarrow (a)$: Si $n - 5$ és parell, aleshores $n - 5 = 2k$, per a algun $k \in \mathbb{Z}$. Per tant, $n = 2k + 5 = 2(k+2) + 1 = 2k' + 1$, senar.

PROBLEMA 6.23

Sigui n un nombre natural, $n \geq 2$. Siguin A, B matrius quadrades d'ordre n. Proveu que són equivalents les afirmacions següents:

a) $AB = BA$

b) $(A+B)^2 = A^2 + 2AB + B^2$

c) $(A-B)^2 = A^2 - 2AB + B^2$

d) $(A+B)(A-B) = A^2 - B^2$

Solució. *Estructura de la demostració*: Cal demostrar que cadascuna de les afirmacions implica qualsevol altra. Per transitivitat, es pot demostrar el mateix adoptant altres esquemes demostratius i provant menys implicacions. Una possibilitat és provar:

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) \Rightarrow (a) \qquad \begin{array}{ccc} \text{(a)} & \Rightarrow & \text{(b)} \\ \Uparrow & & \Downarrow \\ \text{(d)} & \Leftarrow & \text{(c)} \end{array}$$

Ara s'haurien de demostrar separadament cadascuna d'aquestes implicacions. Demostrem-ne només alguna:

$(a) \Rightarrow (b)$: ...

$(b) \Rightarrow (c)$: $(A-B)^2 = (A+(-B))^2 \overset{(b)}{=} A^2 + 2A(-B) + (-B)^2 = A^2 + 2(-AB) + B^2 = A^2 - 2AB + B^2$.

$(c) \Rightarrow (d)$: ...

$(d) \Rightarrow (a)$: Tenim $(A+B)(A-B) = A(A-B) + B(A-B) = A^2 + A(-B) + BA + B(-B) = A^2 - AB + BA - B^2$. Aplicant aquesta última igualtat i (d), resulta $-AB + BA = 0$, és a dir, $AB = BA$, o sigui, (a).

6.8. Contraexemples

Un **contraexemple** per a una afirmació $\mathscr{A}$ (amb quantificador universal) sobre un domini Ω és un element del domini que nega (contradiu) l'afirmació.

Suposem que tenim una afirmació del tipus $\forall x P(x)$ (x en un determinat domini Ω). És falsa si, i només si, la negació és certa, és a dir, si, i només si, $\neg\forall x P(x)$ és cert. Però això és equivalent a afirmar que $\exists x \neg P(x)$ és cert, en el mateix domini. És a dir, per a aquest x, és $P(x)$ fals.

De manera més completa pel que fa a la formalització:

Afirmació: $\forall x (x \in \Omega \to P(x))$.

Negació de l'afirmació: $\neg\forall x (x \in \Omega \to P(x))$.

Equivalentment, $\exists x \neg(x \in \Omega \to P(x))$.

Equivalentment, $\exists x (x \in \Omega \wedge \neg P(x))$.

Es pot reformular dient que "existeix algun $x_0 \in \Omega$ tal que $P(x_0)$ és fals". Si aquesta última afirmació és certa, aleshores, amb l'existència d'aquest element x_0, demostrem la falsetat de l'afirmació original: $\forall x (x \in \Omega \to P(x))$. Es diu que x_0 és un **contraexemple** per a l'afirmació $\forall x (x \in \Omega \to P(x))$ i que en demostra la falsedat.

Per tant, per a demostrar la falsedat d'enunciats com $\forall x P(x)$, n'hi ha prou a *aportar-ne un contraexemple*.

Exemple 6.39 Considerem l'afirmació: "Tot nombre primer és senar".

És falsa: n'hi ha prou amb el **contraexemple** $n = 2$, primer parell. ■

En cas que l'afirmació sigui sobre m elements, com a $\forall x_1 \cdots \forall x_m P(x_1, \cdots, x_m)$, aleshores un contraexemple, si escau, serà una m-pla d'elements $a_1, \cdots, a_m$ per als quals $P(a_1, \cdots, a_m)$ sigui fals. Aquesta és la situació que es presenta als dos exemples següents:

Exemple 6.40 Considerem l'afirmació: "El producte de matrius quadrades d'ordre $n \geq 2$ és commutatiu". L'afirmació és, per a matrius d'ordre n, $\forall A \forall B (AB = BA)$.

L'afirmació és falsa. Ho demostrem amb un **contraexemple**:

$$\left(\begin{array}{cc|ccc} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right) \cdot \left(\begin{array}{cc|ccc} 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right) = \left(\begin{array}{cc|ccc} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right)$$

$$\left(\begin{array}{cc|ccc} 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right) \cdot \left(\begin{array}{cc|ccc} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right) = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right)$$

Les caixes matricials 2×2 "no commutatives" de l'extrem superior esquerre poden ser substituïdes per altres caixes que no commutin i també es poden localitzar en altres posicions de les matrius.

És cert: $\forall n (n \geq 2 \to \exists A \exists B\ (AB \neq BA))$.

Observació. Estem dient que per a cada $n \geq 2$, $\exists A \exists B (AB \neq BA)$, cosa que no impedeix que hi pugui haver parelles de matrius que commuten. Per exemple, $AI = IA = A$, $AA^{-1} = A^{-1}A = I$ (per a matrius invertibles), o el producte de dos canvis d'escala, o el producte de dues matrius de rotació en el pla respecte de l'origen. ■

Moltes vegades es fan conjectures sobre possibles propietats que no se sap si són certes. Una possibilitat per a demostrar que no ho són és buscar-ne un contraexemple (amb un n'hi ha prou, però pot no ser fàcil de trobar). Sabem que en el conjunt dels nombres reals es compleix la propietat distributiva del producte respecte de la suma. Però podem afirmar el mateix per a una hipotètica distributivitat de la suma respecte del producte?

Exemple 6.41 Considerem l'afirmació en el conjunt dels nombres reals:

"La suma és distributiva respecte del producte". És cert?

Formalment, seria: $\forall x \forall y \forall z\ (x + yz = (x+y)(x+z))$.

L'afirmació és **falsa**. Ho demostrem amb un **contraexemple**:

$x = 1$, $y = 1$, $z = 1$: per a aquests valors, no es compleix la igualtat.

No sempre és fàcil trobar contraexemples (és possible que no se sàpiga si la propietat és certa). En aquest exemple, pot ser útil imposar la condició i potser això ens portarà a veure que la propietat és falsa, i proporcionarà al mateix temps una font de contraexemples (encara que amb un n'hi hagi prou). Vegem-ho, en relació amb l'exemple anterior:

Imposem:

$x+yz=(x+y)(x+z)$

$x+yz=x^2+xz+yx+yz$

$x=x^2+xz+yx$

$x^2+xz+yx-x=0$

$x(x+y+z-1)=0$

D'on $x=0$ o $x+y+z-1=0$. Per tant, si $x\neq 0$ i $x+y+z-1\neq 0$, amb els valors corresponents no es compleix la igualtat i així en tenim contraexemples. Per exemple, $x=5$, $y=3$, $z=-2$.

Comentari. Observem que hem deduït:

$x+yz=(x+y)(x+z)\Rightarrow (x=0\vee x+y+z-1=0)$.

Per tant (contrarecíproc), $\neg(x=0\vee x+y+z-1=0)\Rightarrow \neg(x+yz=(x+y)(x+z))$. És a dir, aplicant De Morgan, $(x\neq 0\wedge x+y+z-1\neq 0)\Rightarrow x+yz\neq (x+y)(x+z)$. ■

De vegades, el que busquem és un **exemple** que validi (demostri) una afirmació:

Exemples 6.42

Exemple 1. "El producte de matrius no és commutatiu" (en el sentit que no ho és sempre), és a dir, que algunes matrius no commuten (però no necessàriament tota parella). És a dir, interpretat així és $\exists A\exists B(AB\neq BA)$. La demostració d'aquest resultat consisteix a mostrar dues matrius concretes que no commutin. És a dir, un exemple concret com a demostració d'un resultat d'existència. Per exemple,

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

$$AB=\begin{pmatrix}1&0\\-1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\0&-1\end{pmatrix}$$

$$BA=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\-1&0\end{pmatrix}=\begin{pmatrix}-1&0\\1&0\end{pmatrix}$$

De fet, la parella anterior de matrius A,B és un contraexemple per a l'afirmació (falsa) "El producte de matrius és commutatiu". ■

Exemple 2. "La composició d'aplicacions en un conjunt no és commutativa" (en el sentit que existeix un parell d'aplicacions que no commuten; no s'afirma que per a qualsevol parella no hi hagi commutativitat). També queda demostrada l'afirmació aportant dos exemples concrets de funcions en un conjunt A ($f,g:A\mapsto A$).

És a dir, s'hauria de veure que existeix un A convenient (per exemple, el conjunt dels nombres reals) i que, definides en A, $\exists f\exists g(f\circ g\neq g\circ f)$. És a dir, $\exists f\exists g\exists x((f\circ g)(x)\neq (g\circ f)(x))$.

Per exemple, $A = \mathbb{R}$, $f(x) = x+1$, $g(x) = x^2 - 1$. Aleshores:

$(f \circ g)(x) = f(g(x)) = f(x^2-1) = (x^2-1)+1 = x^2$,
$(g \circ f)(x) = g(f(x)) = g(x+1) = (x+1)^2 - 1 = (x^2+2x+1) - 1 = x^2 + x$. Per exemple, per a $x = 1$, no hi ha igualtat.

És a dir, $(f \circ g)(1) \neq (g \circ f)(1)$.

Naturalment, aquest exemple seria un contraexemple per a l'afirmació falsa: "La composició d'aplicacions és commutativa". ■

6.9. Demostrar una conjunció ("A i B")

$A \wedge B$ **Problema**: Cal demostrar una afirmació de la forma $A \wedge B$.

Exemples 6.43

Exemple 1. $2|4a \wedge 3|6b$ (a, b enters). ■

Exemple 2. $2|n(n+1) \wedge 3|n(n+1)(n+2)$ (n enter). ■

Exemple 3. $2|(n-3)(n-2) \wedge 3|(n-1)n(n+1) \wedge 4|n(n+1)(n+2)(n+3)$ (n enter). ■

Exemple 4. $2|n^2+n+2 \wedge 2|n^2-n+4$ (n enter). ■

En genèric, cal provar per separat (amb dues demostracions independents):

- que A és cert
- que B és cert

Es fan dues demostracions independents, pels mètodes que convinguin, depenent de l'estructura de les afirmacions A i B. Cada una de les A, B pot tenir qualsevol estructura, de manera que difícilment podem aquí dir res en general: per exemple, si $A = A_1 \to A_2$, posem per cas, aleshores es pot intentar demostrar A mitjançant una demostració directa, pel contrarecíproc, per reducció a l'absurd, per inducció si escau, per casos si escau, o per altres mètodes.

La descripció anterior de com procedir és la més senzilla i natural, sobretot si A, B no estan relacionades. Ara bé, hi pot haver altres situacions que reclamin altres possibilitats.

Vegem altres possibilitats, que indiquem simplement a efectes teòrics:

Per reducció a l'absurd

Si es tracta de demostrar $\mathscr{A} = A \wedge B$,

- Suposem (cert) $\neg\mathscr{A}$, és a dir $\neg(A \wedge B)$.
- L'argumentació avança a partir de $\neg(A \wedge B)$ o bé, aplicant l'equivalència de De Morgan, a partir de $\neg A \vee \neg B$.

– Cal arribar a una contradicció a cada un dels casos anteriors ($\neg A \vee \neg B$):
  - a partir només de $\neg A$, cal arribar a contradicció i
  - a partir només de $\neg B$, cal arribar a contradicció

  En efecte, cap de les dues pot ser certa (si el mètode funciona), ja que si una fos certa, aleshores ja ho seria la disjunció $\neg A \vee \neg B$.

– Aconseguit l'anterior, es conclou que $A \wedge B$ és cert.

  També es pot plantejar un camí alternatiu fent servir les equivalències (de fet observeu que a les fórmules de la dreta l'una és contrarecíproca de l'altra).

  $(\neg A \vee \neg B) \equiv A \rightarrow \neg B$
  $(\neg A \vee \neg B) \equiv (\neg B \vee \neg A) \equiv B \rightarrow \neg A$

  i hem de demostrar que qualsevol de les dues (són equivalents) ens porta a contradicció.

  Exercici:

  – Generalitzeu a $A \vee B \vee C$ (el cas de 3).
  – Generalitzeu a $A_1 \vee \cdots \vee A_n$.

6.10. Demostrar una disjunció ("A o B")

$A \vee B$ **Problema**: Cal demostrar una afirmació de la forma $A \vee B$.

En el cas anterior de demostracions de conjuncions, és clar i nítid que s'ha de demostrar separadament A i B, ja que el significat de la conjunció és clar. Intuïtivament, la disjunció és menys clara: què vol dir que hem de demostrar A o B? La situació resulta incòmoda, no tenim cap punt de partida: resulta més còmode demostrar implicacions o veracitat de condicionals, on tenim un punt de partida.

Per a això, intentem convertir una disjunció en un condicional, a continuació.

Convertim l'enunciat en un condicional

Apliquem diverses equivalències lògiques:

$A \vee B \equiv \neg(\neg A) \vee B \equiv \neg A \rightarrow B$ (per l'equivalència de la doble negació i l'expressió del condicional en termes de negació i disjunció).

Així, provar que és $A \vee B$ cert és el mateix que provar que $\neg A \rightarrow B$ és cert, és a dir, $\neg A \Rightarrow B$. Cal veure, doncs, que, si $\neg A$ és cert, aleshores B. "Si no es compleix A, aleshores es compleix B". "Es parteix de $\neg A$ i s'arriba a B".

Alternativament, podem considerar el contrarecíproc de $\neg A \rightarrow B$, que és $\neg B \rightarrow \neg\neg A \equiv \neg B \rightarrow A$ i, per tant hauríem de provar $\neg B \rightarrow A$. "Si no es compleix B, aleshores es compleix A". "Es parteix de $\neg B$ i s'arriba a A". Observem que també hi podem arribar per una altra seqüència d'equivalències lògiques:

$A \vee B \equiv B \vee A \equiv \neg(\neg B) \vee A \equiv \neg B \to A$

Per tant, cal provar una de les afirmacions següents:

"si A no és cert, vegem que B és cert"

"si B no és cert, vegem que A és cert"

Exemples 6.44 (amb "o")

Exemple 1. $2|n \vee 2 \nmid n$ (n enter). Equival a $2 \nmid n \to 2 \nmid n$. ■

Exemple 2. $3 \nmid n \vee 27|n^3$ (n enter). Equival a $3|n \to 27|n^3$. ■

Exemple 3. $3|n \vee 3|n+1 \vee 3|n+2$ (n enter) (amb 3). ■

Vegem-ne alguns exemples:

Exemple 6.45 Sigui n un nombre enter. Aleshores:

$3 \nmid n \vee 27|n^3$.

En efecte, equival a $3|n \to 27|n^3$, que es comprova fàcilment: existeix un enter k tal que $n = 3k$, d'on $n^3 = (3k)^3 = 3^3k^3 = 27k^3 = 27k'$, amb $k' = k^3$. ■

Exemple 6.46 Sigui n un nombre enter. Aleshores:

$2 \nmid n \vee 2 \nmid n^3 - 1$. És $A = 2 \nmid n$, $B = 2 \nmid n^3 - 1$.

Mètode 1. Podem provar equivalentment $\neg A \Rightarrow B$, és a dir, $\neg 2 \nmid n \Rightarrow 2 \nmid n^3 - 1$. En efecte:

$\neg 2 \nmid n \Rightarrow 2|n \Rightarrow \exists k \in \mathbb{Z} \wedge n = 2k$. Amb aquest k,

$n = 2k \Rightarrow n^3 - 1 = (2k)^3 - 1 = 2(2^2k^2) - 1 = 2k' - 1 \Rightarrow 2 \nmid n^3 - 1$, amb $k' = 2^2k^2$.

Mètode 2. Podem provar $\neg B \Rightarrow A$:

$\neg 2 \nmid n^3 - 1 \Rightarrow 2|n^3 - 1 \overset{\exists k \in \mathbb{Z}}{\Rightarrow} n^3 - 1 = 2k \Rightarrow n^3 = 2k + 1 \Rightarrow 2 \nmid n^3 \overset{(*)}{\Rightarrow} 2 \nmid n$.

(*): la implicació es pot demostrar pel contrarecíproc, per reducció a l'absurd, per aplicació del lema d'Euclides (vegeu el capítol de preliminars), per casos segons paritat de n.

Observació. També s'hauria pogut demostrar pel contrarecíproc directament. ■

Exemple 6.47 Sigui n un nombre enter. Aleshores:

$2|n \vee 2|n^3 - 1$. ($A = 2|n$, $B = 2|n^3 - 1$).

Podem demostrar equivalentment que $\neg 2|n \Rightarrow 2|n^3 - 1$ ($\neg A \Rightarrow B$). És a dir,

$2 \nmid n \overset{\exists k \in \mathbb{Z}}{\Rightarrow} n = 2k + 1 \Rightarrow n^3 - 1 = (2k+1)^3 - 1 = (2^3k^3 + 3(2k)^2 + 3(2k) + 1) - 1 = 2(2^2k^3 + 3 \cdot 2 \cdot k^2 + 3k) \overset{\exists k' \in \mathbb{Z}}{\Rightarrow} n^3 - 1 = 2k' \Rightarrow 2|n^3 - 1$. ■

Una altra possibilitat és **per reducció a l'absurd**:

$\mathscr{A} = A \vee B$

Suposem $\neg\mathscr{A} = \neg(A \vee B) \equiv (\neg A \wedge \neg B)$ (per De Morgan), és a dir, suposem $\neg A$ i $\neg B$ i arribem a una contradicció.

També podríem fer servir:

$\neg\mathscr{A} = \neg(A \vee B) \equiv (\neg A \wedge \neg B) \equiv \neg(A \to \neg B)$

Exercici:

- generalitzeu a $A \wedge B \wedge C$ (el cas de 3)
- generalitzeu a $A_1 \wedge \cdots \wedge A_n$

6.11. Prova d'enunciats del tipus $A \to B$ (casos especials)

Considerem alguns casos especials de condicionals.

6.11.1. Disjunció a l'antecedent

$(A \vee B) \to C$

Resulta útil l'equivalència lògica $(A \vee B) \to C \equiv (A \to C) \wedge (B \to C)$

Exemple 6.48 Si a, b són nombres enters,

$(7|a \vee 7|b) \Rightarrow 7|ab.$

En efecte:

Cas $7|a$. Si $7|a$, és $a = 7k$ per a algun enter k, d'on $ab = (7k)b = 7(kb)$. Per tant, existeix un enter k' tal que $ab = 7k'$ (prenent $k' = kb$). Així doncs, $7|ab$. Hem demostrat $7|a \Rightarrow 7|ab$.

Cas $7|b$. Si $7|b$, és $b = 7k$ per a algun enter k, d'on $ab = a(7k) = 7(ka)$. Per tant, existeix un enter k' tal que $ab = 7k'$ (prenent $k' = ka$). Així doncs, $7|ab$. Hem demostrat $7|a \Rightarrow 7|ab$.

Observació. D'aquest resultat, se'n deriva la veracitat del contrarecíproc:

$7 \nmid ab \Rightarrow \neg(7|a \vee 7|b)$ i, per De Morgan,

$7 \nmid ab \Rightarrow (\neg(7|a) \wedge \neg(7|b))$, és a dir,

$7 \nmid ab \Rightarrow (7 \nmid a \wedge 7 \nmid b)$.

Anàlogament:

$2 \nmid ab \Rightarrow (2 \nmid a \wedge 2 \nmid b)$.

$3 \nmid ab \Rightarrow (3 \nmid a \wedge 3 \nmid b)$. ■

Observació. A la demostració per casos trobem aquesta estructura.

6.11.2. Conjunció a l'antecedent

$(A \wedge B) \rightarrow C$

Exemple 6.49 $(12|a \wedge 18|a) \rightarrow 6|a$ (a enter). ■

Vegem una col·lecció d'exemples d'enunciats de tipus similar.

Exemple 6.50 Per a a, b nombres enters:

$(2|a \wedge 2|b) \Rightarrow 2|a+b$.

$(2 \nmid a \wedge 2|b) \Rightarrow 2 \nmid a+b$.

$(2|a \wedge 2 \nmid b) \Rightarrow 2 \nmid a+b$.

$(2 \nmid a \wedge 2 \nmid b) \Rightarrow 2|a+b$.

$(3|a \wedge 3|b) \Rightarrow 3|a+b$.

$(5|a \wedge 5|b) \Rightarrow 5|a+b$.

$(3 \nmid a \wedge 3|b) \Rightarrow 3 \nmid a+b$.

$(2 \nmid a+b \wedge 2|a) \rightarrow 2 \nmid b$. ■

Demostrem-ne alguns:

Exemple 6.51 Per a a, b nombres enters, $(2 \nmid a \wedge 2|b) \Rightarrow 2 \nmid a+b$.

Demostració

$2 \nmid a \Rightarrow \exists k(k \in \mathbb{Z} \wedge a = 2k+1)$ (per hipòtesi).

$2|b \Rightarrow \exists k'(k' \in \mathbb{Z} \wedge b = 2k')$ (per hipòtesi).

Per tant:

$a+b = (2k+1)+2k' = 2(k+k')+1 = 2k''+1$ (amb $k'' = k+k' \in \mathbb{Z}$). Per tant:

$\exists k''(k'' \in \mathbb{Z} \wedge a+b = 2k''+1)$. Per tant: $2 \nmid a+b$ (tesi). ■

Exemple 6.52 Per a a, b nombres enters, $(3|a \wedge 3|b) \Rightarrow 3|a+b$.

Hipòtesi: $3|a \wedge 3|b$. Completa: $a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 3|a \wedge 3|b$.

Tesi: $3|a+b$ (també $3|a \pm b$).

Demostració. Per la hipòtesi, existeixen enters k,k' tals que $a = 3k$ i $b = 3k'$, d'on $a + b = 3k + 3k' = 3(k + k') = 3k''$ (amb $k'' = k + k'$). Per tant, $3|a + b$. ■

Exemple 6.53 Per a a,b nombres enters, $(3 \nmid a \wedge 3|b) \Rightarrow 3 \nmid a \pm b$.

Suposem que a no és múltiple de 3. Per la divisió entera de a per 3, és $a = 3q + r$, amb q,r enters i amb $1 \leq r \leq 2$ (atès que $r \neq 0$, per ser a no divisible per 3; en general, és $0 \leq r < 3$).

Si $3|b$, existeix un k enter tal que $b = 3k$.

Per tant, $a + b = (3q + r) + 3k = 3(q + k) + r$, amb $1 \leq r \leq 2$.

Cas 1: $r = 1$. Aleshores $a + b = 3q' + 1$, no múltiple de 3 (*per reducció a l'absurd*: si ho fos, seria $1 + 3q' = 3q''$, d'on $1 = 3(q'' - q')$ i així $3|1$, contradicció).

Cas 2: $r = 2$. Aleshores $a + b = 3q' + 2$, no múltiple de 3 (si ho fos, seria $2 + 3q' = 3q''$, d'on $2 = 3(q'' - q')$ i així $3|2$, i això és una contradicció). ■

Exemple 6.54 Per a a,b nombres enters, $(2 \nmid a + b \wedge 2|a) \rightarrow 2 \nmid b$.

Per ser senar, $a + b = 2k + 1$ per a algun enter k. Per ser parell, $a = 2k'$ per a un enter k'. Aleshores $b = (a + b) - a = (2k + 1) - 2k' = 2(k - k') + 1 = 2k'' + 1$, senar, com havíem de veure.

Alternativament, $b = (a + b) - a$, senar, per ser la diferència d'un senar i un parell. ■

6.11.3. Disjunció al conseqüent

$A \rightarrow (B \vee C)$

Per a tractar aquest cas, resulta útil l'equivalència lògica:

$A \rightarrow (B \vee C) \equiv (A \wedge \neg B) \rightarrow C$

$A \rightarrow (B \vee C) \equiv (A \wedge \neg C) \rightarrow B$

En el cas de 3 (dues disjuncions al conseqüent), $A \rightarrow (B \vee C \vee D)$ és lògicament equivalent a diverses fórmules:

$(A \wedge \neg B) \rightarrow (C \vee D)$ (i altres de similars)

$(A \wedge \neg B \wedge \neg C) \rightarrow D$ (i altres de similars, com les següents)

$(A \wedge \neg B \wedge \neg D) \rightarrow C$

$(A \wedge \neg C \wedge \neg D) \rightarrow B$

Exemples 6.55 Per nombre reals x,y,z,n,m,

Exemple 1. $x + y \leq 1 \Rightarrow (x \leq \frac{1}{2} \vee y \leq \frac{1}{2})$.

Exemple 2. $x+y \leq n+m \Rightarrow (x \leq n \vee y \leq m)$. I també $x+y \leq n+m \Rightarrow (x \leq m \vee y \leq n)$.

Exemple 3. $x+y+z \leq 3 \Rightarrow (x \leq 1 \vee y \leq 1 \vee z \leq 1)$. ■

També es pot tractar per reducció a l'absurd, prenent com a punt de partida la suposició de veracitat de:

$A \wedge \neg B \wedge \neg C$

$A \wedge \neg B \wedge \neg C \wedge \neg D$

Aquestes fórmules s'obtenen per negació dels condicionals corresponents i aplicació posterior de l'equivalència de De Morgan.

També es podria demostrar pel contrarecíproc:

Exemple 6.56 Vegem $x+y+z \leq 3 \Rightarrow (x \leq 1 \vee y \leq 1 \vee z \leq 1)$.

Vegem $\neg(x \leq 1 \vee y \leq 1 \vee z \leq 1) \Rightarrow \neg(x+y+z \leq 3)$.

Per De Morgan, tenim $x > 1 \wedge y > 1 \wedge z > 1$. Per tant, $x+y+z > 1+1+1 = 3$, negació de $x+y+z \leq 3$. ■

Exemple 6.57 Siguin x, y nombres reals positius. Proveu:

$z = xy \Rightarrow (x \leq \sqrt{z} \vee y \leq \sqrt{z})$

Mètode 1. Pel mètode específic indicat al principi de la secció, veient

$(z = xy \wedge \neg(x \leq \sqrt{z})) \Rightarrow y \leq \sqrt{y}$. És a dir,

$(z = xy \wedge \neg(x > \sqrt{z})) \Rightarrow y \leq \sqrt{y}$.

Observeu que $z > 0$ i $\sqrt{z} > 0$. Aplicant $x > \sqrt{z}$, resulta $z = xy > \sqrt{z}y$, d'on $\frac{x}{\sqrt{z}} > y$. Ara bé, $\frac{z}{\sqrt{z}} = \frac{z\sqrt{z}}{(\sqrt{z})^2} = \sqrt{z}$. Per tant, $\sqrt{z} > y$, d'on $y \leq \sqrt{z}$.

Mètode 2. Pel contrarecíproc. Hem de demostrar equivalentment

$\neg(x \leq \sqrt{z} \vee y \leq \sqrt{z}) \Rightarrow \neg(z = xy)$. Per De Morgan, hem de demostrar:

$(x > \sqrt{z} \wedge y > \sqrt{z}) \Rightarrow z \neq xy$. En efecte, per la hipòtesi, resulta que

$xy > \sqrt{z}\sqrt{z} = (\sqrt{z})^2 = z$, d'on $xy > z$, i, doncs, $xy \neq z$.

Mètode 3. Per reducció a l'absurd. Suposem certa la negació del condicional:

$z = xy \wedge \neq (x \leq \sqrt{z} \vee y \leq \sqrt{z})$, equivalent per De Morgan a $z = xy \wedge (x > \sqrt{z} \wedge y > \sqrt{z})$.

Essent $y > 0$, $z > 0$, podem escriure $x > \sqrt{z} \Rightarrow xy > y\sqrt{z} \Rightarrow xy > \sqrt{z}\sqrt{z} = z$, d'on $xy \neq z$, la qual cosa és una contradicció. ■

6.11.4. Condicional al conseqüent

$A \rightarrow (B \rightarrow C)$

Per tractar aquest cas, resulta útil l'equivalència lògica:

$A \rightarrow (B \rightarrow C) \equiv (A \wedge B) \rightarrow C$

Exemples 6.58

Exemple 1. $3|n \Rightarrow (5|n \Rightarrow 15|n)$ (n enter). Equival a $(3|n \wedge 5|n) \Rightarrow 15|n$. ■

Exemple 2. $5|a \rightarrow (5|b \rightarrow 5|a+b)$ (a, b enters). Equival a $(5|a \wedge 5|b) \rightarrow 5|(a+b)$. ■

Exemple 3. $(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \rightarrow ((5|a \wedge 5|b) \rightarrow 5|a-b)$. Equival a $(a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge 5|a \wedge 5|b) \rightarrow 5|a-b$. ■

Exemple 4. $n \in \mathbb{Z} \rightarrow (2 \nmid n \rightarrow 2 \nmid n^3)$. ■

Exemple 6.59 "La suma de parells és parell"

Suposem r un nombre natural; $a_1, \cdots, a_r$ nombres enters. Tenim:

$2|r \rightarrow ((2|a_1 \wedge \cdots \wedge 2|a_r) \rightarrow 2|a_1 + \cdots + a_r)$, que equival a

$(2|r \wedge 2|a_1 \wedge \cdots \wedge 2|a_r) \rightarrow 2|a_1 + \cdots + a_r)$.

Considerant la pertinença als dominis indicats, podem quantificar:

$\forall r(2|r \rightarrow (\forall a_1 \forall a2 \cdots \forall a_r (2|a_1 \wedge \cdots \wedge 2|a_r) \rightarrow 2|a_1 + \cdots + a_r))$, que equival a

$\forall r \forall a_1 \forall a_2 \cdots \forall a_r ((2|r \wedge 2|a_1 \wedge \cdots \wedge 2|a_r) \rightarrow 2|a_1 + \cdots + a_r)$. ■

Exemple 6.60 "La Suma d'un nombre parell de senars és parell"

Suposem r un nombre natural; $a_1, \cdots, a_r$ nombres enters. Tenim:

$2|r \rightarrow ((2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_r) \rightarrow 2|a_1 + \cdots + a_r)$, que equival a $(2|r \wedge 2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_r) \rightarrow$

$2|a_1 + \cdots + a_r)$. ■

Exemple 6.61 "Suma d'un nombre senar de senars és senar"

Suposem r nombre natural, $a_1, \cdots, a_r$ nombres enters. Tenim

$2 \nmid r \rightarrow ((2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_r) \rightarrow 2 \nmid a_1 + \cdots + a_r)$, que equival a

$(2 \nmid r \wedge 2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_r) \rightarrow 2 \nmid a_1 + \cdots + a_r)$. ■

Exemples 6.62 Siguin a, b nombres enters.

Exemple 1. $2|a+b \rightarrow (2|a \rightarrow 2|b)$. Equival a $(2|a+b \wedge 2|a) \rightarrow 2|b$. ■

Exemple 2. $2|a+b \rightarrow (2 \nmid a \rightarrow 2 \nmid b)$. Equival a $(2|a+b \wedge 2 \nmid a) \rightarrow 2 \nmid b$. ■

Exemple 3. $2 \nmid a+b \rightarrow (2|a \rightarrow 2 \nmid b)$. Equival a $(2 \nmid a+b \wedge 2|a) \rightarrow 2 \nmid b$. ■

Exemple 4. $2 \nmid a+b \rightarrow (2 \nmid a \rightarrow 2|b)$. Equival a $(2 \nmid a+b \wedge 2 \nmid a) \rightarrow 2 \nmid b$.

Demostració de $2 \nmid a+b \rightarrow (2 \nmid a \rightarrow 2|b)$. Demostrem equivalentment $(2 \nmid a+b \wedge 2 \nmid a) \rightarrow 2 \nmid b$. Per hipòtesi, existeixen enters k, k' tals que $a+b = 2k+1$ i $a = 2k'+1$. Aleshores $b = (a+b)-a = (2k+1)-(2k'+1) = 2(k-k')$, parell. ■

Exemple 5. $3|a \rightarrow (3|a+b \rightarrow 3|b)$. Equival a $(3|a \wedge 3|a+b) \rightarrow 3|b$. ■

6.11.5. Conjunció al conseqüent

Considerem enunciats amb l'estructura $A \rightarrow (B \wedge C)$.

Per exemple:

Exemples 6.63

Exemple 1. Sense quantificar (sense generalitzar):

Per a x, y nombres reals,

$x^2 + y^2 = 0 \Rightarrow (x = 0 \wedge y = 0)$.

Generalització: $\forall x \forall y((x \in \mathbb{R} \wedge y \in \mathbb{R}) \rightarrow (x^2 + y^2 = 0 \rightarrow (x = 0 \wedge y = 0)))$.

$\forall x \forall y(x^2 + y^2 = 0 \rightarrow (x = 0 \wedge y = 0))$ (suposant com a universal el conjunt dels nombres reals). ■

Exemple 2. Per a x, y nombres reals,

$xy \neq 0 \Rightarrow (x \neq 0 \wedge y \neq 0)$. ■

Exemple 3. Per a x nombre enter,

$15|x \Rightarrow (3|x \wedge y5|x)$. ■

Què fer quan hem de demostrar enunciats amb l'estructura: $A \rightarrow (B \wedge C)$? És pràcticament obvi que cal provar separadament B i C a partir de A. Es veurà també formalitzadament.

Vegem diversos mètodes possibles per a efectuar aquestes demostracions.

Mètode 1: **Descomponent el problema (una implicació) en dos problemes (dues implicacions)**.

Tenim una equivalència lògica: $A \to (B \wedge C) \equiv (A \to B) \wedge (A \to C)$

La demostració de l'equivalència es pot fer per taules de veritat o utilitzant altres equivalències prèviament demostrades i disponibles:

$A \to (B \wedge C) \equiv \neg A \vee (B \wedge C)$
(per l'equivalència del condicional en termes de negació i disjunció)

$\equiv (\neg A \vee B) \wedge (\neg A \vee C)$ (per la distributivitat de $\vee$ respecte de $\wedge$)

$\equiv (A \to B) \wedge (A \to C)$ (per l'equivalència del condicional en termes de negació i disjunció).

En conseqüència, demostrar

$A \to (B \wedge C)$

equival a demostrar $(A \to B) \wedge (A \to C)$. És a dir, en termes d'implicació, demostrar $A \Rightarrow (B \wedge C)$ equival a demostrar separadament $A \Rightarrow B$ i $A \Rightarrow C$.

Apliquem el mètode amb l'exemple 1 anterior.

Exemple 6.64 Per a x, y nombres reals,

$x^2 + y^2 = 0 \Rightarrow (x = 0 \wedge y = 0)$.

Hem de demostrar separadament que:

$x^2 + y^2 = 0 \Rightarrow x = 0 \quad$ i

$x^2 + y^2 = 0 \Rightarrow y = 0$.

Les demostracions són anàlogues. Vegem la primera (i semblantment la segona):

Sempre és $x^2 \geq 0$ i $y^2 \geq 0$. Essent $y^2 \geq 0$, resulta $x^2 \leq x^2 + y^2$. Per tant, $0 \leq x^2 \leq x^2 + y^2$. Ara bé, per hipòtesi, és $x^2 + y^2 = 0$, d'on $0 \leq x^2 \leq x^2 + y^2 = 0$ i, per tant, $x^2 = 0$. En conseqüència, $x = 0$. ■

Exemple 6.65 Si a, b són enters, demostrar $2 \nmid ab \Rightarrow (2 \nmid a \wedge 2 \nmid b)$ equival a demostrar separadament $2 \nmid ab \Rightarrow 2 \nmid a$ i $2 \nmid ab \Rightarrow 2 \nmid b$.

Per exemple, per a la primera (i anàlogament per a la segona), podem procedir:

Mètode 1 Pel contrarecíproc, provant $2|a \Rightarrow 2|ab$ (si $a = 2k$, substituint a ab, resulta que $2|ab$).

Mètode 2 Per reducció a l'absurd, provant que $2 \nmid ab \wedge \neg 2 \nmid a$, és a dir, $2 \nmid ab \wedge \neg 2|a$ porta a contradicció (si $a = 2k$, substituint a ab resulta que $2|ab$, contradicció). ■

Aquest mètode també es pot veure com un exemple de conversió d'un problema en una col·lecció de problemes; en aquest cas, dues implicacions.

Mètode 2: **Pel contrarecíproc**. També es pot demostrar l'enunciat original pel contrarecíproc: $A \to D \equiv \neg D \to \neg A$.

Exemple 6.66 Seguint amb l'exemple 1 inicial, el contrarecíproc seria

$\neg(x = 0 \wedge y = 0) \Rightarrow x^2 + y^2 \neq 0.$

Observem que, per De Morgan, la negació de $x = 0 \wedge y = 0$ equival a $x \neq 0 \vee y \neq 0$.

Vegem que, a partir de $x \neq 0 \vee y \neq 0$, obtenim $x^2 + y^2 \neq 0$. Fem servir que, per a tot nombre real t, és $t^2 \geq 0$. I que tenim $(t \neq 0 \wedge t^2 \geq 0) \Rightarrow t^2 > 0$.

En efecte, $(x \neq 0 \vee y \neq 0) \Rightarrow (x^2 > 0 \vee y^2 > 0) \Rightarrow x^2 + y^2 > 0 \Rightarrow x^2 + y^2 \neq 0$. ■

Mètode 3: **Per reducció a l'absurd**

La negació de la implicació $A \to (B \wedge C)$ és (lògicament equivalent a) $A \wedge \neg(B \wedge C)$. Per l'equivalència de De Morgan, la fórmula anterior equival lògicament a $A \wedge (\neg B \vee \neg C)$.

Exemple 6.67 Seguint amb l'exemple 1, en el nostre exemple seria $x^2 + y^2 = 0 \wedge (x^2 \neq 0 \vee y^2 \neq 0)$. Per la distributivitat de $\wedge$ respecte de $\vee$, la fórmula proposicional equival a $(A \wedge \neg B) \vee (A \wedge \neg C)$, que es concreta per a uns determinats x, y en $[x^2 + y^2 = 0 \wedge x^2 \neq 0] \vee [x^2 + y^2 = 0 \wedge y^2 \neq 0]$.

Vegem que arribem a contradicció.

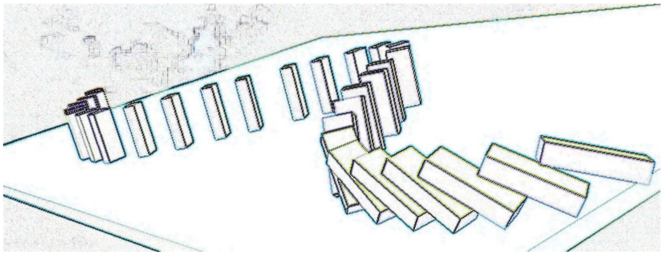
De $x^2 + y^2 = 0 \wedge x^2 \neq 0$, se'n deriva una contradicció. En efecte, de $y^2 \geq 0$ i de $x^2 \neq 0$ $(x^2 > 0)$, se'n deriva $x^2 + y^2 > 0$, d'on $x^2 + y^2 \neq 0$, contradicció.

Anàlogament al cas anterior, a partir de $x^2 + y^2 = 0 \wedge y^2 \neq 0$ també s'arriba a una contradicció. Realment, hauríem de quantificar i negar la fórmula quantificada. ■

Observació. Amb l'exemple 2, fent servir el mètode 1 hauríem de demostrar $(xy \neq 0 \to x \neq 0) \wedge (xy \neq 0 \to y \neq 0)$.

→ 7

Inducció



Un mètode de demostració important és el **mètode d'inducció**. N'hi ha diverses variants possibles. Veurem:

- el mètode d'inducció simple o ordinària o feble (que anomenarem simplement inducció) i
- la inducció completa (o forta).

Dediquem aquest capítol a la inducció simple.

Es podria presentar el mètode de demostració per inducció a partir del principi d'inducció per als naturals, partint de propietats dels nombres naturals, però aquí preferirem una aproximació totalment pràctica, sense massa teoricismes, que en tot cas deixem per a un altre tipus de text. Tampoc no tractarem altres tipus d'inducció o de mètode inductiu, com l'"estructural", que en últim terme es pot reduir a l'ordinària.

7.1. El mètode

7.1.1. Algunes fórmules útils

Recordem algunes fórmules que poden ser útils a algunes demostracions per inducció, depenent de la tipologia del problema.

1. En problemes que s'han de resoldre per inducció amb fórmules que contenen sumatoris, sol ser útil tenir en compte que:

$$\sum_{i=1}^{n+1} a_i = (\sum_{i=1}^{n} a_i) + a_{n+1}, \qquad \sum_{i=1}^{n} a_i = (\sum_{i=1}^{n-1} a_i) + a_n$$

Així, per exemple:

$$\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1),\ n \in \mathbb{N},\ n \geq 1$$
$$\sum_{i=1}^{n} i = (\sum_{i=1}^{n-1} i) + n,\ n \in \mathbb{N},\ n \geq 2$$

O, desplegat:

$$1+2+\cdots+(n+1) = (1+2+\cdots+n)+(n+1),$$
$$1+2+\cdots+n = (1+2+\cdots+(n-1))+n$$

2. Recordem que $0! = 1$ i que, per a $n \geq 1$, $n! = 1 \cdot 2 \cdot 3 \cdots (n-2)(n-1)n$. Solen ser útils, per a problemes amb factorials, les fórmules recurrents:

$$n! = n \cdot (n-1)! = (n-1)!n,$$
$$(n+1)! = (n+1) \cdot n! = n!(n+1),$$
$$n! = n(n-1) \cdot (n-2)! = (n-2)!n(n-1),$$

que permeten fer el pas necessari en el pas inductiu.

3. La fórmula recurrent per als nombres binomials o combinatoris

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r} \ (n, r \text{ naturals}, n \geq r \geq 1)$$

pot ser útil per a demostracions per inducció.

4. Recordem també el concepte de divisibilitat per a enters: a és divisor de b (o bé b és múltiple d'a) si, i només si, existeix un nombre enter k tal que $b = ka$. Expressat d'una altra manera, $a|b \Leftrightarrow \exists k(k \in \mathbb{Z} \wedge b = ka)$. També resulta útil saber $(a|b \wedge a|c) \Rightarrow a|xb + yc$, per a a, b, x, y enters. En particular, $(a|b \wedge a|c) \Rightarrow a|b \pm c$.

Si calen resultats addicionals sobre sumatoris i sumes especials, vegeu el capítol 3. També els capítols inicials de preliminars aporten dades útils en aquest sentit.

7.1.2. Esquema d'una demostració per inducció

Encara que aquest capítol es dedica específicament a la inducció, hi ha moltes demostracions per inducció disperses en diversos capítols, segons convingui o sigui escaient. En aquest capítol, només es pretén presentar el mètode i d'il·lustrar-lo amb uns quants exemples, però no acumular aquí totes les demostracions per inducció.

Descripció del mètode. Suposem formulada una propietat $P(n)$ en termes del nombre natural n, per a n a partir d'un cert nombre natural n_0 en endavant, és a dir, $n \geq n_0 \geq 0$; el valor n_0 és el valor inicial.

Més formalment:

Propietat que es vol demostrar: $P(n)$, per a tot $n \geq n_0$.
Valor inicial: n_0.

En el mètode de demostració per inducció, hem de provar que, per a n_0, n nombres naturals, és cert el següent:

$P(n_0) \wedge \forall n(n \geq n_0 \rightarrow (P(n) \rightarrow P(n+1)))$

Aleshores, queda demostrat que $P(n)$ és cert per a tot $n \geq n_0$.

De fet, la fórmula següent expressa la situació completa, suposant n, n_0 naturals:

$(P(n_0) \wedge \forall n(n \geq n_0 \rightarrow (P(n) \rightarrow P(n+1))) \rightarrow \forall n(n \geq n_0 \rightarrow P(n))$

La variable n pot ser substituïda per qualsevol altra i així podem escriure:

$P(n_0) \wedge \forall k(k \geq n_0 \rightarrow (P(k) \rightarrow P(k+1)))$

Quin és l'esquema demostratiu, el patró de demostració? Com es fa una demostració per inducció? És l'esquema següent, que concorda amb la fórmula de predicats anterior.

ESQUEMA DEMOSTRATIU

• **PAS BÀSIC**. En aquest pas, es demostra que la propietat és certa per a n_0 (el nombre natural més petit per al qual s'afirma la veracitat de l'afirmació o la fórmula). És a dir, cal provar que:
$P(n_0)$ és cert.

Comentari: sol ser un pas senzill, tot i que no sempre.

• **PAS INDUCTIU**. En aquest pas, es demostra la implicació

$P(n) \Rightarrow P(n+1)$, per a tot $n \geq n_0$.

Comentaris i reformulacions. Verbalment, atès que és un condicional, és:

"si $P(n)$ és cert, aleshores $P(n+1)$ és cert".

La suposició, en el context d'aquest condicional, que "$P(n)$ és cert" s'anomena clàssicament "hipòtesi d'inducció" (HI).

Aplicant $P(n)$ (cert), demostrarem $P(n+1)$; és a dir, aplicant la HI, demostrarem que $P(n+1)$ és cert.

Suposant la propietat certa per a n, provarem que també és certa per a $n+1$.

Aquestes implicacions es demostren en genèric, per a tot $n \geq n_0$, de manera que resulten demostrades per a tot $n \geq n_0$.

Noteu que $P(n+1)$ és el que resulta de substituir n per $n+1$.

Sintetitzant i en resum:

PAS BÀSIC. Provar que $P(n_0)$ és cert.

PAS INDUCTIU. Provar que $P(n) \Rightarrow P(n+1)$ és cert per a tot $n \geq n_0$.

Exemple 7.1 Vegem com es concretaria l'esquema anterior per a l'exemple següent (sense resoldre):

"$1+2+\cdots+k+\cdots+n \overset{P(n)}{=} \frac{n(n+1)}{2}$, per a tot nombre natural $n \geq 1$."

Esquema demostratiu (resum): Només diem què s'ha de fer, sense resoldre el problema:

PAS BÀSIC. Cal provar que $P(1)$ és cert, és a dir, que $1+2+\cdots+k+\cdots+n = \frac{n(n+1)}{2}$ és cert per a $n=1$.

PAS INDUCTIU. Cal provar que $P(n) \Rightarrow P(n+1)$ per a tot $n \geq 1$ (n nombre natural). Això es concreta a provar:

$1+2+\cdots+k+\cdots+n \overset{(\mathrm{HI})}{=} \frac{n(n+1)}{2} \Rightarrow 1+2+\cdots+k+\cdots+n+(n+1) = \frac{(n+1)((n+1)+1)}{2}$, és a dir,

$1+2+\cdots+k+\cdots+n \overset{(\mathrm{HI})}{=} \frac{n(n+1)}{2} \Rightarrow 1+2+\cdots+k+\cdots+n+(n+1) = \frac{(n+1)(n+2)}{2}$. O bé, en termes de sumatoris:

$$\sum_{k=1}^{n} k \overset{(\mathrm{HI})}{=} \frac{n(n+1)}{2} \Rightarrow \sum_{k=1}^{n+1} k = \frac{(n+1)((n+1)+1)}{2}, \text{ és a dir,}$$

$$\sum_{k=1}^{n} k \overset{(\mathrm{HI})}{=} \frac{n(n+1)}{2} \Rightarrow \sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}. \blacksquare$$

Es resol el problema com a tal a continuació, amb tot detall.

7.1.3. El primer exemple de demostració per inducció

A continuació es resol el problema anterior, amb tot detall. Com és tradició, és el primer exemple d'inducció que se sol presentar.

PROBLEMA 7.1

La suma dels n primers nombres naturals. *Demostreu per inducció que*

$1+2+\cdots+k+\cdots+n = \frac{n(n+1)}{2}$, *per a tot nombre natural* $n \geq 1$.

Solució. La propietat que es vol demostrar demostrar és, en termes de sumatoris,

$$P(n): \sum_{i=1}^{n} i = \frac{n(n+1)}{2}, \text{ per a qualsevol nombre natural } n \geq 1.$$

En aquest cas, $n_0 = 1$.

Demostrem la propietat $P(n)$ per inducció sobre n, amb valor inicial $n_0 = 1$. Sempre és el mateix esquema. L'esquema demostratiu consta de dos passos: el pas bàsic i el pas inductiu.

Pas bàsic: ($n_0 = 1$). Cal provar que la propietat és certa per a $n_0 = 1$, és a dir, que $P(1)$ és cert. Atès que es tracta d'una igualtat, hem de veure que el membre de la dreta ($D(n)$) i el de l'esquerra ($E(n)$) coincideixen per a $n = 1$, és a dir, $E(1) = D(1)$. Ara bé, això és només una comprovació de rutina:

$$E(1) = \sum_{j=1}^{1} j = 1$$

$$D(1) = \frac{1(1+1)}{2} = 1$$

Per tant, coincideixen i queda demostrat el pas bàsic.

Pas inductiu: ($P(k) \to P(k+1), \forall k(k \in \mathbb{N} \wedge k \geq 1)$). El pas inductiu consisteix a fixar $k \geq n_0$ arbitrari i a demostrar la implicació:

$P(k) \Rightarrow P(k+1)$, per a tot $k \geq n_0$ (natural), és a dir, en aquest cas,

$P(k) \Rightarrow P(k+1)$, per a tot $k \geq 1$. Concretant al nostre problema:

$$\sum_{i=1}^{k} i \overset{(HI)}{=} \frac{k(k+1)}{2} \Rightarrow \sum_{i=1}^{k+1} i = \frac{(k+1)((k+1)+1)}{2}, \text{ és a dir,}$$

$$\sum_{i=1}^{k} i \overset{(HI)}{=} \frac{k(k+1)}{2} \Rightarrow \sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}.$$

La igualtat HI és la hipòtesi (d'inducció).

Estratègia demostrativa. Com aplicar la hipòtesi d'inducció? Aquest sol ser l'aspecte més difícil en aquest tipus de demostracions.

Idea clau. Una idea possible és partir d'una part de $P(n)$, el membre de l'esquerra de la igualtat en aquest exemple, efectuar manipulacions algebraiques fins a fer aparèixer una subfórmula que sigui la que figura a la HI, per tal de poder fer la substitució oportuna (en aquest cas, ja que no sempre es tracta d'una substitució), en aplicació de la HI.

En efecte, reescrivim:

$$\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k+1)$$

Ara podem aplicar HI i substituir a la fórmula anterior $\sum_{i=1}^{k} i$ per $\frac{k(k+1)}{2}$, i així resulta

$\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k+1) = \frac{k(k+1)}{2} + (k+1)$. Ara, amb càlculs rutinaris, es demostrarà finalment $\frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$.

Resumint:

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) \overset{HI}{=} \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Observació. Hem presentat la resolució del pas inductiu en termes de la variable k. L'elecció de la variable "de treball", k en aquest cas, és irrelevant. S'hauria pogut plantejar el pas inductiu en termes de demostrar, per exemple, $P(n) \Rightarrow P(n+1)$ o $P(m) \Rightarrow P(m+1)$.

Observació: exposició alternativa. On i com aplicar la HI? En aquest exemple, la HI no s'ha aplicat a l'inici de la demostració, sinó en un pas més avançat de l'argumentació. Se'n pot presentar una variant argumental de manera que el punt de partida del raonament sigui la HI (però no sempre serà possible, depenent de la tipologia de l'enunciat). Vegem-ho:

$$\sum_{i=1}^{k} i \overset{(HI)}{=} \frac{k(k+1)}{2}$$

$\Downarrow$ (sumant $k+1$ a ambdós membres de la igualtat)

$$\sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$\Downarrow$ per propietats del sumatori: associativitat de la suma

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + (k+1)$$

$\Downarrow$

$$\sum_{i=1}^{k+1} i = \frac{k(k+1) + 2(k+1)}{2}$$

$\Downarrow$ es treu factor comú, per distributivitat del producte respecte de la suma

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

Una altra formulació (“$P(n-1) \Rightarrow P(n)''$).

Es pot reformular el principi d’inducció, amb una variant que consisteix a “passar de $n-1$ a n”, en comptes de “de n a $n+1$”. És totalment equivalent. Es formularia com

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

$P(n_0) \wedge \forall k(k > n_0 \rightarrow (P(k-1) \rightarrow P(k)))$

Esquema demostratiu per al pas inductiu: $P(k-1) \Rightarrow P(k)$, per a qualsevol $k \geq n_0 + 1$, que aplicarem al problema anterior per tal de proporcionar una variant argumental:

PROBLEMA 7.2

La suma dels n primers nombres naturals. *Demostreu per inducció que*

$1+2+\cdots+k+\cdots+n = \frac{n(n+1)}{2}$*, per a tot nombre natural* $n \geq 1$*,*

aplicant l’esquema demostratiu per al pas inductiu: $P(k-1) \Rightarrow P(k)$*, per a qualsevol* $k \geq 2$.

Solució. Aquest problema ja s’ha resolt amb detall a l’exercici anterior. Només es tracta de presentar-ne una variant en la resolució del pas inductiu. Per completesa, repetirem alguns apartats.

La propietat que es vol demostrar és, en termes de sumatoris, $P(n) : \displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, per a qualsevol nombre natural $n \geq 1$. En aquest cas, $n_0 = 1$.

Pas bàsic: ($n_0 = 1$, $P(n_0)$ és cert). Cal provar que la propietat és certa per a $n_0 = 1$, és a dir, que $P(1)$ és cert. Atès que es tracta d’una igualtat, hem de veure que el membre de la dreta ($D(n)$) i el de l’esquerra ($E(n)$) coincideixen per a $n = 1$, és a dir, $E(1) = D(1)$. Ara bé, això és només una comprovació:

$$E(1) = \sum_{j=1}^{1} j = 1$$

$$D(1) = \frac{1(1+1)}{2} = 1$$

Per tant, coincideixen i queda demostrat el pas bàsic.

Pas inductiu: ($P(k-1) \rightarrow P(k)$, $\forall k(k \in \mathbb{N} \wedge k \geq 2)$). El pas inductiu consisteix a fixar $k \geq n_0 + 1$ arbitrari i a demostrar la implicació:

$P(k-1) \Rightarrow P(k)$, per a tot $k \geq n_0 + 1$ (natural), és a dir,

$P(k-1) \Rightarrow P(k)$, per a tot $k \geq 2$. Concretant al nostre problema:

$$\sum_{i=1}^{k-1} i \stackrel{(HI)}{=} \frac{(k-1)k}{2} \Rightarrow \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

Com aplicar la hipòtesi d'inducció? Aquest sol ser l'aspecte més difícil.

Idea guia. Una idea és partir d'una part de $P(k)$, el membre de l'esquerra de la igualtat en aquest exemple i efectuar manipulacions algebraiques fins a fer aparèixer una subfórmula que sigui la que figura a la HI, per tal de poder fer l'oportuna substitució (en aquest cas), en aplicació de la HI.

$$\sum_{i=1}^{k} i = (\sum_{i=1}^{k-1} i) + k$$

Ara podem aplicar HI i substituir a la fórmula anterior $\sum_{i=1}^{k-1} i$ per $\frac{(k-1)k}{2}$, i així resulta:

$\sum_{i=1}^{k} i = (\sum_{i=1}^{k-1} i) + k = \frac{(k-1)k}{2} + k$. Ara, amb càlculs rutinaris, es demostrarà finalment:

$$\frac{(k-1)k)}{2} + k = \frac{(k-1)k)}{2} + \frac{2k}{2} = \frac{(k-1)k+2k}{2} = \frac{k(k-1+2)}{2} = \frac{k(k+1)}{2}.$$

Resumint:

$$\sum_{i=1}^{k} i = (\sum_{i=1}^{k-1} i) + k \stackrel{HI}{=} \frac{(k-1)k}{2} + k = \frac{k(k+1)}{2}.$$

Això completa la demostració del pas inductiu i també completa la demostració per inducció.

7.1.4. Redacció de la resolució

Resumim quina ha de ser la guia de la redacció d'una demostració per inducció. Els dos primers apartats que figuren a continuació corresponen a una primera etapa de preparació. Els dos següents constitueixen la demostració pròpiament dita. L'últim apartat serveix per donar per acabada la prova i la seva exposició, i explica el que s'ha aconseguit.

a) Identifiqueu clarament la propietat $P(n)$ que es vol demostrar i identifiqueu quin és el valor inicial n_0 a l'enunciat, i assegureu-vos que previsiblement serà demostrable en principi per inducció. Formuleu $P(n)$ si no està explícitament enunciat. Indiqueu l'expressió completa de la propietat amb quantificació universal.

b) Escriviu que es procedeix a demostrar la propietat $P(n)$ per inducció. Indiqueu la modalitat d'inducció, respecte de quin paràmetre i quin és el seu valor mínim (a l'enunciat).

c) Demostreu el “pas bàsic”:

- Escriviu l’enunciat $P(n_0)$, indicant que s’ha de veure que és cert.
- Demostreu $P(n_0)$, és a dir, que $P(n_0)$ és cert.

d) Demostreu el “pas inductiu”:

- Fixeu $k \geq n_0$ arbitrari.
- Escriviu que aneu a demostrar $P(k) \Rightarrow P(k+1)$, $\forall k \geq n_0$.
- Concreteu, particularitzeu, a l’enunciat del problema el pas inductiu $P(k) \Rightarrow P(k+1)$, és a dir, per a la propietat P concreta del problema.
- Indiqueu quina és la HI (hipòtesi d’inducció), és a dir, la suposició que $P(k)$ és cert en el marc del condicional.
- Feu la demostració de la implicació $P(k) \Rightarrow P(k+1)$, és a dir: suposant $P(k)$ cert, proveu que se’n dedueix que $P(k+1)$ és cert. Exposeu amb claredat el fil argumental. No escriviu com a demostrat allò que s’ha de demostrar.
- En el curs de l’apartat anterior, indiqueu on i com apliqueu la HI, és a dir, la suposició que $P(k)$ és cert.
- Indiqueu clarament el final de la demostració del pas inductiu i de la demostració.

e) És recomanable escriure la conclusió de tot l’anterior.

7.1.5. Quines propietats es poden intentar demostrar per inducció?

Quines propietats són susceptibles de ser demostrades per inducció? Dit d’una altra manera, quina tipologia de propietats podem intentar demostrar per inducció? I quines no?

Les propietats que ens podem plantejar de demostrar per inducció són les que es formulen en termes d’un nombre natural n, $P(n)$ en genèric, a partir d’un cert lloc en endavant, és a dir, per a tot $n \geq n_0$, amb $n_0 \in \mathbb{N}$.

Molts enunciats no compleixen aquesta condició i no s’hi pot aplicar el mètode. Per exemple, al teorema de Pitàgores tenim que, si a, b, c són les longituds dels costats d’un triangle rectangle (catets) i c és la longitud de la hipotenusa, aleshores $a^2 + b^2 = c^2$. Observeu que a, b, c són nombres reals; no és un enunciat en termes de nombres naturals. Per tant, no té sentit plantejar el mètode d’inducció per a demostrar el teorema.

En general, l’enunciat que es vol demostrar es formula amb afirmacions del tipus que segueix:

Sigui $n_0 \in \mathbb{N}$. Per a tot nombre natural $n \geq n_0$, $P(n)$, o bé

Sigui $n_0 \in \mathbb{N}$. Per a tot nombre natural $n \geq n_0$, $P(n)$ és cert, o bé

$P(n)$ és cert per a tot nombre natural $n \geq n_0$, on $n_0 \in \mathbb{N}$, o bé

$P(n), \forall n \geq n_0$ (sobreentenent el domini $\mathbb{N}$), o bé

$\forall n \geq n_0 \; P(n)$, o bé

$\forall n((n \in \mathbb{N} \wedge n \geq n_0) \rightarrow P(n))$.

Observeu que totes les afirmacions anteriors volen dir el mateix: "per a tot $n \geq 0$", " per a cada $n \geq 0$", "per a qualsevol $n \geq 0$".

Exemple 7.2 Suposem que hem de demostrar $1+2+\cdots+k+\cdots+n = \dfrac{n(n+1)}{2}$, per a tot nombre natural $n \geq 1$. En termes de sumatoris, $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Amb el formalisme anterior, la propietat que es vol demostrar és

$P(n)$: "$1+2+\cdots+k+\cdots+n = \frac{n(n+1)}{2}$", per a tot $n \geq 1$. Formalment, l'enunciat complet és

$$\forall n((n \in \mathbb{N} \wedge n \geq 1) \rightarrow \sum_{k=1}^{n} k = \frac{n(n+1)}{2}).$$

En aquest exemple, $n_0 = 1$.

Es faria una demostració de $P(n)$ per inducció respecte de n. ■

"Sobre n". Quan es fa una demostració per inducció, es diu que es fa una demostració per inducció respecte de n o "sobre n" (per exemple). Hem de triar respecte de quin paràmetre (nombre natural) es farà la demostració per inducció, en aquest cas n. És convenient indicar-ho, ja que pot passar en alguna ocasió que hi hagi més d'un paràmetre possible respecte del qual es pugui fer la demostració per inducció. Per exemple, en un graf tenim diverses possibilitats: pot ser respecte del nombre de vèrtexs, d'arestes, de components connexos, de cares (si és planari) o altres.

En alguns enunciats on apareguin diverses variables, hem de distingir les variables respecte de les quals es pot demostrar per inducció, de les variables auxiliars d'una fórmula, com pot ser una variable que sigui índex d'iteració o sumació. Per exemple, si considerem l'afirmació

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2},$$

la variable k és només auxiliar i l'afirmació no "diu" res sobre k. L'enunciat és sobre n, sobre la qual "es diu" la igualtat anterior. Per tant, si es vol demostrar per inducció, ha de ser respecte de n, és a dir "sobre n". No podem fer inducció sobre la variable k de la fórmula.

Se suposa que n creix d'un en un, de manera ascendent. Si no és així a l'enunciat, aleshores potser no serà adequat per a aplicar el mètode o s'haurà de fer algun tipus de manipulació o argumentació per a reduir-lo al cas estàndard.

Altres exemples en què és possible aplicar el mètode de demostració per inducció són:

$1^2+2^2+3^2+\cdots+k^2+\cdots+n^2=\dfrac{n(n+1)(2n+1)}{6}$, $\forall n\geq 1$ (igualtats),

$2^n>n$, $\forall n\geq 0$ (desigualtats),

$2n^2-2n-1\geq 0$, $\forall n\geq 0$ (desigualtats),

$n!>n$, per a tot $n\geq 3$,
$79|80^n-1$. per a tot $n\geq 0$ (divisibilitat).

Pot passar que un enunciat estigui formulat en termes dels nombres naturals, però això no vol dir que forçosament s'hagi de poder demostrar per inducció.

Observació. Que un problema es pugui resoldre per inducció no significa que no es pugui resoldre per un mètode diferent. Dependrà de cada cas. En alguns exemples que es veuen en aquest capítol, són possibles demostracions no inductives, i també al capítol dedicat a sumatoris. És també un exercici recomanable que el lector s'ho plantegi a cada problema que es demostri per inducció.

Mostrem un exemple formulat en termes de nombres naturals, en què és possible una demostració no inductiva (en aquest cas, per casos). Més endavant en aquest capítol, es demostra per inducció:

PROBLEMA 7.3

Demostreu que $n^2-2n-1\geq 0$ *per a tot nombre natural* $n\geq 3$ sense utilitzar inducció.

Solució

Mètode 1. Vegem-ho ***per casos*** segons la paritat de n.

Cas 1. Sigui n parell. Aleshores existeix k enter tal que $n=2k$. Essent $n\geq 3$ i parell, és $n\geq 4$ i, per tant, $k\geq 2$. Aleshores $n^2-2n-1=(2k)^2-2(2k)-1=((2k-1)^2-1)-1=(2k-1)^2-2\overset{k\geq 2}{\geq}(2\cdot 2-1)^2-2=7>0$.

Cas 2. Sigui n senar. Aleshores existeix k enter tal que $n=2k+1$. Essent $n\geq 3$, és $2k+1=n\geq 3$, d'on $2k\geq 2$, d'on $k\geq 1$. Aleshores $n^2-2n-1=(2k+1)^2-2(2k+1)-1=4k^2-2=2(2k^2-1)>0$, ja que $k\geq 1$.

Mètode 2. Alternativament, es pot resoldre el problema estudiant la funció

$f:\mathbb{R}\to\mathbb{R}$, donada per $f(x)=x^2-2x-1$ i veient que $f(x)\geq 0$ per a tot $x\geq 3$. La gràfica de la funció és una paràbola d'eix paral·lel a l'eix Oy, oberta cap al semiplà de les y positives i amb interseccions amb l'eix Ox en els punts d'abscisses les solucions de $x^2-2x-1=0$, és a dir, $x_1=1-\sqrt{2}$, $x_2=1+\sqrt{2}$. Per a $x>x_2$, és $f(x)>0$. Si $n\geq 3$, $n>x_1$ i, per tant, $f(n)>0$. És a dir, $n^2-2n-1>0$.

No tota propietat que es formuli en termes d'un nombre natural s'ha de poder demostrar per inducció. La següent n'és un exemple, juntament amb moltes altres de tipus similar.

Propietat: “Per a tot nombre natural, $\text{mcd}(2n+3, 4n+5) = 1$”.

Si intentem resoldre el problema per inducció sobre n, tindrem dificultats per relacionar $P(n)$ amb $P(n+1)$ i, per tant, per a aplicar la hipòtesi d'inducció, malgrat que sigui una propietat que es formula en termes del nombre natural n. En aquest cas, és preferible optar per resoldre el problema per algun altre mètode, no inductiu.

Tampoc no són (directament) propietats que es formulen en termes d'un nombre enter, tot i que potser es pugui reduir al cas dels naturals. La propietat del problema anterior també és certa per a nombres enters, però, per a la demostració d'aquest fet, no podem fer servir directament el mètode d'inducció (tot i que se'n podria intentar alguna adaptació).

7.2. Diverses tipologies a través dels exemples

Vegem diverses tipologies de demostracions per inducció, a través d'exemples. No es tracta d'una autèntica classificació, sinó només d'una exposició de casos freqüents. Potser el tipus més difícil és el dels enunciats de propietats amb desigualtats.

7.2.1. Enunciats amb igualtats, sumatoris

Cal dir que molts dels exercicis d'inducció amb igualtats estan al capítol de sumatoris (cap. 3).

El primer exemple que hem resolt correspon a aquesta tipologia. Vegem-ne alguns més:

PROBLEMA 7.4

La suma dels n primers nombres naturals parells no nuls. *Sigui n un nombre natural qualsevol, amb $n \geq 1$. Proveu per inducció*

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

Solució. Denotem per $P(n)$ la propietat anterior, és a dir, $\sum_{k=1}^{n} 2k \overset{P(n)}{=} n(n+1)$, per a tot $n \geq 1$. La demostració per inducció sobre n segueix el patró usual de les demostracions per inducció; el valor inicial és $n_0 = 1$.

Pas bàsic. És el pas en què es demostra que la propietat $P(n)$ és certa per a $n_0 = 1$. Que $P(1)$ és cert és una comprovació: $\sum_{k=1}^{n} 2k \overset{?}{=} n(n+1)$ per a $n = 1$, és a dir, $\sum_{k=1}^{1} 2k \overset{?}{=} 1(1+1)$. El valor del membre de l'esquerra és $E = 2 \cdot 1 = 2$; el de la dreta, $D = 2$. Atès que hi ha coincidència, queda demostrat i superat el pas bàsic.

Pas inductiu. Hem de veure que $P(n) \Rightarrow P(n+1)$, per a tot $n \geq 1$, que es concreta en

$$\sum_{k=1}^{n} 2k \overset{\textbf{(HI)}}{=} n(n+1) \Rightarrow \sum_{k=1}^{n+1} 2k = (n+1)((n+1)+1), \text{ per a tot } n \geq 1, \text{ és a dir,}$$

$$\sum_{k=1}^{n} 2k \overset{\textbf{(HI)}}{=} n(n+1) \Rightarrow \sum_{k=1}^{n+1} 2k = (n+1)(n+2), \text{ per a tot } n \geq 1.$$

Idea de la demostració del pas inductiu. Partirem de $\sum_{k=1}^{n+1} 2k$. Manipularem algebraicament la fórmula per fer-hi aparèixer com a subfórmula $\sum_{k=1}^{n} 2k$, que substituirem per $n(n+1)$ en aplicació de la HI. La resta és rutina fins a aconseguir $\sum_{k=1}^{n+1} 2k = (n+1)(n+2)$.

En efecte:

$$\sum_{k=1}^{n+1} 2k = \Big(\sum_{k=1}^{n} 2k\Big) + 2(n+1) \overset{\text{(HI)}}{=} n(n+1) + 2(n+1) = (n+1)(n+2).$$

Certament, també es pot començar per $n = 0$, ja que la suma no varia:

$$0 + 2 + 4 + \cdots + 2k + \cdots + 2n = 2 + 4 + \cdots + 2k + \cdots + 2n.$$

Observació. En capítols anteriors (preliminars, per exemple), s'han fet demostracions diverses d'aquest resultat sense utilitzar el mètode d'inducció.

PROBLEMA 7.5

La suma dels n+1 primers nombres naturals senars. *Sigui n un nombre natural qualsevol. Proveu per inducció la propietat $P(n)$ donada per*

$$1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2.$$

Solució. Demostrarem la igualtat per inducció sobre n, amb el valor inicial $n_0 = 0$. Observem que, en termes de sumatoris, la propietat es pot escriure com:

$$\sum_{k=0}^{n} (2k+1) = (n+1)^2$$

Segons l'esquema demostratiu habitual, cal demostrar els dos passos següents:

Pas bàsic. Provem que $P(n_0)$ (és a dir, $P(0)$) és cert. Comprovem que

$\sum_{k=0}^{0}(2k+1)=(0+1)^2$. En efecte, a l'esquerra és $\sum_{k=0}^{0}(2k+1)=2\cdot 0+1=1$; a la dreta, és $(0+1)^2=1^2=1$. Hi ha coincidència.

Pas inductiu. Cal provar $P(n)\Rightarrow P(n+1)$, per a tot $n\geq 0$. És a dir:

$\sum_{k=0}^{n}(2k+1)=(n+1)^2\Rightarrow\sum_{k=0}^{n+1}(2k+1)=((n+1)+1)^2$, o sigui:

$\sum_{k=0}^{n}(2k+1)=(n+1)^2\Rightarrow\sum_{k=0}^{n+1}(2k+1)=(n+2)^2$, o sigui:

$1+3+5+\cdots+(2n+1)=(n+1)^2\Rightarrow 1+3+5+\cdots+(2(n+1)+1)=(n+2)^2$, o sigui

$1+3+5+\cdots+(2n+1)=(n+1)^2\Rightarrow 1+3+5+\cdots+(2n+3)=(n+2)^2$.

La hipòtesi d'inducció (HI) és la suposició que $\sum_{k=0}^{n}(2k+1)=(n+1)^2$ és cert (en el marc del condicional).

Com aplicar la hipòtesi d'inducció? La idea és efectuar manipulacions algebraiques sobre $\sum_{k=0}^{n+1}(2k+1)$ per tal de fer-hi aparèixer una subfórmula que sigui igual a la fórmula que apareix a la HI, en aquest cas $\sum_{k=0}^{n}(2k+1)$, per tal de poder substituir, aplicant la hipòtesi d'inducció. En efecte:

$\sum_{k=0}^{n+1}(2k+1)=(\sum_{k=0}^{n}(2k+1))+(2(n+1)+1)\overset{(\text{HI})}{=}(n+1)^2+(2(n+1)+1)=(n^2+2n+1)+(2n+3)=n^2+4n+4=(n+2)^2$.

Amb això hem demostrat la fórmula per inducció.

Observeu que hem aplicat la HI en un lloc intermedi de l'argumentació. També es pot reformular la demostració de manera que el punt de partida sigui la HI:

$\sum_{k=0}^{n}(2k+1)\overset{(\text{HI})}{=}(n+1)^2\Rightarrow(\sum_{k=0}^{n}(2k+1))+(2(n+1)+1)=(n+1)^2+(2(n+1)+1)\Rightarrow$
$\sum_{k=0}^{n+1}(2k+1)=n^2+4n+4\Rightarrow\sum_{k=0}^{n+1}(2k+1)=(n+2)^2$.

Observeu que, amb aquesta fórmula, tenim també altres fórmules derivades, com per exemple:

$1+3+5+\cdots+(2n-1)=1+3+5+\cdots+(2(n-1)+1)=((n-1)+1)^2=n^2$, que és la suma dels n primers nombres naturals senars.

Observació. En capítols anteriors (sobre preliminars i sumatoris, per exemple), s'han fet demostracions diverses d'aquest resultat sense utilitzar el mètode d'inducció.

PROBLEMA 7.6

Sigui a un nombre real, $a \neq 1$. Demostreu per inducció que, per a tot n natural ($n \geq 0$), es compleix:

$$1+a+a^2+a^3+\cdots+a^k+\cdots+a^n=\frac{1-a^{n+1}}{1-a}$$

Solució. Observeu que la propietat es pot reescriure com:

$$a^0+a^1+a^2+a^3+\cdots+a^k+\cdots+a^n=\frac{1-a^{n+1}}{1-a}$$

i també en termes de sumatoris:

$$\sum_{k=0}^{n} a^k=\frac{1-a^{n+1}}{1-a}$$

La demostració per inducció sobre n consta de dues parts. Denotem per $P(n)$ la propietat, és a dir, la igualtat anterior, per a tot $n \geq 0$. El valor inicial és $n_0=0$.

Pas bàsic. Consisteix a demostrar que la propietat $P(n)$ és certa per a $n=0$, és a dir, que $P(0)$ és cert. En aquest cas, és només una comprovació. En efecte, el membre de l'esquerra E de la igualtat val, per a aquest valor de n, $E=1^0=1$. El membre D de la dreta val $D=\frac{1-a^{0+1}}{1-a}=\frac{1-a}{1-a}=1$. És $D=E$. Per tant, queda demostrada la igualtat per a $n=0$.

Pas inductiu. Hem de demostrar que $P(n) \Rightarrow P(n+1)$, per a tot $n \geq 0$. Concretant, hem de demostrar que, per a tot $n \geq 0$, es compleix:

$$1+a^2+\cdots+a^n \stackrel{(HI)}{=} \frac{1-a^{n+1}}{1-a} \Rightarrow 1+a^2+\cdots+a^n+a^{n+1}=\frac{1-a^{(n+1)+1}}{1-a},$$

és a dir,

$$1+a^2+\cdots+a^n \stackrel{(HI)}{=} \frac{1-a^{n+1}}{1-a} \Rightarrow 1+a^2+\cdots+a^n+a^{n+1}=\frac{1-a^{n+2}}{1-a}.$$

El problema és *com apliquem la hipòtesi d'inducció (HI)*: es tracta de fer aparèixer a $1+a^2+\cdots+a^n+a^{n+1}$ (o a un desenvolupament d'aquesta fórmula) una *subfórmula* que coincideixi exactament amb la que tenim a la hipòtesi d'inducció, per tal de poder aplicar-la, substituint en aquest cas. En efecte, per associativitat de la suma:

$$1+a^2+\cdots+a^n+a^{n+1}=(1+a^2+\cdots+a^n)+a^{n+1}\overset{(HI)}{=}\tfrac{1-a^{n+1}}{1-a}+a^{n+1}.$$

La resta és rutina:

$$1+a^2+\cdots+a^n+a^{n+1}=\tfrac{1-a^{n+1}}{1-a}+a^{n+1}=\tfrac{1-a^{n+1}+(1-a)a^{n+1}}{1-a}=\tfrac{1-a^{n+1}+a^{n+1}-a\cdot a^{n+1}}{1-a}=\tfrac{1-a^{n+2}}{1-a}.$$

Això conclou el pas inductiu i la demostració.

7.2.2. Enunciats amb desigualtats

Exemple 7.3 Vegem un exemple on es demostra una desigualtat per inducció. La propietat que es vol demostrar, per a tot nombre natural $n \geq 1$, és $n < 2^n$. El problema se sol presentar en la demostració del pas inductiu, en què no sempre és clar què cal fer, en aquest tipus de problemes amb desigualtats.

Demostrem la propietat per inducció sobre n, amb valor inicial $n_0 = 1$. Si denotem per $P(n)$ la propietat que volem demostrar, cal provar:

$P(n_0)$, és a dir, $P(1)$ (pas base)

$P(n) \Rightarrow P(n+1)$, $\forall n \geq 1$ (pas inductiu).

Aquest esquema es concreta en el següent:

Pas base. Vegem la propietat per al valor inicial $n = 1$. Només cal provar $1 < 2^1$, que es compleix trivialment.

Pas inductiu. Hem de veure $n \overset{(HI)}{<} 2^n \Rightarrow n+1 < 2^{n+1}$, per a tot $n \geq 1$.

En efecte:

$$2^{n+1} = 2^n \cdot 2 = 2 \cdot 2^n \overset{(HI)}{>} 2n = n+n \geq n+1, \text{ ja que } n \geq 1.$$

O bé es pot argumentar segons la variant:

$$n < 2^n \Rightarrow 2n < 2 \cdot 2^n \Rightarrow 1+n \leq n+n < 2^{n+1} \blacksquare$$

PROBLEMA 7.7

Proveu per inducció $5^n > 5^{n-1}$, *per a tot nombre natural* $n \geq 1$.

Solució

Observació. Se'n poden aportar demostracions directes senzilles, no inductives.

Mètode 1. Tenim les equivalències següents ($n \geq 1$):

$5^n > 5^{n-1} \Leftrightarrow 5^n - 5^{n-1} > 0 \Leftrightarrow 5^{n-1}(5-1) > 0 \Leftrightarrow 5^{n-1} \cdot 4 > 0$. L'última afirmació és òbvia; per tant, resulta demostrada la primera, per transitivitat.

Mètode 2. Essent $5^{n-1} > 0$, tenim les equivalències següents ($n \geq 1$):

$5^n > 5^{n-1} \Leftrightarrow \frac{5^n}{5^{n-1}} > 1 \Leftrightarrow 5^{n-(n-1)} > 1 \Leftrightarrow 5^1 > 1 \Leftrightarrow 5 > 1$. L'última afirmació és certa; per consegüent, queda demostrada la primera, ateses les equivalències, per transitivitat.

Demostració per inducció. Encara que se'n pugui fer una demostració directa senzilla, com ja s'ha vist anteriorment, demostrem la propietat per inducció, atès que és un capítol d'exposició del mètode demostratiu.

Fem una demostració per inducció sobre n, amb $n_0 = 1$. Denotem per $P(n)$ la propietat "$5^n > 5^{n-1}$"

Pas bàsic. Vegem que $P(1)$ és cert. Això es concreta a provar $5^1 > 5^{1-1}$, és a dir, $5 > 1$, que és cert.

Pas inductiu. Fixem k natural, $k \geq 1$, arbitrari (però fix per a aquesta demostració; k no varia). Cal provar $P(k) \Rightarrow P(k+1)$. Equivalentment, i concretant,

$5^k > 5^{k-1} \Rightarrow 5^{k+1} > 5^{(k+1)-1}$ (és a dir, $5^k > 5^{k-1} \Rightarrow 5^{k+1} > 5^k$)

"Si $5^k > 5^{k-1}$, aleshores $5^{k+1} > 5^k$".

HI (*hipòtesi d'inducció*): se suposa cert $5^k > 5^{k-1}$ (al condicional anterior).

Cal veure que és cert $5^{k+1} > 5^k$ com a conseqüència de HI.

Essent $5 > 0$, multiplicar els dos membres d'una desigualtat per 5 en conserva l'orientació de la desigualtat; ho apliquem a la desigualtat $5^k > 5^{k-1}$, de manera que:

$$5^k \overset{HI}{>} 5^{k-1} \Rightarrow 5 \cdot 5^k > 5 \cdot 5^{k-1} \Rightarrow 5^{k+1} > 5^{(k-1)+1} \Rightarrow 5^{k+1} > 5^k.$$

Queda demostrat el pas inductiu i això conclou la demostració per inducció.

Observació. Es pot fer una presentació diferent del pas inductiu, partint de 5^{k+1}, que manipularem per a donar entrada a la HI, fent que hi aparegui com a subfórmula "5^k", que apareix a la HI:

$$5^{k+1} = 5^k \cdot 5 \overset{HI}{>} 5^{k-1} \cdot 5 = 5^{(k-1)+1} = 5^k.$$

PROBLEMA 7.8

Demostreu que $3^n > n$ per a tot nombre natural $n \geq 1$.

Solució. Relació que es vol demostrar: $P(n) : 3^n > n$. Realment, és la desigualtat: $3^n \overset{P(n)}{>} n$.

Propietat que es vol demostrar: $\forall n((n \in \mathbb{N} \wedge n \geq 1) \rightarrow 3^n > n)$.

Mètode: per inducció sobre n (inducció simple).

$n_0 = 1$.

Pas bàsic ($P(1)$). Vegem que $P(1)$ és cert. Quina és l'afirmació $P(1)$? És $3^1 > 1$. Només cal comprovar que $3^1 > 1$, que es compleix trivialment, ja que $3 = 3^1 > 1$.

Pas inductiu ($P(n) \Rightarrow P(n+1), \forall n \geq 1$).

Cal demostrar que, per a tot $n \geq 1$, es compleix $P(n) \Rightarrow P(n+1)$, que es concreta en:

$3^n \overset{(HI)}{>} n \Rightarrow 3^{n+1} > (n+1)$.

És a dir, fixant $n \geq 1$ i suposant que $3^n > n$ és cert, ara provarem que és certa la desigualtat del mateix tipus o patró però amb n substituït per $n+1$.

Guia de resolució: Prenent l'expressió "3^{n+1}", s'efectuaran les manipulacions que convinguin per tal de fer-hi aparèixer la fórmula "3^n", com a subfórmula, i així poder aplicar la hipòtesi d'inducció (HI).

En efecte:

$3^{n+1} = 3 \cdot 3^n \overset{HI}{>} 3n$ ($3^n > n \Rightarrow 3 \cdot 3^n > 3n$, ja que multipliquem per $3 > 0$ i, per tant, es conserva l'orientació o el sentit de la desigualtat).

Si fos $3n \overset{(*)}{>} (n+1)$, el problema estaria resolt, per transitivitat, ja que aleshores tindríem $3^{n+1} > 3n > n+1$, d'on $3^{n+1} > n+1$.

Vegem si aconseguim demostrar-ho (no en tenim cap garantia a priori; en que cas que no sigui així, hauríem de buscar una altra via de resolució). Vegem-ne diferents variants argumentals.

Variant argumental 1. Escrivim $3n = n + 2n$. Atès que $n \geq 1$, és $2n \geq 2 > 1$. Per tant, $3n > n + 2n > n + 1$.

Variant argumental 2. Serà $3n > (n+1)$, si, i només si,

$3n - (n+1) > 0$, és a dir, si i només si,

$2n - 1 > 0$, que és cert si

$n \geq 1$, que és cert.

Observeu que es podria refer l'última argumentació i es podria presentar així (n'hi hauria prou amb només implicacions $\Rightarrow$):

$n \geq 1 \Rightarrow 2n - 1 > 0 \Leftrightarrow 3n - (n+1) > 0 \Leftrightarrow 3n > (n+1)$.

Variant argumental 3. També es podria argumentar així: $3n = n + (n+n) \overset{n \geq 1}{\geq} 1 + (n+n) \overset{n \geq 1}{\geq} 1 + (1+n) > 1 + n$.

Observació. La propietat també és certa per a $n = 0$, com es pot comprovar trivialment, de forma directa i separada de la inducció. Només cal comprovar que $3^0 > 0$, que es compleix, ja que $1 = 3^0 > 0$. Ara bé, la demostració per inducció la fem en el cas $n \geq 1$: això és degut que el pas que ens convé (*) no és cert per a $n = 0$ (no representa cap problema, ja que només és una fita superior). Finalment, amb els dos procediments, aquesta observació i la demostració per inducció, la propietat es pot enunciar per a tot $n \geq 0$.

Observació: Seria un exercici similar demostrar $2^n > n$, $4^n > n$, per exemple.

PROBLEMA 7.9

Demostreu que $3^n > n^2$ *per a tot nombre natural* $n \geq 2$.

Solució

$P(n) := 3^n > n^2$

$\forall n (n \in \mathbb{Z} \wedge n \geq 2) \rightarrow 3^n > n^2$

Mètode de demostració: per inducció simple respecte de n.

$n_0 = 2$.

Pas bàsic. Provem la propietat $P(n)$ per a $n = 2$, és a dir, $3^2 > 2^2$, que és trivialment cert.

Pas inductiu. Hem de demostrar que, per a tot $n \geq 2$, es compleix:

$3^n > n^2 \Rightarrow 3^{n+1} > (n+1)^2$. Per a això, fixem $n \geq 2$ i demostrem la implicació, és a dir, $P(n) \Rightarrow P(n+1), \forall n \geq 2$. En altres paraules, vegem que, si $3^n > n^2$, aleshores $3^{n+1} > (n+1)^2$.

HI (hipòtesi d'inducció): és la hipòtesi de la implicació, la suposició que $3^n > n^2$ és cert.

Tesi d'inducció: $3^{n+1} > (n+1)^2$.

Volem demostrar (aplicant HI): $3^{n+1} > (n+1)^2$.

Com a conseqüència de la HI, podem escriure: $3^{n+1} = 3 \cdot 3^n \overset{HI}{>} 3n^2$. És a dir, $3^n \overset{HI}{>} n^2 \overset{3>0}{\Rightarrow} 3 \cdot 3^n < 3n^2$.

Aconseguiríem demostrar el que volem si fos $3n^2 \geq (n+1)^2$ (que no sabem si és cert), ja que aleshores $3^{n+1} > 3n^2 > (n+1)^2$.

Ara bé, seria $3n^2 \geq (n+1)^2$, si, i només si,

$3n^2 \geq n^2 + 2n + 1$, i això si, i només si,

$2n^2 - 2n - 1 \geq 0$.

Observi el lector que, "sobre la marxa" no tenim cap garantia que això sigui cert; podria no ser-ho. Ens aniria bé si ho fos. Ens plantegem estudiar si és certa aquesta última propietat, amb la qual cosa ens veiem obligats a resoldre un *problema auxiliar* en el curs de la demostració del pas inductiu (a l'interior de la demostració del pas inductiu).

Resolució del problema auxiliar (fem un incís en l'argumentació general).

Mètode 1. Als problemes 38 i 3 d'aquest mateix capítol, es demostra un resultat per a $n \geq 3$, $n^2 - 2n - 1 \geq 0$, que podem utilitzar per a resoldre el nostre problema, ja que $2n^2 - 2n - 1 = n^2 + (n^2 - 2n - 1) \geq n^2 > 0$, que es pot estendre per comprovació directa a $n = 2$.

Mètode 2. També se'n pot fer una demostració directa. Escrivim $n^2 - 2n - 1 = 2n(n - 1) - 1$. De $n \geq 2$, resulta $n - 1 \geq 1$. Per tant, $2n(n-1) \geq 2 \cdot 2 \cdot 1 = 4$. Per tant, $n^2 - 2n - 1 = 2n(n-1) - 1 \geq 4 - 1 = 3 \geq 0$.

Mètode 3 (inducció dins de la inducció). Vegem una demostració de $2n^2 - 2n - 1 \geq 0$, per a $n \geq 2$ per inducció (inducció dins del pas inductiu per tal de demostrar un resultat auxiliar); de fet es demostra la desigualtat estricta:

Pas bàsic (propietat auxiliar): $2n^2 - 2n - 1 \geq 0$ per a $n = 2$, que es comprova rutinàriament substituint n per 2 (noteu que no es compleix per a $n = 0, 1$).

Pas inductiu (propietat auxiliar): per a tot $n \geq 2$, demostrem que $2n^2 - 2n - 1 \geq 0 \Rightarrow 2(n+1)^2 - 2(n+1) - 1 \geq 0$. En efecte, desenvolupem $2(n+1)^2 - 2(n+1) - 1$ de manera que aparegui $2n^2 - 2n - 1$ com a part de la fórmula i es pugui afirmar $2n^2 - 2n - 1 \geq 0$, en aplicació de la hipòtesi d'inducció: $2(n+1)^2 - 2(n+1) - 1 = 2(n^2 + 2n + 1) - 2n - 2 - 1 = (2n^2 - 2n - 1) + 4n \geq 0 + 4n > 0$.

Mètode 4. Estudiant la funció, en especial la gràfica, $f(x) = 2x^2 - 2x - 1$, per a $x \geq 2$. Cal veure $f(x) \geq 0$ per a $x \geq 2$.

Reprenem ara el fil argumental principal:

Ha resultat ser cert. Aleshores, per transitivitat, de $3^{n+1} = 3 \cdot 3^n > 3n^2 > (n+1)^2$ resulta $3^{n+1} > (n+1)^2$, que és el que volíem veure.

En un pas de la demostració, s'ha fet servir que $n \geq 2$, però es pot fer una comprovació directa de la propietat $3^n > n^2$ per als casos $n = 0, 1$, i així estenem el resultat a tot $n \geq 0$.

PROBLEMA 7.10

Proveu per inducció que $2n \leq 2^n$ per a tot nombre natural $n \geq 1$.

Solució. Demostrarem la propietat per inducció, amb valor inicial $n_0 = 1$.

Pas bàsic. Cal provar la propietat per a $n = n_0 = 1$, és a dir, que $2 \times 1 \leq 2^1$, que és obvi.

Pas inductiu. Cal provar la implicació

$2n \leq 2^n \Rightarrow 2(n+1) \leq 2^{n+1}$, per a tot $n \geq n_0 = 1$.

La hipòtesi (HI, hipòtesi d'inducció) és $2n \overset{(HI)}{\leq} 2^n$.

Observant la desigualtat de la tesi, es pot reescriure com $2n+2 \leq 2^{n+1}$. Justament l'expressió $2n$ de l'esquerra apareix a la hipòtesi, i aquest detall ens permetrà connectar la hipòtesi amb la tesi:

$$2n \overset{HI}{\leq} 2^n \Rightarrow 2n+2 \leq 2^n+2 \Rightarrow 2n+2 \leq 2^n+2 \overset{n\geq 1}{\leq} 2^n+2^n = 2\cdot 2^n = 2^{n+1}.$$

Per tant, $2n \overset{HI}{\leq} 2^n \Rightarrow 2n+2 \leq 2^{n+1}$.

Queda demostrada la propietat per inducció.

PROBLEMA 7.11

Proveu per inducció que $3n \leq 2^n$ *per a tot nombre natural* $n \geq 4$.

Solució. Demostrarem la propietat per inducció, amb valor inicial $n_0 = 4$.

Pas bàsic. Cal provar la propietat per a $n = n_0 = 4$, és a dir, que $3\cdot 4 \leq 2^4$, que és cert.

Pas inductiu. Cal provar la implicació $3n \leq 2^n \Rightarrow 3(n+1) \leq 2^{n+1}$, per a tot $n \geq n_0 = 4$. La hipòtesi d'inducció (HI) és $3n \leq 2^n$, per a $n \geq 4$.

Tenim $3(n+1) = 3n+3 \overset{(HI)}{\leq} 2^n+3$.

Essent $n \geq 4$, és $3 \leq 2^n$ (de fet, ja és cert per a $n = 2$). En efecte, essent la funció exponencial creixent, $4 \leq n \Rightarrow 2^4 \leq 2^n$, d'on $3 \leq 2^4 \leq 2^n$.

Per tant, $3(n+1) = 3n+3 \overset{(HI)}{\leq} 2^n+3 < 2^n+2^n = 2\cdot 2^n = 2^{n+1}$.

Queda demostrada la propietat per inducció.

PROBLEMA 7.12

Proveu per inducció que $1+2n \leq 3^n$ *per a tot nombre natural* $n \geq 1$.

Solució. Demostrarem la propietat per inducció, amb valor inicial $n_0 = 1$.

Pas bàsic. Cal provar la propietat per a $n = n_0 = 1$, és a dir, que $1+2\cdot 0 \leq 3^0$, que és cert.

Pas inductiu. Cal provar la implicació:

$$1+2n \overset{(HI)}{\leq} 3^n \Rightarrow 1+2(n+1) \leq 3^{n+1}, \text{ per a tot } n \geq n_0 = 1.$$

Considerem el terme de l'esquerra de la tesi: $1+2(n+1) = (1+2n)+2$, reescrit de manera que hi aparegui el membre de l'esquerra de la hipòtesi (HI). Amb aquesta reescriptura, podem aplicar la hipòtesi:

$1+2(n+1)=(1+2n)+2\overset{(HI)}{\leq} 3^n+2\leq 3^n+3\leq 3^n+3^n\leq 3^n+3^n+3^n=3\cdot 3^n=3^{n+1}$, com volíem veure. Així queda demostrada la implicació del pas inductiu.

Queda demostrada la propietat per inducció.

PROBLEMA 7.13

Proveu per inducció que $n^2<2^{2n}$ per a tot nombre natural $n\geq 2$.

Altres resultats similars: $2^{2n}>n$, $2^{3n}>n^2$, $3^{3n}>n^2$, $3^{2n}>n^2$, $3^{2n}>n$, $2^{2n}>n^3$, $2^{3n}>n^3$.

Solució. Demostrem la propietat per inducció sobre n, amb valor inicial $n_0=2$.

Pas base. Es demostra la propietat per al valor inicial $n_0=2$. Cal comprovar $2^2<2^{2\cdot 2}$, és a dir, $4<2^4$, que és cert.

Pas inductiu. Provem que, per a $n\geq 2$, es compleix:

$$n^2\overset{(HI)}{<}2^{2n}\Rightarrow (n+1)^2<2^{2(n+1)}.$$

En efecte:

$$2^{2(n+1)}=2^{2n+2}=2^2\cdot 2^{2n}=4\cdot 2^{2n}\overset{(HI)}{>}4n^2.$$

Si fos $4n^2>(n+1)^2$, hauríem resolt el problema. Però això equival a $4n^2>n^2+2n+1$, que equival a $3n^2>2n+1$. Ara bé, $3n^2=2n^2+n^2$. És $2n^2>2n$, $n^2>1$. Per tant, queda demostrat $3n^2>2n+1$, i el problema queda resolt.

Així doncs, queda provat el pas inductiu, i conclou la demostració per inducció.

PROBLEMA 7.14

Sigui $a\in\mathbb{R}$ i $a\geq -1$. Proveu que $(1+a)^n\geq 1+na$ per a tot nombre natural n.

Solució. Demostrarem el resultat per inducció sobre n, amb valor inicial $n_0=0$. Denotem per $P(n)$ la propietat que volem demostrar, és a dir, $P(n)$:"$(1+a)^n\geq 1+na$", per a tot $n\geq 0$ (fixat a).

Pas bàsic ($P(n_0)$ és cert). Vegem que $P(0)$ és cert. En aquest cas, es concreta a comprovar que $(1+a)^0\geq 1+0\cdot a$, que és trivialment cert.

Pas inductiu ($P(n)\Rightarrow P(n+1)$, per a tot $n\geq 0$). La implicació que es vol demostrar es concreta a:

$$(1+a)^n\overset{HI}{\geq}1+na\Rightarrow (1+a)^{n+1}\geq 1+(n+1)a, \text{ per a tot } n\geq 0.$$

La propietat $a\geq -1$ equival a $a+1\geq 0$, de manera que podem multiplicar els dos membres d'una desigualtat per $a+1$ i l'orientació de la desigualtat es manté. Així, a partir de la HI, que és $(1+a)^n\geq 1+na$, multipliquem membre a membre la desigualtat anterior ($(1+a)^n\geq 1+na$) per $1+a$ i n'obtenim

$(1+a)^n(1+a) \geq (1+na)(1+a)$, és a dir, $(1+a)^{n+1} \geq (1+na)(1+a)$.

Ara, si fos $(1+na)(1+a) \geq 1+(n+1)a$, quedaria resolt el nostre problema, ja que tindríem $(1+a)^{n+1} \geq (1+na)(1+a) \geq 1+(n+1)a$, d'on $(1+a)^{n+1} \geq 1+(n+1)a$ (per transitivitat). I és fàcil veure que és així: podem veure, equivalentment, que $(1+na)(1+a)-(1+(n+1)a) \geq 0$. Ara bé, per un càlcul rutinari,

$(1+na)(1+a)-(1+(n+1)a) = na^2 \geq 0$, no negatiu com a producte de dos no negatius. El problema està resolt.

Variant argumental. També es pot procedir segons una altra variant:

$(1+na)(1+a) = 1+a+na+na^2 = (1+(n+1)a)+na^2 \geq 1+(n+1)a$, ja que $na^2 \geq 0$.

Variant argumental. Fins ara s'ha partit de la HI. Es pot procedir d'una altra manera, prenent com a punt de partida l'expressió $(1+a)^{n+1}$ de $P(n+1)$, fórmula que manipularem fins a fer-hi aparèixer alguna subfórmula que ens permeti aplicar la HI. En efecte:

$(1+a)^{n+1} = (1+a)^n(1+a) \overset{HI}{\geq} (1+na)(1+a)$, ja que $1+a \geq 0$ (aquí apliquem que $((\alpha \geq \beta) \wedge \gamma \geq 0) \Rightarrow \alpha\gamma \geq \beta\gamma$). Ara, $(1+a)^{n+1} \geq (1+na)(1+a) = (1+na)+(1+na)a = 1+na+a+na^2 = (1+(n+1)a)+na^2 \geq 1+(n+1)a$, ja que $na^2 \geq 0$.

7.2.3. Enunciats amb propietats de divisibilitat

PROBLEMA 7.15

Demostreu que, per a tot nombre natural n, es compleix: $2|n^2+n$. *És a dir,* $\forall n(2|n^2+n)$, *suposant n nombre natural.*

Solució Cal provar $\forall n(2|n^2+n)$, amb $n \in \mathbb{N}$, $n \geq 0$. És a dir, $\forall n\ P(n)$, amb $P(n) := (2|n^2+n)$.

Fem la demostració per inducció sobre n, amb $n_0 = 0$.

Pas bàsic (Provem que $P(0)$ és cert). És a dir, cal veure que $2|0^2+0$, que és trivial.

Pas inductiu (Demostrem que $P(n) \Rightarrow P(n+1)$ per a tot nombre natural).

Cal provar $2|n^2+n \Rightarrow 2|(n+1)^2+(n+1)$ per a tot n natural.

Equivalentment, hem de veure: si existeix $t \in \mathbb{N}$ tal que $n^2+n = 2t$, aleshores existeix $t' \in \mathbb{N}$ tal que $(n+1)^2+(n+1) = 2t'$, és a dir:

$\exists t(n^2+n = 2t) \Rightarrow \exists t'((n+1)^2+(n+1) = 2t')$ (amb t, t' nombres naturals)

Guia de resolució: Efectuem càlculs amb el membre de l'esquerra, $(n+1)^2+(n+1)$, amb l'objectiu de fer aparèixer n^2+n com a subfórmula i així poder-hi aplicar la hipòtesi d'inducció. En efecte:

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

$=2t+(2n+2)$, per la hipòtesi d'inducció,

$=2t+2(n+1)=2(t+n+1)$.

Prenent $t'=t+n+1 \in \mathbb{N}$, es conclou que existeix un nombre natural t' tal que $(n+1)^2+(n+1)=2t'$, com s'havia de veure.

Observacions:

1. El resultat és vàlid per a tot enter (per exemple, demostrable per casos segons paritat de n).

   Si admetem que, de cada dos enters consecutius, exactament un és parell (i, per tant, l'altre senar), aleshores resulta de $n^2+n=n(n+1)$.

   També es pot fer servir el que s'ha provat per a nombres naturals per a estendre el resultat a nombres enters negatius. Sigui $m<0$. Sigui $m'=-m>0$. Ara es pot aplicar el resultat a m': $m'(m'+1)$ és parell. Ara bé, $m'(m'+1)=-m(-m+1)=m(-(-m+1))=m(m-1)$, que resulta ser parell.

2. Un resultat similar és vàlid per a $n^2-n=n(n-1)$, on un dels dos factors és parell. També es podria demostrar per inducció de manera similar.

PROBLEMA 7.16

Proveu per inducció que el producte de tres nombres naturals consecutius és múltiple de 3. És a dir, $3|n(n+1)(n+2)$ *per a tot n natural.*

Observació*: Són variants equivalents* $3|(n-2)(n-1)n$ *(per a* $n\geq 2$*) i* $3|(n-1)n(n+1)$ *(per a* $n\geq 1$*).*

Observació*: El resultat és generalitzable a tot enter (demostrable per casos, per exemple).*

Solució Hem de demostrar $\forall n(3|n(n+1)(n+2))$, on n és un nombre natural. Es fa la demostració per inducció sobre n, amb $n_0=0$, ja que l'enunciat és per a tots els nombres naturals. Aquí, $P(n)$ és $3|n(n+1)(n+2)$.

Pas bàsic. ($P(0)$ és cert?). Vegem que $P(n)$ és cert per a n_0, és a dir, per a $n=0$. Però això es redueix a comprovar que $3|0(0+1)(0+2)$, que és una obvietat, ja que $3|0$.

Pas inductiu ($\forall n\geq 0\ (P(n)\Rightarrow P(n+1))$).

Comentaris i preparatius per a la demostració. L'afirmació $P(n+1)$ s'obté a partir de $P(n)$ substituint n per $n+1$ a l'afirmació. Així:

$P(n):\ 3|n(n+1)(n+2)$

$P(n+1):\ 3|(n+1)((n+1)+1)((n+1)+2)$.

Vegem que, per a tot $n \geq 0$, es compleix:

$3|n(n+1)(n+2) \Rightarrow 3|(n+1)((n+1)+1)((n+1)+2)$, és a dir,

$3|n(n+1)(n+2) \Rightarrow 3|(n+1)(n+2)(n+3)$

$\overbrace{3 \mid n(n+1)(n+2)}^{P(n)} \Rightarrow \overbrace{3 \mid (n+1)(n+2)(n+3)}^{P(n+1)}$.

Observeu que l'afirmació de l'esquerra de la implicació és la hipòtesi d'inducció (HI).

$\overbrace{3 \mid n(n+1)(n+2)}^{(HI)} \Rightarrow 3|(n+1)(n+2)(n+3)$.

Una opció possible seria desenvolupar els productes, desfent la factorització. Preferim no seguir per aquesta via i a aquest efecte, fem alguna manipulació algebraica de $(n+1)(n+2)(n+3)$ per tal d'utilitzar la HI. Observeu que els factors $(n+1)(n+2)$ apareixen a ambdues fórmules, i això és el que *guia* la resolució.

La hipòtesi d'inducció equival a $\exists k(k \in \mathbb{Z} \wedge n(n+1)(n+2) = 3k)$ (de fet, k és natural, en aquest cas). Hem de veure $\exists k'(k' \in \mathbb{Z} \wedge (n+1)(n+2)(n+3) = 3k')$. És a dir:

$\exists k(k \in \mathbb{Z} \wedge n(n+1)(n+2) = 3k) \Rightarrow \exists k'(k' \in \mathbb{Z} \wedge (n+1)(n+2)(n+3) = 3k')$.

Demostració del pas inductiu. Expressem $(n+1)(n+2)(n+3)$ de manera que hi aparegui $n(n+1)(n+2)$ i s'hi pugui aplicar la HI.

Aleshores, escrivim:

$(n+1)(n+2)(n+3) = (n+1)(n+2)n + (n+1)(n+2) \cdot 3 = n(n+1)(n+2) + 3(n+1)(n+2) \stackrel{(HI)}{=} 3k + 3(n+1)(n+2)$ per a algun enter k.

De fet, seria més exacte dir $\exists k(k \in \mathbb{Z} \wedge (n+1)(n+2)(n+3) = 3k + 3(n+1)(n+2))$.

O millor:

$\exists k(k \in \mathbb{Z} \wedge n(n+1)(n+2) = 3k) \Rightarrow \exists k(k \in \mathbb{Z} \wedge (n+1)(n+2)(n+3) = 3k + 3(n+1)(n+2))$.

Ara bé, $(n+1)(n+2)(n+3) = 3k + 3(n+1)(n+2) = 3(k + (n+1)(n+2))$, i prenent $k' = k + (n+1)(n+2)$, resulta $(n+1)(n+2)(n+3) = 3k'$, amb la qual cosa hem acabat la demostració.

PROBLEMA 7.17

Proveu per inducció que, per a tot nombre natural n, l'expressió

$n^3 + 3n^2 + 2n$ *és múltiple de 3.*

Observació*: el resultat ja s'ha provat d'una altra forma, desenvolupant* $n(n+1)(n+2)$*; és* $n(n+1)(n+2) = n^3 + 3n^2 + 2n$.

Observació*: el resultat és generalitzable a tot enter (demostració per casos, per exemple).*

Solució. Denotem $P(n):\ 3|n^3+3n^2+2n$.

Fem la demostració per inducció (simple) sobre n, amb $n_0=0$.

Pas bàsic. Cal demostrar que $P(0)$ és cert, és a dir, $3|n^3+3n^2+2n$ per a $n=0$, és a dir, que $3|0^3+3\cdot 0^2+2\cdot 0$, que és cert. En efecte, $3|0$, ja que $0=0\cdot 3$.

Pas inductiu. Cal provar que, per a tot nombre natural ($n\geq 0$), se satisfà:

$P(n)\Rightarrow P(n+1)$, que es concreta, per a aquest enunciat, en:

$3|n^3+3n^2+2n \Rightarrow 3|(n+1)^3+3(n+1)^2+2(n+1)$

La HI (hipòtesi d'inducció) és $3|n^3+3n^2+2n$, que equival a dir que existeix algun enter k tal que $n^3+3n^2+2n=3k$.

Guia de resolució. Efectuem manipulacions algebraiques a la fórmula

$(n+1)^3+3(n+1)^2+2(n+1)$

per tal de fer-hi aparèixer com a subfórmula o subexpressió justament la que figura a la HI (hipòtesi d'inducció), és a dir, n^3+3n^2+2n, i així poder aplicar-hi la hipòtesi (HI).

De fet, hem de veure que, si $n^3+3n^2+2n=3k$ per a algun enter k convenient (en aquest cas, natural), aleshores $(n+1)^3+3(n+1)^2+2(n+1)=3k'$ per a un cert k' enter adequat.

Calculem i agrupem convenientment, per associativitat i commutativitat de la suma:

$$
\begin{aligned}
&(n+1)^3+3(n+1)^2+2(n+1)\\
&=(n^3+3n^2+3n+1)+3(n+1)^2+(2n+2)\\
&=(n^3+3n^2+2n)+3n+3(n+1)^2+(1+2)\\
&=(n^3+3n^2+2n)+3(n+(n+1)^2+1)\\
&\overset{HI}{=}3k+3(n+(n+1)^2+1)=3(k+n+(n+1)^2+1).
\end{aligned}
$$

Amb $k'=k+n+(n+1)^2+1$ és $(n+1)^3+3(n+1)^2+2(n+1)=3k'$, com s'havia de veure, i això conclou la demostració.

PROBLEMA 7.18

Proveu per inducció que, per a tot nombre natural n, l'expressió n^3-n és múltiple de 3.

Formuleu una variant de la demostració per a provar $6|n^3-n$.

Observació: *El resultat és generalitzable a tot enter.*

Solució Demostració per inducció simple sobre n, amb $n_0 = 0$.

Pas bàsic. Cal demostrar que la propietat és certa per a $n_0 = 0$, és a dir, que $3|0^3 - 0$, és a dir, que $3|0$, que és obvi.

Pas inductiu. Suposant cert $3|n^3 - n$ (HI, hipòtesi d'inducció), vegem que també és cert $3|(n+1)^3 - (n+1)$.

Per a això, fem manipulacions algebraiques amb $(n+1)^3 - (n+1)$, amb l'objectiu de fer-hi aparèixer la fórmula $n^3 - n$ i així poder aplicar la hipòtesi d'inducció. En efecte, $(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = (n^3 - n) + 3n^2 + 3n$. És $n^3 - n = 3k$ per a algun enter k, en aplicació de HI. Per tant, $(n+1)^3 - (n+1) = (n^3 - n) + 3n^2 + 3n = 3k + 3(n^2 + n) = 3(k + n^2 + n)$ per a un k enter convenient. així doncs, existeix un enter $k' = k + n^2 + n$ tal que $(n+1)^3 - (n+1) = 3k'$, és a dir, $3|(n+1)^3 - (n+1)$, com s'havia de veure.

Amb una modificació de les argumentacions, podem demostrar $6|n^3 - n$. En efecte:

Pas bàsic. Cal demostrar que la propietat és certa per a $n_0 = 0$, és a dir, que $6|0^3 - 0$, és a dir, que $6|0$, que és evident.

Pas inductiu. Suposant cert $6|n^3 - n$ (HI, hipòtesi d'inducció), vegem que també és cert $6|(n+1)^3 - (n+1)$.

Per a això, fem manipulacions algebraiques amb $(n+1)^3 - (n+1)$, amb l'objectiu de fer-hi aparèixer la fórmula $n^3 - n$ i així poder aplicar la hipòtesi d'inducció. En efecte, $(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = (n^3 - n) + 3n^2 + 3n$. És $n^3 - n = 6k$ per a algun enter k, en aplicació de HI. Per tant, $(n+1)^3 - (n+1) = (n^3 - n) + 3n^2 + 3n = 6k + 3(n^2 + n)$ per a un k enter convenient. La idea és que cal un factor 2 a $3(n^2 + n)$. Escrivim $n^2 + n = n(n+1)$, parell, perquè és producte de dos enters consecutius (un dels dos és parell). Per tant, $n^2 + n = 2\alpha$, per a un enter α, i així $(n+1)^3 - (n+1) = 6k + 3 \cdot 2\alpha = 6k + 6\alpha = 6(k + \alpha)$.

Per tant, existeix un enter $k' = k + \alpha$ tal que $(n+1)^3 - (n+1) = 6k'$, és a dir, $6|(n+1)^3 - (n+1)$, com s'havia de veure.

Observació. Es pot demostrar $3|n^3 - n$ directament, sense inducció:

Factoritzem: $n^3 - n = n(n^2 - 1) = n(n^2 - 1^2) = n(n+1)(n-1) = (n-1)n(n+1)$.

Per resultats coneguts i, en tot cas, demostrats en altres llocs del llibre, per a cada tres enters consecutius n'hi ha exactament un que és múltiple de 3; per tant, un dels factors de l'expressió anterior és múltiple de 3 i, en conseqüència, $(n-1)n(n+1)$ és múltiple de 3; aquí només cal que n'hi hagi almenys un que sigui múltiple de 3.

També es pot demostrar per casos segons els valors possibles del residu de la divisió entera de n per 3.

Aquestes demostracions directes farien innecessària la demostració inductiva, però això aquí és irrellevant, ja que es tracta d'adquirir tècnica demostrativa.

Observació. Resultat addicional independent: també es pot demostrar que l'expressió és múltiple de 2 (per inducció, per casos segons paritat de n o per la factorització anterior, en què apareixen dos enters consecutius $n(n+1)$ a $n^3-n=n(n^2-1)=n(n^2-1^2)=n(n+1)(n-1)=(n-1)n(n+1)$).

Observació. També es pot demostrar que n^3-n és múltiple de 6 (per inducció, com hem vist; descomponent el problema en dos problemes (ser múltiple de 2 i ser múltiple de 3 separadament)).

PROBLEMA 7.19

Demostreu per inducció $6|7^n+5$ *per a tot nombre natural* $n\geq 0$.

Solució. Demostració per inducció sobre n amb valor inicial $n_0=0$.

Pas base. Provem la propietat per al valor inicial, és a dir, que $6|7^n+5$ per a $n=n_0=0$. Concretant, vegem que és cert $6|7^0+5$. Ara bé, $7^0+5=1+5=6$. Per tant, la propietat és certa per al valor inicial.

Pas inductiu. Vegem que, per a tot $n\geq 0$, es compleix $6|7^n+5 \Rightarrow 6|7^{n+1}+5$. La hipòtesi d'inducció (HI) és, doncs, suposar cert $6|7^n+5$.

Podem escriure, intentant que aparegui 7^n+5, amb l'objectiu de poder-hi aplicar la HI:

$7^{n+1}+5=7^n\cdot 7+5=7^n(6+1)+5=7^n\cdot 6+7^n+5=6\cdot 7^n+(7^n+5)$.

Aleshores, amb la suposició anterior (HI), podem escriure l'argumentació següent.

El primer sumand $6\cdot 7^n$ és múltiple de 6. El segon sumand 7^n+5 és també múltiple de 6 en aplicació de la hipòtesi d'inducció (HI), és a dir, $7^n+5=6k$ per a algun enter k. Així, $7^{n+1}+5=6(7^n+k)=6k'$, múltiple de 6, amb $k'=7^n+k\in\mathbb{Z}$.

Això conclou la demostració.

Vegem una altra presentació de l'argumentació en el pas inductiu. Per la HI, existeix un enter k tal que $7^n+5=6k$. Aleshores podem escriure $7^n=6k-5$. Apliquem aquesta expressió:

$7^{n+1}+5=7\cdot 7^n+5\overset{HI}{=}7\cdot(6k-5)+5=7\cdot 6k-7\cdot 5+5=7\cdot(6k-5)30=6(7k-5)=6k'$, amb $k'=7k-5$, enter. Per tant, $6|7^{n+1}+5$ i queda demostrada la implicació $6|7^n+5\Rightarrow 6|7^{n+1}+5$ del pas inductiu.

PROBLEMA 7.20

Proveu per inducció que, per a tot nombre natural $n\geq 0$*, es compleix:* $3|5\cdot 2^{4n}+1$.

Solució. Demostració per inducció sobre n amb valor inicial $n_0=0$.

Pas base. Cal veure que la propietat és certa per al valor inicial n_0, és a dir, que $3|5\cdot 2^{4n}+1$ per a $n=n_0=0$. Es concreta en $3|5\cdot|2^{4\times 0}+1=5\cdot 1+1=6$, que és obvi.

Pas inductiu. Cal provar que $3|5\cdot 2^{4n}+1 \Rightarrow 3|5\cdot 2^{4(n+1)}+1$, per a tot $n\geq 0$.

Hipòtesi d'inducció (HI): suposar cert $3|5\cdot 2^{4n}+1$.

Això significa que existeix un enter k tal que $5\cdot 2^{4n}+1=3k$. Es pot reescriure com $5\cdot 2^{4n}=3k-1$.

Intentem expressar $5\cdot 2^{4(n+1)}+1$ en termes de $5\cdot 2^{4n}$ per tal de poder-hi aplicar la hipòtesi d'inducció:

$5\cdot 2^{4(n+1)}+1=5\cdot 2^{4n+4}+1=5\cdot 2^4\cdot 2^{4n}+1=5\cdot 16\cdot 2^{4n}+1\stackrel{HI}{=}16(3k-1)+1=16\cdot 3k-16+1=16\cdot 3k-15=3(16k+5)$, múltiple de 3.

Això conclou la demostració per inducció.

Observació. També es pot seguir una altra variant argumental:

$5\cdot 2^{4(n+1)}+1=5\cdot 2^{4n+4}+1=5\cdot 2^4\cdot 2^{4n}+1=5\cdot 16\cdot 2^{4n}+1=5\cdot 2^{4n}(15+1)+1=5\cdot 2^{4n}\cdot 15+(5\cdot 2^{4n}+1)=3\cdot 25\cdot 2^{4n}+(5\cdot 2^{4n}+1)\stackrel{HI}{=}3\cdot 25\cdot 2^{4n}+3k=3(25\cdot 2^{4n}+k)$, múltiple de 3.

PROBLEMA 7.21

Estudieu si es pot provar per inducció que, per a tot nombre natural $n\geq 0$, es compleix:

a) $2|2n^3+3n^2+n$

b) $30|n^5-n$

c) $6|2n^3+3n^2+n$

d) $4|n^4+2n^3+n^2$

Solució. En demostrarem algun. Per exemple, $4|n^4+2n^3+n^2$.

Observació. Es pot demostrar **directament**:

Tenim $n^4+2n^3+n^2=n^2(n^2+2n+1)=n^2(n+1)^2=(n(n+1))^2$. El producte $n(n+1)$ és producte de dos enters consecutius i, per tant, atès que un dels dos factors és múltiple de 2, resulta múltiple de 2. És a dir, $n(n+1)=2k$ per a algun enter k. Finalment, $n^4+2n^3+n^2=(n(n+1))^2=(2k)^2=4k^2=4k'$, múltiple de 4, amb $k'=k^2$.

Demostració per inducció. Demostrem $4|n^4+2n^3+n^2$ per inducció sobre n, amb valor inicial $n_0=0$.

Pas bàsic. Cal veure que la propietat es compleix per al valor inicial $n_0=0$, és a dir, que $4|0^4+2\cdot 0^3+0^2$. Però $0^4+2\cdot 0^3+0^2=0$, i és evident que $4|0$.

Pas inductiu. Vegem que, per a tot $n\geq 0$, es compleix:

$4|n^4+2n^3+n^2 \Rightarrow 4|(n+1)^4+2(n+1)^3+(n+1)^2$.

Tenim:

$(n+1)^2 = n^2+2n+1,$
$(n+1)^3 = n^3+3n^2+3n+1,$
$(n+1)^4 = \binom{4}{0}+\binom{4}{1}n+\binom{4}{2}n^2+\binom{4}{3}n^3+\binom{4}{4}n^4$, per la fórmula del binomi de Newton. Així:

$(n+1)^4 = 1+4n+6n^2+4n^3+n^4.$

Per tant:

$(n+1)^4+2(n+1)^3+(n+1)^2$
$= (1+4n+6n^2+4n^3+n^4)+2(n^3+3n^2+3n+1)+(n^2+2n+1).$

Reagrupant de manera que aparegui $n^4+2n^3+n^2$, resulta:

$(n+1)^4+2(n+1)^3+(n+1)^2$
$= (n^4+2n^3+n^2)+4n^3+12n^2+12n+4$
$= (n^4+2n^3+n^2)+4(n^3+3n^2+3n+1).$

Per la hipòtesi (hipòtesi d'inducció), $n^4+2n^3+n^2 = 4k$ per a un enter k convenient. Per tant:

$(n+1)^4+2(n+1)^3+(n+1)^2 = (n^4+2n^3+n^2)+4(n^3+3n^2+3n+1) = 4(k+n^3+3n^2+3n+1) = 4k'$, amb $k' = k+n^3+3n^2+3n+1$.

Així, existeix un enter k' tal que $(n+1)^4+2(n+1)^3+(n+1)^2 = 4k'$, és a dir, $4|(n+1)^4+2(n+1)^3+(n+1)^2$.

Queda demostrat, per tant, el pas inductiu, i completada així la demostració per inducció.

PROBLEMA 7.22

Demostreu per inducció $4|9^n+3$*, per a tot nombre natural* $n \geq 0$.

També és cert $12|9^n+3$ *per a tot nombre natural* $n \geq 1$*. Demostreu-ho per inducció.*

Solució. $4|9^n+3$ Demostrem-ho per inducció sobre n, amb valor inicial $n_0 = 0$.

Pas bàsic. Cal provar que la propietat es compleix per a $n = n_0 = 0$, és a dir, que $4|9^0+3$, cosa que és evident.

Pas inductiu. Cal provar $4|9^n+3 \Rightarrow 4|9^{n+1}+3$, per a tot $n \geq n_0 = 0$.

La hipòtesi d'inducció (HI) és la suposició $4|9^n+3$ en el marc del condicional anterior.

Idea de la demostració. Intentarem expressar $9^{n+1}+3$ com una fórmula on aparegui l'expressió 9^n+3 com a subfórmula i es pugui aplicar la hipòtesi d'inducció. Observeu que escrivim $9=8+1$ amb l'objectiu d'obtenir un sumand 9^n.

Tenim $9^{n+1}+3=9\cdot 9^n+3=(8+1)\cdot 9^n+3=(8\cdot 9^n+9^n)+3=8\cdot 9^n+(9^n+3)$. Per HI, $9^n+3=4k$ per a algun enter k; per tant, $9^{n+1}+3=8\cdot 9^n+4k=4(2\cdot 9^n+k)$, múltiple de 4, com s'havia de veure.

Això conclou la demostració.

Variant expositiva 2. Per la HI, existeix un enter k tal que $9^n+3=4k$, és a dir, $9^n=4k-3$. Aleshores $9^{n+1}+3=9\cdot 9^n+3=9\cdot(4k-3)+3=9\cdot 4k-27+3=4\cdot 9k-24=4(9k-6)$, múltiple de 4.

$12|9^n+3$ És similar a l'anterior.

El *pas bàsic* és immediat, ja que $12|9^1+3$.

Vegem l'adaptació que es pot fer del *pas inductiu*:

$12|9^n+3 \Rightarrow 12|9^{n+1}+3$, per a tot $n\geq 1$.

Per la hipòtesi d'inducció, per a un enter k convenient, $9^n=12k-3$.

Per tant, $9^{n+1}+3=9\cdot 9^n+3=9\cdot(12k-3)+3=9\cdot 12k-9\cdot 3-3=12\cdot 9k-24=12(9k-2)=12k'$, amb $k'=9k-2$, enter. Així, $12|9^{n+1}+3$ i resulta demostrada la implicació $12|9^n+3 \Rightarrow 12|9^{n+1}+3$.

Variant argumental. $9^{n+1}+3=9\cdot 9^n+3=(2\cdot 4+1)\cdot 9^n+3=2\cdot 4\cdot 9^n+(9^n+3)=2\cdot 4\cdot 3\cdot 3\cdot 9^{n-1}=12\cdot 6\cdot 9^{n-1}+(9^n+3)$ (recordem que $n\geq 1$). Per hipòtesi d'inducció, és $9^n+3=12k$, per a algun enter k. Per tant, $9^{n+1}+3=12k'$, múltiple de 12, amb $k'=6\cdot 9^{n-1}+k$.

PROBLEMA 7.23

Demostreu per inducció $2|n^2+n-2$, *per a tot nombre natural* $n\geq 0$.

Solució. Demostració per inducció sobre n, amb valor inicial $n_0=0$.

Pas base. Vegem que $2|0^2+0-2=-2$, que és obvi.

Pas inductiu. Vegem que, per a tot $n\geq 0$, es compleix

$2|n^2+n-2 \Rightarrow 2|(n+1)^2+(n+1)-2$.

Desenvolupem la fórmula $(n+1)^2+(n+1)-2$ reescrivint-la de manera que en el desenvolupament hi aparegui la fórmula n^2+n-2 i es pugui aplicar la hipòtesi:

$(n+1)^2+(n+1)-2=(n^2+2n+1)+(n+1)-2=(n^2+n-2)+(2n+2)=(n^2+n-2)+2(n+1)$. És suma de dos parells i, per tant, parell, ja que per hipòtesi n^2+n és parell.

PROBLEMA 7.24

Demostreu per inducció $6|n^3+3n^2+2n$*, per a tot nombre natural* $n \geq 0$.

Solució. Demostració per inducció sobre n, amb valor inicial $n_0 = 0$.

Pas base. Vegem que la propietat és certa per al valor inicial $n_0 = 0$, és a dir, que $6|0^3 + 3 \times 0^2 + 2 \times 0 = 0$, cosa òbvia.

Pas inductiu. Cal provar $6|n^3+3n^2+2n \Rightarrow 6|(n+1)^3+3(n+1)^2+2(n+1)$ per a tot $n \geq 0$.

Hipòtesi (d'inducció): $6|n^3+3n^2+2n$, és a dir, existeix un enter k tal que $n^3+3n^2+2n = 6k$.

Tesi: $6|(n+1)^3+3(n+1)^2+2(n+1)$, és a dir, existeix un enter k' tal que $(n+1)^3 + 3(n+1)^2+2(n+1) = 6k'$.

Efectuarem càlculs amb $(n+1)^3+3(n+1)^2+2(n+1)$, amb l'objectiu de poder-hi aplicar la hipòtesi d'inducció.

$(n+1)^3+3(n+1)^2+2(n+1) = (n^3+3n^2+3n+1)+3(n^2+2n+1)+2n+2$.

Ara reagrupem termes per tal de fer-hi aparèixer n^3+3n^2+2n, si és possible:

$(n+1)^3+3(n+1)^2+2(n+1) = (n^3+3n^2+2n)+3n+1+3n^2+6n+3+2 = (n^3+3n^2+2n)+3(n+n^2)+6n+6 \overset{HI}{=} 6k+6n+6+3(n+n^2)$.

Sembla que hi falta un factor 2. Escrivim $n+n^2 = n(1+n)$, producte de dos enters consecutius: un d'ells és parell, és a dir, múltiple de 2 i, per tant, també ho és el producte. Així, $n+n^2 = 2\alpha$ i, per tant:

$(n+1)^3+3(n+1)^2+2(n+1) = 6k+6n+6+3(n+n^2) = 6k+6n+6+3\cdot 2\alpha = 6(k+n+\alpha) = 6k'$, múltiple de 6.

Hem demostrat la implicació: final de la demostració per inducció.

PROBLEMA 7.25

Demostreu per inducció $25|4^{2n}+10n-1$*, per a tot nombre natural* $n \geq 0$.

Solució. Demostració per inducció sobre n amb valor inicial $n_0 = 0$.

Pas base. Cal provar la propietat per a $n_0 = 0$, cosa que és una obvietat, ja que $25|4^{2\times 0} + 10 \times 0 - 1 = 1+0-1 = 0$.

Pas inductiu. Vegem que, per a qualsevol $n \geq 0$:

$25|4^{2n}+10n-1 \Rightarrow 25|4^{2(n+1)}+10(n+1)-1$.

La hipòtesi (hipòtesi d'inducció) és: $25|4^{2n}+10n-1$.

Reformulació de la hipòtesi. Per la hipòtesi, existeix un enter k tal que

$4^{2n} + 10n - 1 = 25k$, igualtat que podem reescriure com $4^{2n} \stackrel{*}{=} 25k - 10n + 1$.

Ara efectuem càlculs amb $4^{2(n+1)} + 10(n+1) - 1$, amb l'objectiu de fer-hi aparèixer 4^{2n} i aplicar la hipòtesi (*):

$4^{2(n+1)} + 10(n+1) - 1 = 4^{2n+2} + 10n + 10 - 1 = 16 \cdot 4^{2n} + 10n + 10 - 1 \stackrel{*}{=} 16 \cdot (25k - 10n + 1) + 10n + 9 = 16 \cdot 25k - 150n + 25 = 25(k - 6n + 1)$, múltiple de 25, com s'havia de veure.

Això conclou la demostració per inducció.

PROBLEMA 7.26

Demostreu per inducció

$9|n^3 + (n+1)^3 + (n+2)^3$ *per a tot nombre natural* $n \geq 0$.

Solució. Vegem una demostració per inducció sobre n, amb valor inicial $n_0 = 0$.

Sigui $P(n) :=$ "$9|n^3 + (n+1)^3 + (n+2)^3$" la propietat que es vol demostrar.

Pas bàsic. Cal provar $P(n_0)$, és a dir, $P(0)$. Això significa que hem de provar que la propietat és certa per a $n = 0$, o sigui, $9|0^3 + (0+1)^3 + (0+2)^3$. Però $0^3 + (0+1)^3 + (0+2)^3 = 9$ i, per tant, és cert.

Pas inductiu. Hem de demostrar la implicació:

$P(n) \stackrel{?}{\Rightarrow} P(n+1)$, per a tot $n \geq n_0 = 0$. Concretant, s'ha de provar:

$9|n^3 + (n+1)^3 + (n+2)^3 \stackrel{?}{\Rightarrow} 9|(n+1)^3 + ((n+1)+1)^3 + ((n+1)+2)^3$, és a dir, $9|n^3 + (n+1)^3 + (n+2)^3 \stackrel{?}{\Rightarrow} 9|(n+1)^3 + (n+2)^3 + (n+3)^3$.

La suposició $9|n^3 + (n+1)^3 + (n+2)^3$ és la hipòtesi d'inducció (HI), i es pot expressar com $n^3 + (n+1)^3 + (n+2)^3 = 9k$ per a algun enter k convenient (que existeix). A la vista de la tesi, i amb la intenció de fer-ne una substitució posterior, podem reescriure-la com $(n+1)^3 + (n+2)^3 = 9k - n^3$.

Ara considerem l'expressió que figura a la tesi: $(n+1)^3 + (n+2)^3 + (n+3)^3$, que relacionarem amb la hipòtesi. En aplicació de la hipòtesi d'inducció:

$$(n+1)^3 + (n+2)^3 + (n+3)^3$$
$$= [(n+1)^3 + (n+2)^3] + (n+3)^3$$
$$= (9k - n^3) + (n+3)^3.$$

Vegem que aquesta última expressió és múltiple de 9: $(9k - n^3) + (n+3)^3 = 9k - n^3 + (n^3 + 9n^2 + 27n + 27) = 9k + 9n^2 + 27n + 27 = 9(k + n^2 + 3n + 3)$, múltiple de 9.

La demostració està acabada.

Variant expositiva. Partim de la HI (amb la idea d'"aproximar-nos" a la tesi):

$n^3+(n+1)^3+(n+2)^3=9k$. Restem n^3, membre a membre, a la igualtat:

$(n+1)^3+(n+2)^3=9k-n^3$. Sumem $(n+3)^3$:

$(n+1)^3+(n+2)^3+(n+3)^3=9k-n^3+(n+3)^3$.

Ara només resta demostrar que $9k-n^3+(n+3)^3$ és múltiple de 9, cosa que s'ha fet anteriorment.

PROBLEMA 7.27

Demostreu per inducció $64|9^n-8n-1$ *per a tot nombre natural* $n\geq 0$.

Solució. Es demostra per inducció sobre n, amb valor inicial $n_0=0$.

Pas bàsic. Cal demostrar la propietat per a $n=n_0=0$.

Cal demostrar $64|9^0-8\times 0-1$, és a dir, $64|1-0-1=0$, cert.

Pas inductiu. Cal demostrar que, si la propietat és certa per a n, aleshores també ho és per a $n+1$, per a tot $n\geq 0$. És a dir, $64|9^n-8n-1 \Rightarrow 64|9^{n+1}-8(n+1)-1$, per a tot $n\geq 0$.

Suposant cert $9^n-8n-1=64k$ per a algun enter k (hipòtesi, hipòtesi d'inducció), hem de veure que és cert $9^{n+1}-8(n+1)-1=7k'$ per a algun enter k' adequat (tesi).

Efectuem càlculs sobre $9^{n+1}-8(n+1)-1$ amb la idea de fer-hi aparèixer la fórmula del mateix patró de la hipòtesi, per tal de poder aplicar-la:

$9^{n+1}-8(n+1)-1=9\cdot 9^n-8n-8-1=(8+1)\cdot 9^n-8n-8-1=8\cdot 9^n+9^n-8n-8-1=(8\cdot 9^n-8)+(9^n-8n-1)\overset{HI}{=}(8\cdot 9^n-8)+64k=8(9^n-1)+64k$.

Atès que $64=8^2$, vegem si 9^n-1 aporta el factor 8 que ens convindria. En efecte, podem utilitzar la fórmula $x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1})$ expressant $9^n-1=9^n-1^n=(9-1)(9^{n-1}+9^{n-2}y+\cdots+9+1)=8(9^{n-1}+9^{n-2}y+\cdots+9+1)$.

Per tant, finalment, $9^{n+1}-8(n+1)-1=8(9^n-1)+64k=8(8k')+64k=64(k'+k)=64k''$, múltiple de 64.

Observació: Resolem el problema auxiliar $8|9^n-1$ utilitzant alternativament la fórmula del binomi de Newton (amb $9=8+1$):

Suposem que $n\geq 1$.

$$9^n-1=(8+1)^n-1=(\sum_{j=0}^{n}\binom{n}{j}8^j1^{n-j})-1=(\sum_{j=0}^{n}\binom{n}{j}8^j)-1=\binom{n}{0}8^0+$$

$$+(\sum_{j=1}^{n}\binom{n}{j}8^{j})-1=1+(8\sum_{j=1}^{n}\binom{n}{j}8^{j-1})-1=8\sum_{j=1}^{n}\binom{n}{j}8^{j-1}=8\alpha,$$

amb $\alpha=\sum_{j=1}^{n}\binom{n}{j}8^{j-1}\in\mathbb{Z}$.

Argumentació alternativa. Utilitzeu la reexpressió de la hipòtesi d'inducció:

$9^{n}=64k+8n+1$ per a un enter k convenient.

PROBLEMA 7.28

Demostreu per inducció $7|3^{2n+1}+2^{n+2}$ *per a tot nombre natural* $n\geq 0$.

Solució. Sigui $P(n):=$ "$7|3^{2n+1}+2^{n+2}$", que demostrem per inducció sobre n, amb valor inicial $n_0=0$.

Pas base. Demostrem que $P(0)$ és cert, és a dir, que $7|3^{2\cdot 0+1}+2^{0+2}$ és cert. Això és $7|3+4=7$, obvi.

Pas inductiu. Demostrem $P(n)\Rightarrow P(n+1)$ per a tot $n\geq 0$, és a dir,

$7|3^{2n+1}+2^{n+2}\Rightarrow 7|3^{2(n+1)+1}+2^{(n+1)+2}$.

La hipòtesi d'inducció (HI) és suposar que $7|3^{2n+1}+2^{n+2}$ és cert.

S'ha de veure:

$\exists k(3^{2n+1}+2^{n+2}=7k)\Rightarrow\exists k'(3^{2(n+1)+1}+2^{(n+1)+2}=7k')$ $(k,k'$ enters).

Idea per a la demostració. Desenvolupem $3^{2(n+1)+1}+2^{(n+1)+2}$ de manera que hi aparegui $3^{2n+1}+2^{n+2}$ i puguem aplicar la HI:

$3^{2(n+1)+1}+2^{(n+1)+2}$

$=3^{(2n+1)+2}+2^{(n+2)+1}$ (intentant obtenir les expressions que apareixen a la HI)

$=9\cdot 3^{2n+1}+2\cdot 2^{n+2}$

$=(7+2)\cdot 3^{2n+1}+2\cdot 2^{n+2}$

$=7\cdot 3^{2n+1}+2\cdot 3^{2n+1}+2\cdot 2^{n+2}$

$=7\cdot 3^{2n+1}+2(3^{2n+1}+2^{n+2})$

$\overset{HI}{=}7\cdot 3^{2n+1}+2(7k)$ per a un enter k.

Així, $3^{2(n+1)+1}+2^{(n+1)+2}=7(3^{2n+1}+2k)=7k'$, múltiple de 7, amb $k'=3^{2n+1}+2k$.

Això conclou la demostració del pas inductiu i de la demostració per inducció.

Argumentació alternativa a la demostració del pas inductiu. Escrivim la HI, $7|3^{2n+1} + 2^{n+2}$, de la forma $3^{2n+1} = 7k - 2^{n+2}$ per a cert enter k. Substituïm:

$$\begin{aligned}
&3^{2(n+1)+1} + 2^{(n+1)+2}\\
&= 3^{(2n+1)+2} + 2^{(n+2)+1}\\
&= 9 \cdot 3^{2n+1} + 2 \cdot 2^{n+2}\\
&= 9(7k - 2^{n+2}) + 2 \cdot 2^{n+2}\\
&= 9 \cdot 7k - 9 \cdot 2^{n+2} + 2 \cdot 2^{n+2}\\
&= 9 \cdot 7k + (2-9)2^{n+2} = 7(9k - 2^{n+2}), \text{ múltiple de 7.}
\end{aligned}$$

PROBLEMA 7.29

Demostreu per inducció $5|8^n - 3^n$ *per a tot nombre natural* $n \geq 0$.

Solució. Sigui $P(n) :=$ “$5|8^n - 3^n$”, que demostrarem per inducció sobre n, amb valor inicial $n_0 = 0$.

Pas base. Demostrem que $P(0)$ és cert, és a dir, que $5|8^0 - 3^0$. Això és $5|1-1 = 0$, cosa òbvia.

Pas inductiu. Demostrem $P(n) \Rightarrow P(n+1)$ per a tot $n \geq 0$, és a dir,

$5|8^n - 3^n \Rightarrow 5|8^{n+1} - 3^{n+1}$.

La hipòtesi d'inducció (HI) és suposar $5|8^n - 3^n$.

S'ha de veure: $\exists k(8^n - 3^n = 5k) \Rightarrow \exists k'(8^{n+1} - 3^{n+1} = 5k')$ (k, k' enters).

Idea clau. Desenvolupem $8^{n+1} - 3^{n+1}$ de manera que aparegui $8^n - 3^n$ a la fórmula i puguem aplicar-hi la HI:

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

Per la HI, existeix un enter k tal que $8^n - 3^n = 5k$, d'on

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

múltiple de 5, amb $k'' = 8^n + 3k$.

Això conclou la demostració del pas inductiu i de la demostració per inducció.

Argumentació alternativa a la demostració del pas inductiu. Escrivim la HI de la forma $8^n = 5k + 3^n$. Aleshores, podem substituir: $8^{n+1} - 3^{n+1} = 8 \cdot 8^n - 3 \cdot 3^n = 8 \cdot (5k + 3^n) - 3 \cdot 3^n = 8 \cdot 5 \cdot k + 8 \cdot 3^n - 3 \cdot 3^n = 8 \cdot 5 \cdot k + (5+3) \cdot 3^n - 3 \cdot 3^n = 8 \cdot 5 \cdot k + 5 \cdot 3^n + 3 \cdot 3^n - 3 \cdot 3^n = 8 \cdot 5 \cdot k + 5 \cdot 3^n = 5 \cdot (8k + 3^n)$, múltiple de 5.

PROBLEMA 7.30

Demostreu per inducció $81|10^n - 9n - 1$ *per a tot nombre natural* $n \geq 0$.

Solució. Sigui $P(n) :=$ “$81|10^n - 9n - 1$”, que demostrarem per inducció sobre n, amb valor inicial $n_0 = 0$.

Pas base. Demostrem que $P(0)$ és cert, és a dir, que $81|10^0 - 9 \cdot 0 - 1$. Això és $81|1 - 0 - 1 = 0$, que és obvi.

Pas inductiu. Demostrem $P(n) \Rightarrow P(n+1)$ per a tot $n \geq 0$, és a dir:

$81|10^n - 9n - 1 \Rightarrow 81|10^{n+1} - 9(n+1) - 1$.

La hipòtesi d’inducció (HI) és suposar $81|10^n - 9n - 1$.

Idea clau. Desenvolupem $10^{n+1} - 9(n+1) - 1$, de manera que aparegui $10^n - 9n - 1$ a la fórmula i es pugui aplicar la HI:

$10^{n+1} - 9(n+1) - 1 = 10 \cdot 10^n - 9n - 9 - 1 = (9+1) \cdot 10^n - 9n - 9 - 1 = 9 \cdot 10^n + 10^n - 9n - 9 - 1 = 9 \cdot 10^n - 9 + (10^n - 9n - 1) \overset{HI}{=} 9 \cdot 10^n - 9 + 81k = 9(10^n - 1) + 81k$.

Es pot demostrar que $9|10^n - 1$ per diversos mètodes: per inducció, desenvolupant per la fórmula del binomi de Newton o amb la igualtat

$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots xy^{n-2} + y^{n-1})$ amb $x = 10$, y^1. Així, doncs, fet això, tenim $10^n - 1 = 10^n - 1^n = (10-1)k' = 9k'$ per a algun enter k'.
Per tant:

$10^{n+1} - 9(n+1) - 1 = 9(10^n - 1) + 81k = 9 \cdot 9k' + 81k = 81(k + k') = 81k''$, múltiple de 81.

Observació: Resolem el problema auxiliar $9|10^n - 1$ utilitzant la fórmula del binomi de Newton (esquema: amb $10 = 9 + 1$, vegeu-ne el capítol corresponent, amb l’exercici similar resolt $6|7^n - 1$):

Per a $n = 0$, substituint resulta $9|10^0 - 1 = 1 - 1 = 0$. Suposem, per tant, que $n \geq 1$.

$$10^n - 1 = (9+1)^n - 1 = \left(\sum_{j=0}^{n} \binom{n}{j} 9^j 1^{n-j}\right) - 1 = \left(\sum_{j=0}^{n} \binom{n}{j} 9^j\right) - 1 = \binom{n}{0} 9^0 + \left(\sum_{j=1}^{n} \binom{n}{j} 9^j\right) - 1 = 1 + \left(9 \sum_{j=1}^{n} \binom{n}{j} 9^{j-1}\right) - 1 = 9 \sum_{j=1}^{n} \binom{n}{j} 9^{j-1} = 9\alpha, \text{ amb } \alpha = \sum_{j=1}^{n} \binom{n}{j} 9^{j-1} \in \mathbb{Z}.$$

També es demostra $9|10^n - 1$ per inducció en un problema independent en aquest mateix capítol.

Això conclou la demostració del pas inductiu i de la demostració per inducció.

Argumentació alternativa a la demostració del pas inductiu. Escrivim la HI $81|10^n - 9n - 1$ en la forma $10^n = 81k + 9n + 1$ per a algun enter k. Aleshores, podem substituir: $10^{n+1} - 9(n+1) - 1 = 10 \cdot 10^n - 9n - 9 - 1 = 10 \cdot (81k + 9n + 1) - 9n - 9 - 1 = 10 \cdot 81k + 10 \cdot 9n + 10 - 9n - 9 - 1 = 10 \cdot 81k + 10 \cdot 9n - 9n = 10 \cdot 81k + 81n = 81(10k + n)$, múltiple de 81.

PROBLEMA 7.31

Demostreu per inducció $9|10^n - 1$ *per a tot nombre natural* $n \geq 0$.

Solució. Sigui $P(n) :=$ "$9|10^n - 1$", que demostrarem per inducció sobre n, amb valor inicial $n_0 = 0$.

Pas base. Demostrem que $P(0)$ és cert, és a dir, que $9|10^0 - 1$. Això és $9|1 - 1 = 0$, que és obvi.

Pas inductiu. Demostrem $P(n) \Rightarrow P(n+1)$ per a tot $n \geq 0$, és a dir:

$9|10^n - 1 \Rightarrow 9|10^{n+1} - 1$.

La hipòtesi d'inducció (HI) és suposar que $9|10^n - 1$ és cert.

Idea clau. Desenvolupem $10^{n+1} - 1$, de manera que aparegui $10^n - 1$ a la fórmula i es pugui aplicar la HI:

$10^{n+1} - 1 = 10 \cdot 10^n - 1 = (9+1) \cdot 10^n - 1 = 9 \cdot 10^n + 10^n - 1$

$= 9 \cdot 10^n + (10^n - 1) \stackrel{HI}{=} 9 \cdot 10^n + 9k = 9(10^n + k) = 9k''$, múltiple de 9.

Això conclou la demostració del pas inductiu i de la demostració per inducció.

Argumentació alternativa a la demostració del pas inductiu. Escrivim la HI en la forma $10^n = 9k + 1$. Aleshores, podem substituir: $10^{n+1} - 1 = 10 \cdot 10^n - 1 = 10(9k+1) - 1 = 9 \cdot 10k + 10 - 1 = 9 \cdot 10k + 9 = 9(10k+1) = 9k'''$, múltiple de 9.

7.2.4. Enunciats amb factorials

Els que presentem són majorment amb desigualtats.

PROBLEMA 7.32

Demostreu per inducció que $4^n < n!$ *per a tot nombre natural* $n \geq 9$.

Enunciats anàlegs: $2^n \leq n!$, $3^n \leq n!$, $5^n \leq n!$ *a partir de determinats valors inicials de n (que el lector obtindrà).*

Solució. Efectuem uns càlculs auxiliars que calen per al pas base de la demostració per inducció:

$4^9 = 262144$

$9! = 362880$

Formalment, denotem $P(n) :=$"$4^n < n!$". Cal veure $P(n), \forall n \geq 9$.

Pas base. Demostrem la propietat $P(n)$ per $n = 9$. Així, $n_0 = 9$ (valor inicial).

Equivalentment, provem que $P(9)$ és cert, és a dir, que $4^9 < 9!$. Però això és una simple comprovació a partir dels càlculs anteriors. Observació: Es pot comprovar que, per a valors anteriors a $n_0 = 9$, no es compleix.

Pas inductiu. Cal provar $P(k) \Rightarrow P(k+1)$, per a tot natural $k \geq 9$. És a dir:

$4^k \overset{(HI)}{<} k! \Rightarrow 4^{k+1} < (k+1)!$

En efecte:

$4^{k+1} = 4 \cdot 4^k \overset{(HI)}{<} 4k!$ (aplicant la hipòtesi d'inducció)

$< (k+1)k!$ (ja que $k \geq 9 \Rightarrow k+1 > 10 > 4$)

$= (k+1)!$, per la fórmula recurrent per al factorial.

Això conclou el pas inductiu i també la demostració per inducció.

Afegit. Vegem detalls de la demostració de $3^n < n!$, per a tot $n \geq 7$, per inducció sobre n, amb valor inicial $n_0 = 2$. *Observació*: Per a valors inferiors a 7, la desigualtat no és vàlida.

El *pas bàsic* és una simple comprovació de $3^7 < 7!$ ($3^7 = 2187$, $7! = 5040$).

En el *pas inductiu*, hem de provar $3^n < n! \Rightarrow 3^{n+1} < (n+1)!$, per a tot $n \geq 7$. En efecte, $3^{n+1} = 3 \cdot 3^n \overset{(HI)}{<} 3 \cdot n! < (n+1)(n!) = (n+1)!$, ja que $n+1 > 6+1 = 7 > 3$.

Observació. N'hi ha hagut prou amb $n \geq 2$ per a la demostració del pas inductiu.

PROBLEMA 7.33

Demostreu per inducció que $n! < (n+1)^{n+1}$ per a tot nombre natural $n \geq 2$.

Solució. Afirmació que es vol demostrar:

$P(n), \forall n \geq 2$, amb $P(n) :=$ "$n! < (n+1)^{n+1}$".

Valor inicial: $n_0 = 2$.

Pas bàsic. Demostrar $P(2)$, és a dir, que $2! < (2+1)^{2+1}$, que és una obvietat, ja que $2 = 2! < 3^3$.

Pas inductiu. Hem de demostrar: $P(k) \Rightarrow P(k+1)$, per a tot nombre natural $k \geq 2$, és a dir:

$k! \overset{(HI)}{<} (k+1)^{k+1} \Rightarrow (k+1)! < ((k+1)+1)^{(k+1)+1}$, és a dir:

$k! \overset{(HI)}{<} (k+1)^{k+1} \Rightarrow (k+1)! < ((k+2)^{(k+2)}$.

En efecte:

$$(k+1)! = k!(k+1) \overset{(HI)}{<} (k+1)^{k+1}(k+1) = (k+1)^{(k+1)+1} = (k+1)^{k+2} \overset{(*)}{<} (k+2)^{k+2}$$

(*): hi apliquem $k+1 < k+2 \Rightarrow (k+1)^{k+2} < (k+2)^{k+2}$.

Això conclou la demostració per inducció del resultat.

PROBLEMA 7.34

Demostreu per inducció $n! > n$ per a tot nombre natural $n \geq 3$.

Solució. Fem la demostració per inducció sobre n, amb $n_0 = 3$.

Pas base. Vegem que la propietat és certa per a $n = 3$, és a dir, que $3! > 3$, cosa que és evident.

Pas inductiu. Cal veure que $k! \overset{(HI)}{>} k \Rightarrow (k+1)! > (k+1)$, per a tot $k \geq 3$.

En efecte:

$$(k+1)! = k!(k+1) \overset{(HI)}{>} k(k+1) > 1 \cdot (k+1) = k+1, \text{ ja que } k > 1.$$

PROBLEMA 7.35

Demostreu per inducció $n! > n^2$ per a tot nombre natural $n \geq 4$.

Solució. Fem la demostració per inducció sobre n, amb $n_0 = 4$.

Pas base. Vegem que la propietat és certa per a $n = 4$, és a dir, que $4! > 4^2$, cosa evident.

Pas inductiu. Cal veure que $k! \overset{(HI)}{>} k^2 \Rightarrow (k+1)! > (k+1)^2$, per a tot $k \geq 4$.

En efecte:

$$(k+1)! = k!(k+1) \overset{(HI)}{>} k^2(k+1).$$

Si veiem que $k^2 > k+1$, el problema queda resolt ja que aleshores tenim $k^2(k+1) > (k+1)(k+1) = (k+1)^2$.

Serà cert si $k^2 - k > 1$, que equival a $k(k-1) > 1$. Ara bé, si $k \geq 4$, resulta $k(k-1) \geq 4 \cdot (4-1) = 12 > 1$.

Per tant, per a $k \geq 4$,

$(k+1)! = k!(k+1) \overset{(HI)}{>} k^2(k+1) > (k+1)(k+1) = (k+1)^2$, com havíem de veure.

Queda demostrada la propietat per inducció.

Observació. La propietat auxiliar $k^2 > k+1$ també es pot establir estudiant les funcions x^2, $x+1$ i veient que, a partir d'un cert lloc en endavant, es compleix $x^2 > x+1$ (la gràfica de la paràbola $y = x^2$ està per sobre de la de la recta $y = x+1$), o bé que la funció $x^2 - x - 1$ és positiva d'un cert lloc en endavant.

7.3. Sobre el pas bàsic

Demostrar el pas bàsic és imprescindible per a la demostració per inducció. L'omissió d'aquest pas significa que la propietat resta no provada, encara que es faci la demostració del pas inductiu.

La prova de l'anomenat "pas bàsic" pot que requerir provar més d'un cas, de manera que, segons l'enunciat, s'hagin de demostrar dos o més casos bàsics, a fi que pugui funcionar el mecanisme a partir dels inicis. Un exemple típic és el de determinades successions recurrents, en què tenim una, dues o més condicions inicials.

En molts exemples, la demostració del pas bàsic sol reduir-se a una simple comprovació, però no sempre és així. N'aportarem algun exemple.

1. El pas bàsic no es pot ometre

En el mètode d'inducció, ja es veu que, per raó del mètode, és imprescindible demostrar el pas bàsic (que pot constar, de fet, de més d'una part, i així tenir un, dos o més passos bàsics, o diferents parts del pas bàsic). Vegem un parell d'exemples d'una afirmació **falsa** per a la qual podem demostrar el pas inductiu.

Exemple 7.4 Considerem la suposada propietat següent $P(n)$, per a n nombre natural ($n \geq 1$):

"$1+3+5+7+\cdots+(2k-1)+\cdots+(2n-1) = n^2+1$ ", o bé

"$\forall n (n \geq 1 \rightarrow 1+3+5+7+\cdots+(2k-1)+\cdots+(2n-1) = n^2+1)$ "

Vegem com es pot demostrar el pas inductiu, encara que la propietat **no** sigui certa:

Pas inductiu. $P(n) \Rightarrow P(n+1)$, per tot $n \geq 1$.

Cal provar $\sum_{k=1}^{n}(2k-1)=n^2+1 \Rightarrow \sum_{k=1}^{n+1}(2k-1)=(n+1)^2+1$. En efecte:

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

En aquest cas, no només és falsa l'afirmació, sinó que no és certa per a cap nombre natural. En efecte, la suma autèntica es pot calcular com

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

Vegem que no és cert el pas bàsic, que seria per a $n=1$:

$$\sum_{k=1}^{1}(2k-1)=2\cdot 1-1 \overset{?}{=} 1^2+1, \text{ fals. } \blacksquare$$

Exemple 7.5 Vegem-ne un segon exemple:

Considerem l'enunciat següent:

"$1+2+3+\cdots+k+\cdots+n=\frac{1}{8}(2n+1)^2$, per a tot nombre natural $n\geq 1$".

Aquest enunciat no sols és fals, sinó que és fals per a qualsevol n positiu. En efecte, si existís algun n natural per al qual la igualtat fos certa, aleshores, tenint en compte que $1+2+\cdots+n=\frac{n(n+1)}{2}$ (resultat cert), tindríem:

$$\frac{n(n+1)}{2}=\frac{1}{8}(2n+1)^2.$$

Efectuant els càlculs pertinents, resulta l'absurd $1=0$.

Si intentem demostrar el suposat resultat per inducció, no aconseguirem demostrar-ne cap pas bàsic; en canvi, és demostrable el pas inductiu, i així veiem que el pas bàsic no és superflu.

Pas inductiu. Per al pas inductiu, suposem certa l'afirmació per a n, és a dir:

$$1+2+3+\cdots+k+\cdots+n \overset{HI}{=} \frac{1}{8}(2n+1)^2 \text{ (hipòtesi d'inducció)}$$

i l'aplicarem per a demostrar l'afirmació per a $n+1$, és a dir:

$$1+2+3+\cdots+k+\cdots+n+(n+1)=\frac{1}{8}(2(n+1)+1)^2.$$

En efecte:

$1+2+3+\cdots+k+\cdots+n+(n+1)=(1+2+3+\cdots+k+\cdots+n)+(n+1)\overset{HI}{=}\dfrac{1}{8}(2n+1)^2+(n+1)=\cdots$ càlculs rutinaris $\cdots=\dfrac{1}{8}(2(n+1)+1)^2.$

i així queda demostrat $P(k)\Rightarrow P(k+1)$, per a tot nombre natural $k\geq 1$, malgrat que la propietat és falsa. ■

Vegeu un exemple més de com és imprescindible demostrar el pas bàsic en una demostració per inducció. Observeu que el pas inductiu és demostrable, malgrat que la la propietat és falsa (més encara, és falsa per a tot n).

PROBLEMA 7.36

Considerem l'afirmació

"$P(n):\ 3^n<3^{n-1}$, per a tot nombre natural $n\geq 1$".

a) Proveu que $3^n<3^{n-1}$ és falsa per a tot n natural, $n\geq 1$. En particular, és falsa l'afirmació anterior.

b) Proveu el pas inductiu per a una demostració per inducció sobre n de $P(n)$.

Solució

a) Formalment, i de manera completa, $\forall n((n\in\mathbb{N}\wedge n\geq 1)\rightarrow 3^n<3^{n-1})$. La negació seria $\exists n(n\in\mathbb{N}\wedge n\geq 1\wedge\neg(3^n<3^{n-1}))$, és a dir, $\exists n(n\in\mathbb{N}\wedge n\geq 1\wedge 3^n\geq 3^{n-1})$. Hauríem de demostrar aquesta última afirmació. Resumidament, i suposant les propietats indicades per a n, $\exists n(3^n\geq 3^{n-1})$.

S'ens demana demostrar una propietat més forta: $\forall n(3^n\geq 3^{n-1})$, és a dir:

Per a tot natural $n\geq 1$, $3^n<3^{n-1}$ és fals, és a dir:

Per a tot natural $n\geq 1$, $3^n\geq 3^{n-1}$ és cert.

De fet, si demostrem $\forall n(3^n>3^{n-1})$, com a conseqüència resultarà el que volem veure.

Es pot veure directament: $3^n=3\cdot 3^{n-1}>1\cdot 3^{n-1}=3^{n-1}$.

Fem també la demostració per reducció a l'absurd. Vegem que, si existeix algun n tal que $3^n<3^{n-1}$, aleshores s'arriba a una contradicció.

Mètode 1. Si fos $3^n<3^{n-1}$ (per a algun n), tenint en compte que el logaritme (per exemple neperià o en base 3 o altres) és una funció creixent, resulta:

$3^n<3^{n-1}\Rightarrow\ln 3^n<\ln 3^{n-1}\Rightarrow n\ln 3<(n-1)\ln 3\overset{\ln 3\neq 0}{\Rightarrow}n<n-1\Rightarrow 0<-1$. Deduïm $0<-1$, absurd.

Mètode 2. Si, per a algun $n \geq 1$ és $3^n < 3^{n-1}$, aleshores $\frac{3^n}{3^{n-1}} < 1$, és a dir, $3^{n-(n-1)} < 1$. Per tant, $3^1 < 1$, d'on $3 < 1$, absurd.

Mètode 3. Si, per a algun $n \geq 1$ fos $3^n < 3^{n-1}$, seria $3^n - 3^{n-1} < 0$. Ara bé, $3^{n-1}(3-1) < 0$, és a dir, $0 < 2 \cdot 3^{n-1} < 0$, absurd.

b) *Pas inductiu*. Fixem k arbitrari, k nombre natural, $k \geq 1$. Vegem que $P(k) \Rightarrow P(k+1)$, és a dir, $3^k < 3^{k-1} \Rightarrow 3^{k+1} < 3^{(k+1)-1}$. Finalment, hem de demostrar: $3^k < 3^{k-1} \Rightarrow 3^{k+1} < 3^k$.

Hem de relacionar $P(k+1)$ amb $P(k)$ per tal de poder-hi aplicar la hipòtesi d'inducció (HI), és a dir, la suposició que $P(k)$ és cert, en el marc del condicional anterior. En efecte:

$$3^{k+1} = 3^k \cdot 3 \overset{HI}{<} 3^{k-1} \cdot 3 = 3^{(k-1)+1} = 3^k.$$

També es pot escriure d'una altra manera:

$$3^{k+1} = 3^k \cdot 3 = 3^k + 3^k + 3^k \overset{HI}{<} 3^{k-1} + 3^{k-1} + 3^{k-1} = 3 \cdot 3^{k-1} = 3^{(k-1)+1} = 3^k.$$

O bé, en una *altra variant argumental*, multipliquem per 3 els dos membres de la desigualtat $3^k < 3^{k-1}$, que és la HI. Essent $3 > 0$, es manté l'orientació de la desigualtat i en resulta:

$$3^k \overset{HI}{<} 3^{k-1} \Rightarrow 3 \cdot 3^k < 3 \cdot 3^{k-1} \Rightarrow 3^{k+1} < 3^{(k-1)+1} = 3^k,$$

que és el que havíem de demostrar.

Això prova que no es pot ometre el pas bàsic en cap demostració inductiva.

2. Pas bàsic múltiple

És possible que, per les característiques d'un enunciat, sigui difícil demostrar el pas inductiu per a un n arbitrari, genèric, i, en canvi, sigui factible provar, per exemple $P(k) \Rightarrow P(k+3)$, per a tot $k \geq 1$ (n_0). Demostrant diversos passos bàsics, aconseguim demostrar la propietat per a tot n. En efecte, demostrant $P(1)$, $P(2)$ i $P(3)$, queden demostrats tres fils argumentals inductius (o línies paral·leles), que conjuntament demostren la propietat per a tot $n \geq 1$.

En efecte:

per $P(1)$ i $P(k) \Rightarrow P(k+3)$, $\forall k \geq 1$, resulta demostrada la propietat per a $n = 1, 4, 7, 10, 13, \ldots$

per $P(2)$ i $P(k) \Rightarrow P(k+3)$, $\forall k \geq 2$, resulta demostrada la propietat per a $n = 2, 5, 8, 11, 14, \ldots$

per $P(3)$ i $P(k) \Rightarrow P(k+3)$, $\forall k \geq 3$, resulta demostrada la propietat per a $n = 3, 6, 9, 12, 15, \ldots$

3. El pas bàsic no sempre és trivial. No sempre és una simple comprovació de rutina.

Considerem la generalització de les equivalències de De Morgan per a n proposicions, amb $n \geq 2$:

Siguin $p_1, \cdots, p_n$ proposicions arbitràries, amb $n \geq 2$, n nombre natural. Aleshores, es compleix:

$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv (\neg p_1 \wedge \cdots \wedge \neg p_n)$

$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv (\neg p_1 \vee \cdots \vee \neg p_n)$

Recordem que podem definir $p_1 \vee \cdots \vee p_n = (p_1 \vee \cdots \vee p_{n-1}) \vee p_n$.

Centrem-nos en una d'elles; anàlogament, es procediria amb l'altra.

Exemple 7.6 Considerem la propietat següent:

$P(n) := \neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv (\neg p_1 \wedge \cdots \wedge \neg p_n)$, per a cada $n \geq 2$.

En aquest cas, es demostrarà $P(n)$ per inducció sobre n, amb el valor inicial $n_0 = 2$.

Pas bàsic ($P(2)$ és cert). Cal provar que $\neg(p_1 \vee p_2) \equiv (\neg p_1 \wedge \neg p_2)$. Es pot demostrar per taules de veritat, comprovant que les proposicions tenen la mateixa taula de veritat (les mateixes columnes). D'aquí en resulta l'equivalència lògica.

Taules de veritat:

p_1	p_2	$\neg p_1$	$\neg p_2$	$p_1 \vee p_2$	$\neg(p_1 \vee p_2)$	$\neg p_1 \wedge \neg p_2$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

Això acaba la demostració del pas bàsic.

Pas inductiu ($P(n) \Rightarrow P(n+1)$, per a tot $n \geq 2$).

Fixem $n \geq 2$, nombre natural arbitrari (és a dir, arbitrari però fix per a la demostració).

Cal veure que

$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \overset{HI}{\equiv} (\neg p_1 \wedge \cdots \wedge \neg p_n) \Rightarrow \neg(p_1 \vee p_2 \vee \cdots \vee p_{n+1}) \equiv (\neg p_1 \wedge \cdots \wedge \neg p_{n+1})$

En efecte:

$\neg(p_1 \vee p_2 \vee \cdots \vee p_{n+1}) =$

$\neg((p_1 \vee p_2 \vee \cdots \vee p_n) \vee p_{n+1})$ per associativitat de $\vee$ o per definició,

$\equiv \neg(p_1 \vee p_2 \vee \cdots \vee p_n) \wedge \neg p_{n+1}$ pel que s'ha demostrat per a 2,

$\equiv (\neg p_1 \wedge \cdots \wedge \neg p_n) \wedge \neg p_{n+1}$ per HI,

$\equiv (\neg p_1 \wedge \cdots \wedge \neg p_{n+1})$ per associativitat.

Observació. Aquest esquema és certament especial, ja que en el pas inductiu hem fet servir el resultat del pas bàsic. Res no ho impedeix, però aleshores *de fet* l'esquema demostratiu ha estat $(P(2) \wedge P(n)) \Rightarrow P(n+1)$.■

Anàlogament, demostraríem per inducció les generalitzacions de les fórmules de De Morgan per a conjunts.

Considerem la funció $f(x) = e^{-x}$. És infinitament derivable. En calculem les primeres derivades, aplicant la regla de la cadena:

$f'(x) = -e^{-x}$

$f''(x) = -(-e^{-x}) = e^{-x}$

$f'''(x) = -e^{-x}$

Ja es veu la llei de formació. Recordeu que l'alternança de signe segons paritat es pot aconseguir amb l'expressió $(-1)^n$. Depenent del que interessi, potser s'haurà d'utilitzar alguna altra variant possible, com per exemple $(-1)^{n+1}$. Aleshores, sembla que podem escriure que la derivada n–èsima de f és $f^{(n)} = (-1)^n e^{-x}$ per a qualsevol n nombre natural, $n \geq 1$. Es tracta de demostrar-ho formalment per inducció:

PROBLEMA 7.37

Sigui $f(x) = e^{-x}$. Demostreu que la derivada d'ordre n de f, per a tot n natural positiu, és $f^{(n)} = (-1)^n e^{-x}$.

Solució

Mètode de demostració: per inducció (simple) sobre n.

Propietat que es vol demostrar: $P(n) : f^{(n)} = (-1)^n e^{-x}$, per a tot $n \geq 1$.

Sobre quina variable es fa la demostració per inducció: n.

Valor inicial: $n_0 = 1$.

Pas bàsic. Vegem que $P(1)$ és cert, és a dir, que $f^{(1)}(x) = (-1)^1 e^{-x}$. Cal veure que $f'(x) = -e^{-x}$, que és conseqüència de la regla de la cadena i del fet que $(e^x)' = e^x$, resultats que suposem sabuts i que no cal provar aquí (vegeu qualsevol text de càlcul en una variable). Si no fos així, en això consistiria justament el pas base (i seria un exemple en què el pas base no es limita a una simple comprovació).

Pas inductiu. Cal provar que $P(k) \Rightarrow P(k+1)$, per a tot $k \geq 1$ natural.

Fixem k nombre natural, $k \geq 1$. Vegem que

$$f^{(k)}(x) \overset{HI}{=} (-1)^k e^{-x} \Rightarrow f^{(k+1)}(x) = (-1)^{k+1} e^{-x}.$$

En efecte,

$$f^{(k+1)}(x) = (f^{(k)}(x))' \overset{HI}{=} ((-1)^k e^{-x})' = (-1)^k (e^{-x})' = (-1)^k (-1)(e^{-x}) = (-1)^{k+1} e^{-x}.$$

S'ha aplicat la regla de la cadena i el fet que $(e^x)' = e^x$.

Queda demostrat el pas inductiu i conclosa la demostració per inducció.

5. Més d'un pas bàsic

En el mètode d'inducció (simple), finalment es demostren infinites implicacions. Suposant, per exemple, que $n_0 = 1$:

$P(1) \Rightarrow P(2)$
$P(2) \Rightarrow P(3)$
$P(3) \Rightarrow P(4)$
$P(4) \Rightarrow P(5)$
$\dots$
$P(n-1) \Rightarrow P(n)$
$P(n) \Rightarrow P(n+1)$
$\dots$

Però amb tot això d'abans no resulta demostrada ni una sola propietat $P(k)$.

Cal un inici: el pas bàsic.

Si demostrem $P(1)$, aleshores en cascada resulta demostrat: $P(2)$, $P(3)$, ... i els infinits $P(k)$. En efecte (per *modus ponens*, "MP"):

- de $P(1)$ (obtingut en el pas bàsic) i de $P(1) \Rightarrow P(2)$ en resulta $P(2)$,
- de $P(2)$ (obtingut en el pas anterior) i de $P(2) \Rightarrow P(3)$ se'n deriva $P(3)$,
- de $P(3)$ (obtingut en el pas anterior) i de $P(3) \Rightarrow P(4)$ se'n deriva $P(4)$, i així successivament.

Així, el pas bàsic ens serveix de "palanca" per a iniciar el procés demostratiu. És fonamental que aquest inici es pugui realitzar. Per aquest motiu, de vegades cal considerar un pas bàsic més complex, compost de dos o més passos que s'han de demostrar. Ho exposarem en forma de pas bàsic 1, pas bàsic 2 o part1, part 2 del pas bàsic. El que ha de guiar què cal fer és que es pugui realitzar l'inici de la demostració de totes les propietats $P(n)$, i això s'ha d'analitzar en cada cas. Per tant, hi pot haver altres modalitats de pas bàsic.

Vegem el cas d'una successió recurrent, exemple en què ja s'apunta a una altra modalitat de demostració per inducció, que es tractarà al capítol següent.

Considerem la successió recurrent a_n, $n \geq 1$, donada per les condicions inicials i la fórmula de recurrència:

$a_1 = 1$, $a_2 = 4$ (condicions inicials)

$a_n = 2a_{n-1} - a_{n-2} + 2$, per a $n \geq 3$

El problema consisteix a provar per inducció sobre n que el terme general és $a_n = n^2$, per a tot $n \geq 1$. La propietat $P(n)$ és justament $a_n = n^2$.

Suposem que adoptem l'esquema demostratiu, en el pas inductiu:

$(P(n-2) \wedge P(n-1) \Rightarrow P(n)$. Observeu que això equival a demostrar:

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

$(P(2) \wedge P(3)) \Rightarrow P(4)$

$(P(3) \wedge P(4)) \Rightarrow P(5)$

$\ldots$

Per tal que el mecanisme de demostració pugui arrencar, no n'hi ha prou a demostrar $P(1)$ en el pas bàsic: cal, a més, demostrar $P(2)$. De manera que el pas bàsic constarà de dues parts:

Part 1: demostració de $P(1)$

Part 2: demostració de $P(2)$

D'aquesta manera, havent demostrat $P(1)$, $P(2)$, tenim demostrat $P(1) \wedge P(2)$.

Havent demostrat $(P(1) \wedge P(2)) \Rightarrow P(3)$, resulta demostrat $P(3)$.

Així, tenim demostrat $P(2) \wedge P(3)$; juntament amb $(P(2) \wedge P(3)) \Rightarrow P(4)$, resulta $P(4)$. I així successivament.

Aquí només es fa una reflexió sobre aquesta qüestió. No es resol el problema de demostrar per inducció quin és el terme general.

7.4. La hipòtesi d'inducció (HI) i el pas inductiu

Per raons tradicionals, es manté (però pot no utilitzar-se) la denominació d'"hipòtesi d'inducció" per a la suposició que $P(n)$ és cert en el marc del condicional $P(n) \rightarrow P(n+1)$ del pas inductiu. Per tant, no és que sigui $P(n)$ cert, sinó la suposició de certesa en el curs de la demostració de la implicació $P(n) \Rightarrow P(n+1)$.

Suposem que s'ha de demostrar per inducció una propietat $P(n)$. Se n'ha de demostrar el pas bàsic i el pas inductiu. Un dels problemes en les demostracions del pas inductiu és relacionar $P(n+1)$ amb $P(n)$ de manera que es pugui aplicar "$P(n)$ cert" (que és la HI). El més difícil sol ser com i on aplicar la HI, és a dir, que $P(n)$ és cert, per a demostrar que $P(n+1)$ és cert.

No hi ha regla general en aquest sentit. Depèn de l'habilitat de qui estigui resolent el problema. No sempre és fàcil relacionar $P(n)$ amb $P(n+1)$. És vital per a poder aplicar la HI, és a dir, la suposició que $P(n)$ és cert.

El més típic és manipular o desenvolupar l'expressió de la tesi per tal de fer aparèixer una fórmula (subfórmula) que coincideixi amb la de la HI, de manera que això ens permeti aplicar la hipòtesi d'inducció. Aquesta és la idea principal que guia la resolució (la demostració del pas inductiu). Gran part de les demostracions per inducció del capítol són un exemple d'aquesta manera de procedir.

Vegem-ne un exemple addicional.

PROBLEMA 7.38

Demostreu per inducció que $n^2-2n-1 \geq 0$ *per a tot nombre natural* $n \geq 3$.

Solució. Propietat que es vol demostrar: $P(n): n^2-2n-1 \geq 0$, per a tot $n \geq 3$.

Paràmetre sobre el qual es fa la demostració per inducció: n (per inducció sobre n).

Valor inicial: $n_0 = 3$ (per al pas bàsic).

Pas bàsic. Vegem que $P(3)$ és cert. És a dir, cal veure que $3^2-2\cdot 3-1 \geq 0$, cert.

Observeu (comproveu) que, per a $n = 0,1,2$ l'afirmació no és certa.

Pas inductiu. Fixem $k \geq 3$, arbitrari. Cal provar: $P(k) \Rightarrow P(k+1)$.

Hipòtesi d'inducció (HI): Suposem que la propietat $P(k)$ és certa per a $k \geq 3$, és a dir, que $k^2-2k-1 \geq 0$.

Aplicant la HI, provarem que la propietat és certa per a $k+1$, és a dir, $(k+1)^2-2(k+1)-1 \geq 0$.

Com aplicar la hipòtesi d'inducció? En aquest cas, es tractaria de manipular convenientment la fórmula $(k+1)^2-2(k+1)-1$ per tal que hi aparegui com a subfórmula justament la de la HI, k^2-2k-1 en aquest cas, i aplicar-hi aleshores la hipòtesi (HI). Vegem-ho en aquest exemple, pensat per a il·lustrar la idea.

Desenvolupant:

$$(k+1)^2-2(k+1)-1 = (k^2+2k+1)-2k-2-1 = \underbrace{(k^2-2k-1)}+(2k-1)$$

Per hipòtesi d'inducció, és $k^2-2k-1 \geq 0$. Pel que fa al segon sumand, $2k-1$, si $k \geq 3$, aleshores $2k-1 \geq 6-1 = 5 > 0$. Per tant, $\underbrace{(k^2-2k-1)}+(2k-1) \geq 0+0 = 0$ i, en conseqüència, $(k+1)^2-2(k+1)-1 \geq 0$. Així, hem demostrat $P(k+1)$ a partir de $P(k)$, és a dir, $P(k) \Rightarrow P(k+1)$, és a dir, el pas inductiu.

Queda demostrada per inducció la propietat.

Es poden aplicar altres tècniques, tot depenent de l'enunciat, com per exemple:

– *Sumar i restar una mateixa expressió*. Vegem, per exemple, l'exemple següent:

PROBLEMA 7.39

Siguin x, y nombres enters, i sigui n un nombre natural, $n \geq 1$. Demostreu per inducció que $x-y|x^n-y^n$.

Observació*: Aquest resultat s'ha obtingut per altres mètodes al capítol 10, sense fer servir el mètode de demostració per inducció. No sempre que un enunciat s'expressa en termes de n natural hem de pensar que només es pot demostrar per inducció.*

Solució. Formalment, cal provar:

$\forall n((n \in \mathbb{N} \wedge n \geq 1) \rightarrow x-y|x^n-y^n)$ (fixats x, y).

La propietat que s'ha de provar, doncs, és $P(n) := \ x-y|x^n-y^n$, per a tot $n \geq 1$ (fixats x, y).

La demostrarem per inducció sobre n, amb valor inicial $n_0 = 1$.

Com sempre, l'esquema demostratiu consta dels dos passos característics de les demostracions per inducció: el pas bàsic i el pas inductiu.

Pas bàsic. Cal provar que $P(1)$ és cert. És a dir, que $x-y|x^n-y^n$ és cert per a $n=1$, cosa que és una obvietat, ja que $x-y|x^1-y^1 = x-y$ (de fet, hi ha igualtat).

Pas inductiu. Cal provar $P(n) \Rightarrow P(n+1)$, per a tot n natural, $n \geq 1$. Concretant a l'enunciat, cal provar:

$x-y|x^n-y^n \Rightarrow x-y|x^{n+1}-y^{n+1}$, per a tot $n \geq 1$.

La suposició de veracitat de $P(n)$, és a dir, $x-y|x^n-y^n$, en el marc del condicional és la hipòtesi d'inducció (HI). En aquest tipus de problemes, una de les dificultats és com aplicar la HI. Com veurem en aquest exemple, de vegades és convenient introduir algun artifici.

La hipòtesi d'inducció es pot reformular com: existeix $k \in \mathbb{Z}$ tal que $x^n-y^n = k(x-y)$.

En aquesta mateixa línia, hem de demostrar que existeix $k' \in \mathbb{Z}$ tal que $x^{n+1}-y^{n+1} = k'(x-y)$. És a dir,

$\exists k(k \in \mathbb{Z} \wedge x^n-y^n = k(x-y)) \Rightarrow \exists k'(k' \in \mathbb{Z} \wedge x^{n+1}-y^{n+1} = k'(x-y))$

En efecte, partim de $x^{n+1} - y^{n+1}$:

Sumant i restant una mateixa expressió, podem escriure:

$x^{n+1} - y^{n+1} = x^{n+1} - x^n y + x^n y - y^{n+1} = x^n(x-y) + y(x^n - y^n)$. Aplicant-hi la hipòtesi (HI), existeix k enter tal que

$x^{n+1} - y^{n+1} = x^n(x-y) + y(x^n - y^n) = x^n(x-y) + yk(x-y) = (x^n + yk)(x-y)$. Prenent $k' = x^n + yk$, enter, resulta que existeix un enter k' tal que

$x^{n+1} - y^{n+1} = (x^n + yk)(x-y) = k'(x-y)$.

Queda demostrada la implicació. Això conclou la demostració per inducció.

Observació. Alternativament, podem sumar i restar una altra expressió, diferent de l'anterior, amb la mateixa conclusió final. En efecte:

$x^{n+1} - y^{n+1} = x^{n+1} - y^n x + y^n x - y^{n+1} = x(x^n - y^n) + y^n(x-y)$.

Vegem un exemple addicional sobre les dificultats de relacionar $P(n)$ amb $P(n+1)$, i posteriorment un problema de tipus similar:

Exemple 7.7 Proveu, per inducció sobre $n \geq 1$ (amb valor inicial $n_0 = 1$):

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^n} < 1 + n$$

Millor encara, en termes de sumatoris: $\displaystyle\sum_{k=1}^{2^n} \frac{1}{k} < 1 + n$.

Pas bàsic. Vegem que la propietat és certa per a $n = 1$, cas en què hem de comprovar que $\displaystyle\sum_{k=1}^{2^1} \frac{1}{k} = \frac{1}{1} + \frac{1}{2} < 1 + 1$, que és obvi.

Pas inductiu. Fixat n, provem que $P(n) \Rightarrow P(n+1)$, on

$P(n)$ és $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^n} < 1 + n$.

És molt fàcil caure en l'*error* de pensar que

$P(n+1)$ és $1 + \frac{1}{2} + \cdots + \frac{1}{2^{n+1}} = 1 + \frac{1}{2} + \cdots + \frac{1}{2^n} + \frac{1}{2^{n+1}}$

Faltarien molts de sumands intermedis; els denominadors no són potències de 2; són els nombres naturals consecutius $1, 2, 3, 4, \ldots$, fins a arribar a 2^n, és a dir, $1, 2, 3, \cdots, k, \cdots, 2^n$, amb terme general el sumand $\frac{1}{k}$. De manera que l'enunciat és

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k}+\cdots+\frac{1}{2^n-2}+\frac{1}{2^n-1}+\frac{1}{2^n}<1+n$$

Vegem amb més detall l'expressió:

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k}+\cdots+\frac{1}{2^{n-1}}+\frac{1}{2^{n-1}+1}+\frac{1}{2^{n-1}+2}+\ldots+\frac{1}{2^{n-1}+(2^{n-1}-1)}+\frac{1}{2^n}$$

L'últim sumand és $\frac{1}{2^{(n-1)}+2^{(n-1)}}=\frac{1}{2\cdot 2^{(n-1)}}=\frac{1}{2^{1+(n-1)}}=\frac{1}{2^n}$

O bé:

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

ja que $2^n+2^n=2\cdot 2^n=2^{n+1}$. De manera que cal sumar 2^n sumands; el nombre de sumands l'obtenim per simple inspecció visual o per $2^{n+1}-2^n=2^n(2-1)=2^n$ (o $2^{n+1}=2\cdot 2^n=2^n+2^n$).

Cal veure $\sum_{k=1}^{2^n}\frac{1}{k}\overset{HI}{<}1+n\Rightarrow\sum_{k=1}^{2^{n+1}}\frac{1}{k}<1+(n+1)$.

Escrivim:

$$\sum_{k=1}^{2^{n+1}}\frac{1}{k}=(\sum_{k=1}^{2^n}\frac{1}{k})+(\frac{1}{2^n+1}+\frac{1}{2^n+2}+\frac{1}{2^n+3}+\cdots+\frac{1}{2^n+2^n})=$$

$$(\sum_{k=1}^{2^n}\frac{1}{k})+(\frac{1}{2^n+1}+\frac{1}{2^n+2}+\frac{1}{2^n+3}+\cdots+\frac{1}{2\cdot 2^n})=$$

$$(\sum_{k=1}^{2^n}\frac{1}{k})+(\frac{1}{2^n+1}+\frac{1}{2^n+2}+\frac{1}{2^n+3}+\cdots+\frac{1}{2^{n+1}})$$

Aplicant-hi la HI,

$$\sum_{k=1}^{2^{n+1}}\frac{1}{k}<1+n+(\frac{1}{2^n+1}+\frac{1}{2^n+2}+\frac{1}{2^n+3}+\cdots+\frac{1}{2^{n+1}}).$$

Si fos $(\frac{1}{2^n+1}+\frac{1}{2^n+2}+\frac{1}{2^n+3}+\overset{2^n}{\overbrace{\cdots}}+\frac{1}{2^{n+1}})<1$, el problema quedaria resolt ja que aleshores seria:

$$\sum_{k=1}^{2^{n+1}}\frac{1}{k}<(1+n)+(\frac{1}{2^n+1}+\frac{1}{2^n+2}+\frac{1}{2^n+3}+\cdots+\frac{1}{2^{n+1}})<(1+n)+1=1+(n+1).$$

Vegem que, en efecte, és així.

Analitzem l'expressió: essent els 2^n sumands de la forma $\frac{1}{2^n+j}$, per a $1 \le j \le 2^n$, el sumand més gran és $\frac{1}{2^n+j}$ per a $j=1$, i així resulta:

$$\frac{1}{2^n+1}+\frac{1}{2^n+2}+\frac{1}{2^n+3}+\cdots+\frac{1}{2^{n+1}} < \frac{1}{2^n+1}+\cdots+\frac{1}{2^n+1} = 2^n\frac{1}{2^n+1} = \frac{2^n}{2^n+1} < 1.$$

Això conclou la demostració. ■

PROBLEMA 7.40

Proveu per inducció sobre $n \ge 1$ (amb valor inicial $n_0 = 1$):

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{3^n} < 1+2n$$

Solució. Cal veure $\sum_{k=1}^{3^n}\frac{1}{k} < 1+2n$.

Pas bàsic. Cal veure que $\sum_{k=1}^{3^1}\frac{1}{k} < 1+2\cdot 1 = 3$, és a dir, $1+\frac{1}{2}+\frac{1}{3} < 1+2 = 3$, que és obvi.

Pas inductiu. Fixat n, cal veure $\sum_{k=1}^{3^n}\frac{1}{k} < 1+2n \Rightarrow \sum_{k=1}^{3^{n+1}}\frac{1}{k} < 1+2(n+1)$, i això per a tot $n \ge 1$.

La HI (hipòtesi d'inducció) és $\sum_{k=1}^{3^n}\frac{1}{k} < 1+2n$.

Escrivim

$$\sum_{k=1}^{3^{n+1}}\frac{1}{k} = \left(\sum_{k=1}^{3^n}\frac{1}{k}\right)+\left(\frac{1}{3^n+1}+\cdots+\frac{1}{3^{n+1}}\right) < (1+2n)+\left(\frac{1}{3^n+1}+\cdots+\frac{1}{3^{n+1}}\right)$$

aplicant-hi la HI.

En el segon parèntesi, hi ha $3^{n+1}-3^n = 3^n(3-1) = 2\cdot 3^n$ sumands,

$$\frac{1}{3^n+1},\ldots,\frac{1}{3^n+3^n+3^n} = \frac{1}{3^n+2\cdot 3^n},$$

tots ells menors que el més gran (corresponent a denominador mínim), que és $\frac{1}{3^n+1}$.

Per tant:

$$(\frac{1}{3^n+1}+\cdots+\frac{1}{3^{n+1}}) < \frac{1}{3^n+1}+\cdots+\frac{1}{3^n+1} = 2\cdot 3^n\frac{1}{3^n+1} = 2\frac{3^n}{3^n+1} < 2.$$

Així:

$\sum_{k=1}^{3^{n+1}}\frac{1}{k} < (1+2n)+(\frac{1}{3^n+1}+\cdots+\frac{1}{3^{n+1}}) < (1+2n)+2 = 1+2(n+1)$, com havíem de demostrar.

7.5. Ampliacions, observacions i enunciats diversos

1. A la descripció del mètode d'inducció, s'ha indicat el cas més habitual, en què s'ha de demostrar una propietat $P(n)$ per a tot nombre natural $n \geq n_0$, amb n_0 natural. Es demostra la propietat per al conjunt $n_0, n_0+1, n_0+2, \cdots$. Per exemple, si $n_0 = 2$, resulta demostrat per al conjunt $2,3,4,5,6,7,\cdots$.

   El que és important és que aquests conjunts tenen *primer element*. Això permet estendre el mètode d'inducció a conjunts d'enters a partir d'un cert enter en endavant. Per exemple, si $m_0 \in \mathbb{Z}$, aleshores el conjunt $m_0, m_0+1, m_0+2, \cdots, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots$ és un conjunt amb primer element, m_0, i es pot plantejar la demostració per inducció d'una propietat $P(n)$ per als enters (naturals inclosos) a partir de m_0.

   Vegem un enunciat d'aquest tipus, amb $m \in \mathbb{Z}$:

   $m \geq -3 \Rightarrow 3m^3+21m+37 \geq 0$

2. Com enfocar la demostració per inducció de resultats del tipus:

   $$1 < \frac{1}{n+1}+\cdots+\frac{1}{3n+1} < 2,$$

   per a tota $n \geq 1$?

   En realitat es tracta de demostrar dues propietats per separat, per inducció:

   Propietat 1: $1 < \frac{1}{n+1}+\cdots+\frac{1}{3n+1}$

   Propietat 2: $\frac{1}{n+1}+\cdots+\frac{1}{3n+1} < 2$

   Vegem-ne un parell més:

   $$1^2+2^2+3^2+\cdots+(n-1)^2 < \frac{n^3}{3} < 1^2+2^2+3^2+\cdots+n^2$$

   $$1^3+2^3+3^3+\cdots+(n-1)^3 < \frac{n^4}{4} < 1^3+2^3+3^3+\cdots+n^3$$

Vegem la resolució de la primera:

$$1^2+2^2+3^2+\cdots+(n-1)^2<\frac{n^3}{3}<1^2+2^2+3^2+\cdots+n^2.$$

PROBLEMA 7.41

Demostreu per inducció que, per a cada nombre n natural, $n \geq 2$, es compleix:

$$1^2+2^2+3^2+\cdots+(n-1)^2<\frac{n^3}{3}<1^2+2^2+3^2+\cdots+n^2$$

Solució. Es tracta de resoldre amb demostracions per inducció dos problemes independents:

PROBLEMA 1. Per a tot n natural, amb $n \geq 2$,

$$\frac{n^3}{3}<1^2+2^2+3^2+\cdots+n^2.$$

$$P(n):\frac{n^3}{3}<1^2+2^2+3^2+\cdots+n^2.$$

PROBLEMA 2. Per a tot n natural, amb $n \geq 2$,

$$1^2+2^2+3^2+\cdots+(n-1)^2<\frac{n^3}{3}.$$

$$Q(n):1^2+2^2+3^2+\cdots+(n-1)^2<\frac{n^3}{3}.$$

Es resoldran separadament, per inducció sobre n. Seran també exemples de demostracions per inducció de propietats amb desigualtats.

Resolució del problema 1. Es pot demostrar amb el valor inicial $n_0=1$.

Pas bàsic. Cal veure $\frac{n^3}{3}<\sum_{k=1}^{n}k^2$ per a $n=1$. El membre de l'esquerra de la desigualtat que es vol comprovar, per a $n=1$, és $\frac{n^3}{3}=\frac{1}{3}$. El membre de la dreta és $\sum_{k=1}^{n}k^2=\sum_{k=1}^{1}k^2=1^2=1$. Per tant, $P(1)$ és cert.

Pas inductiu. Fixem $n \geq 1$ arbitrari. Cal provar:

$P(n) \Rightarrow P(n+1), \forall n \geq 1$. És a dir, concretant:

$$\frac{n^3}{3}\overset{HI}{<}1^2+2^2+3^2+\cdots+n^2 \Rightarrow \frac{(n+1)^3}{3}<1^2+2^2+3^2+\cdots+n^2+(n+1)^2$$

Considerem el terme de la dreta i hi apliquem la hipòtesi d'inducció:

$$1^2+2^2+3^2+\cdots+n^2+(n+1)^2=(1^2+2^2+3^2+\cdots+n^2)+(n+1)^2 \overset{HI}{>} \frac{n^3}{3}+(n+1)^2.$$

Si fos $\frac{n^3}{3}+(n+1)^2 \overset{?}{>} \frac{(n+1)^3}{3}$, hauríem resolt el problema. Estudiem aquesta hipotètica desigualtat, que no sabem si és certa:

$\frac{n^3}{3}+(n+1)^2 \overset{?}{>} \frac{(n+1)^3}{3}$, que equival a

$\frac{n^3}{3}+(n+1)^2 \overset{?}{>} \frac{1}{3}(n^3+3n^2+3n+1)$, que equival a

$\frac{n^3}{3}+(n+1)^2 \overset{?}{>} \frac{n^3}{3}+\frac{1}{3}(3n^2+3n+1)$, que equival a

$(n+1)^2 \overset{?}{>} \frac{1}{3}(3n^2+3n+1)$, que equival a

$n^2+2n+1 \overset{?}{>} n^2+n+\frac{1}{3}$, que equival a

$n+1 \overset{?}{>} \frac{1}{3}$.

Però aquesta última desigualtat és certa, ja que: $n \geq 1 \Rightarrow n+1 > 1+1 = 2 > \frac{1}{3}$.

Per tant, a partir d'aquesta última, i per les equivalències, totes les desigualtats anteriors són certes; en particular, la primera, que és la que ens calia.

Encara que hi hagi equivalències, l'esquema demostratiu que aprofitem és el de les implicacions "cap amunt":

$$\frac{n^3}{3}+(n+1)^2 > \frac{(n+1)^3}{3}$$
$$\Uparrow$$
$$\frac{n^3}{3}+(n+1)^2 > \frac{1}{3}(n^3+3n^2+3n+1)$$
$$\Uparrow$$
$$\frac{n^3}{3}+(n+1)^2 > \frac{1}{n^3}+\frac{1}{3}(3n^2+3n+1)$$
$$\Uparrow$$
$$(n+1)^2 > \frac{1}{3}(3n^2+3n+1)$$
$$\Uparrow$$
$$n^2+2n+1 > n^2+n+\frac{1}{3}$$
$$\Uparrow$$
$$n+1 > \frac{1}{3}.$$

O refem l'exposició amb les implicacions "cap avall".

Això acaba la demostració del pas inductiu i completa la demostració per inducció.

Resolució del problema 2. En termes de sumatoris, és: $\sum_{k=1}^{n-1} k^2 < \frac{n^3}{3}$. En aquest problema, el valor inicial és $n_0 = 2$.

Observació: De fet, es podria considerar $n_0 = 1$, però aleshores hauríem de reformular l'enunciat:

$$0^2 + 1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 < \frac{n^3}{3}.$$

Pas bàsic. Cal veure $1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 < \frac{n^3}{3}$ per a $n = 2$, és a dir, $\sum_{k=1}^{n-1} k^2 < \frac{n^3}{3}$ per a $n = 2$. Per a $n = 2$, el membre de l'esquerra és $\sum_{k=1}^{n-1} k^2 = \sum_{k=1}^{2-1} k^2 = \sum_{k=1}^{1} k^2 = 1^2 = 1$; pel mateix valor $n = 2$, el de la dreta és $\frac{n^3}{3} = \frac{2^3}{3} = \frac{8}{3} > 1$. Per tant, $\sum_{k=1}^{n-1} k^2 < \frac{n^3}{3}$ per a $n = 2$.

Pas inductiu. Cal veure $Q(n) \Rightarrow Q(n+1)$, per a tot $n \geq 2$, és a dir, concretant,

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \overset{HI}{<} \frac{n^3}{3} \Rightarrow 1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 + n^2 < \frac{(n+1)^3}{3}$$

per a tot $n \geq 2$ (però ara amb n fix).

Aplicant la hipòtesi d'inducció (HI):

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 + n^2 < \frac{n^3}{3} + n^2.$$

Si fos $\frac{n^3}{3} + n^2 < \frac{(n+1)^3}{3}$, hauríem resolt el problema, ja que aleshores tindríem:

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 + n^2 < \frac{n^3}{3} + n^2 < \frac{(n+1)^3}{3}, \text{ d'on}$$

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 + n^2 < \frac{(n+1)^3}{3}.$$

Vegem, doncs, si és cert $\frac{n^3}{3} + n^2 \overset{?}{<} \frac{(n+1)^3}{3}$.

Efectuant càlculs, la desigualtat anterior, per demostrar, equival a

$\frac{n^3}{3} + n^2 \overset{?}{<} \frac{1}{3}(n^3 + 3n^2 + 3n + 1)$, que equival a

$\frac{n^3}{3} + n^2 \overset{?}{<} \frac{n^3}{3} + n^2 + n + \frac{1}{3}$, que equival a

$0 \overset{?}{<} n + \frac{1}{3}$, que és obvi.

Per aquest encadenament d'equivalències, resulta certa la desigualtat

$\frac{n^3}{3} + n^2 < \frac{(n+1)^3}{3}$, que és el que volíem provar.

Això acaba el pas inductiu i completa la demostració per inducció.

PROBLEMA 7.42

Demostreu per inducció que el producte de n ≥ 2 *nombres naturals senars qualssevol és senar.*

Observació. *La propietat és vàlida per a enters.*

Solució. En aquest enunciat, n és un nombre natural. Fem la demostració per inducció sobre n, amb valor inicial $n_0 = 2$.

Resultat auxiliar: "El producte de dos nombres enters senars és senar".

Per presentar una modalitat argumental, demostrem a part que el producte de *dos* nombres enters senars també és senar. De fet, s'ha provat en capítols anteriors (preliminars), i fins i tot es podria considerar un resultat "general" disponible; en cas que no es consideri així, és el pas bàsic (per a nombres naturals) i allà s'ha de demostrar explícitament.

Formulació de la propietat (fórmula de predicats):

$\forall c \forall d((c \in \mathbb{Z} \wedge c \in \mathbb{Z}) \rightarrow ((2 \nmid c \wedge 2 \nmid d) \rightarrow 2 \nmid cd))$

Si queda sobreentès que c, d són enters, aleshores:

$\forall c \forall d((2 \nmid c \wedge 2 \nmid d) \rightarrow 2 \nmid cd)$

És a dir, fixats c, d nombres enters, $(2 \nmid c \wedge 2 \nmid d) \rightarrow 2 \nmid cd$.

En efecte, com que són senars, existeixen enters r, s adequats tals que $c = 2r + 1$, $d = 2s + 1$. Vegem que cd es pot escriure com a nombre senar: $cd = (2r+1)(2s+1) = 4rs + 2r + +2s + 1 = 2(2rs + r + s) + 1$. Prenent $w = 2rs + r + s \in \mathbb{Z}$, resulta que $cd = 2w + 1$, senar.

Demostració per inducció

Pas bàsic. "El producte de dos nombres naturals senars qualssevol és un nombre senar". Formalment:

$\forall c \forall d((c \text{ senar } \wedge d \text{ senar }) \rightarrow cd \text{ senar }).$

Observeu que aquest és un exemple en el qual el pas bàsic no és trivial, en el sentit d'una simple comprovació, sinó que cal fer una demostració. En aquest cas, o bé reproduïm aquí, a efectes de completesa, la demostració del "resultat auxiliar" que s'ha fet anteriorment o simplement l'utilitzem com a resultat disponible.

Reproduïm la prova:

$$\left.\begin{array}{l} 2 \nmid c \Rightarrow \exists k\ (c = 2k+1) \\ 2 \nmid d \Rightarrow \exists k'\ (d = 2k'+1) \end{array}\right\} \Rightarrow \exists k \exists k' (cd = (2k+1)(2k'+1))$$

Resulta $cd = (2k+1)(2k'+1) = 4kk' + 2k + 2k' + 1 = 2(2kk' + k + k') + 1$; amb $k'' = 2kk' + k + k'$, podem escriure:

$$\left.\begin{array}{l} 2 \nmid c \Rightarrow \exists k(c = 2k+1) \\ 2 \nmid d \Rightarrow \exists k'(d = 2k'+1) \end{array}\right\} \Rightarrow \exists k''(cd = 2k''+1) \Rightarrow 2 \nmid cd.$$

Pas inductiu. Cal provar: "Si el producte de $n \geq 2$ naturals senars qualssevol és senar, aleshores el producte de $n+1$ naturals senars qualssevol és un nombre senar".

La hipòtesi d'inducció és, en el marc del condicional anterior, "el producte de $n \geq 2$ naturals senars qualssevol és senar".

Fixem n, d'altra banda arbitrari. Siguin $b_1, \cdots, b_{n+1}$ $n+1$ nombres naturals senars qualssevol, ara fixos per a la resta de la demostració. Escrivim $p_{n+1} = b_1 \cdots b_{n+1} = (b_1 \cdots b_n) \cdot b_{n+1}$, per associativitat. Però $b_1 \cdots b_n$ és un producte de n nombres senars; *per hipòtesi d'inducció*, és $p_n = b_1 \cdots b_n$ senar. Ara tenim $p_{n+1} = p_n \cdot b_{n+1}$, producte de dos nombres naturals senars. Aplicant el resultat auxiliar del principi, o el pas bàsic, és $p_n b_{n+1}$ un nombre senar, és a dir, $p_{n+1} = b_1 \cdots b_{n+1}$ és senar.

Queda demostrada la propietat per inducció.

Observació. Una altra variant argumental consistiria a demostrar el pas bàsic $P(2)$: "El producte de dos nombres naturals senars és senar", integrant *aquí* la demostració del "resultat auxiliar". Però, aleshores, en el pas inductiu necessitem utilitzar $P(2)$, de manera que l'esquema del pas inductiu seria $(P(2) \wedge P(n)) \Rightarrow P(n+1)$, on:

$P(n)$: "El producte de $n \geq 2$ naturals senars és un enter senar" (hipòtesi d'inducció)

$P(n+1)$: "El producte de $n+1 \geq 2$ naturals senars és un enter senar".

Ho podríem considerar com un cas especial de demostració per inducció completa, basada en l'esquema demostratiu del pas inductiu $(P(2) \wedge \cdots \wedge P(n-1) \wedge P(n)) \Rightarrow P(n+1)$, però en què només fem servir $P(2)$ i $P(n)$.

Observació. En aquest exercici, s'han descrit les propietats, la hipòtesi d'inducció i el pas inductiu de forma verbal, pràcticament de llenguatge natural. A continuació presentem un grau major de formalització.

Propietat completament expressada:

$\forall n((n \in \mathbb{N} \wedge n \geq 2) \rightarrow \forall a_1 \cdots \forall a_n((a_1 \in \mathbb{N} \wedge \cdots \wedge a_n \in \mathbb{N}) \rightarrow ((2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_n) \rightarrow 2 \nmid a_1 \cdots a_n)))$

Es pot simplificar si queden sobreentesos els dominis de les variables, o s'expliciten externament:

$\forall n(n \geq 2 \rightarrow \forall a_1 \cdots \forall a_n((2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_n) \rightarrow 2 \nmid a_1 \cdots a_n))$

Fixat $n \geq 2$,

$P(n): \forall a_1 \cdots \forall a_n((2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_n) \rightarrow 2 \nmid a_1 \cdots a_n)$ (HI)

$P(n+1): \forall b_1 \cdots \forall b_{n+1}((2 \nmid b_1 \wedge \cdots \wedge 2 \nmid b_{n+1}) \rightarrow 2 \nmid b_1 \cdots b_{n+1})$.

El pas inductiu consistiria a provar:

$\forall a_1 \cdots \forall a_n((2 \nmid a_1 \wedge \cdots \wedge 2 \nmid a_n) \rightarrow 2 \nmid a_1 \cdots a_n) \Rightarrow \forall b_1 \cdots \forall b_{n+1}((2 \nmid b_1 \wedge \cdots \wedge 2 \nmid b_{n+1}) \rightarrow 2 \nmid b_1 \cdots b_{n+1})$.

En efecte, siguin $b_1, \cdots, b_{n+1}$ nombres naturals senars. És $b_1 \cdots b_{n+1} = b_1 \cdots b_n b_{n+1} = (b_1 \cdots b_n) b_{n+1}$. *Com aplicar la HI?* Escollim $a_1 = b_1, \cdots a_n = b_a$. Donat que els $b_1, \cdots, b_n$ són senars, també ho són $a_1, \cdots, a_n$. En aplicació de la hipòtesi d'inducció, també és senar el producte $a_1 \cdots a_n$, que és $b_1 \cdots b_n$. Així doncs, $b_1 \cdots b_{n+1} = (b_1 \cdots b_n) b_{n+1}$ és producte de dos senars, i, per tant, és senar.

Observació. Repetim que aquest és un exemple en el qual el pas bàsic no és trivial, en el sentit d'una simple comprovació.

7.6. Enunciats diversos

Altres demostracions per inducció.

PROBLEMA 7.43

Proveu que, per a tot nombre natural $n \geq 2$ i per a tota col·lecció de funcions $f_1, \cdots, f_n : \mathbb{R} \rightarrow \mathbb{R}$ derivables en qualsevol punt (de manera que existeixen les funcions derivades $f_1', \cdots, f_n'$), es compleix:

a) $f_1 + \cdots + f_n$ *és derivable i* $(f_1 + \cdots + f_n)' = f_1' + \cdots + f_n'$.

b) $f_1 \cdots f_n$ *és derivable i*

$$(f_1 \cdots f_n)' = (f_1' f_2 \cdots f_n) + (f_1 f_2' \cdots f_n) + \cdots + (f_1 f_2 \cdots f_i' \cdots f_n) + \cdots + (f_1 f_2 \cdots f_{n-1} f_n').$$

Solució

Comentaris

1. Aquest problema és un exemple en què el pas bàsic no és trivial i requereix una demostració específica.
2. Abans que res, considerem demostrat:

   Resultat auxiliar 1. f, g són derivables $\Rightarrow f + g$ és derivable i $(f + g)' = f' + g'$

   Resultat auxiliar 2. f, g són derivables $\Rightarrow fg$ és derivable i $(fg)' = f'g + fg'$

   Són resultats de teoria general matemàtica i estan disponibles, en el sentit que no cal demostrar-los aquí. Vegeu qualsevol text bàsic de càlcul en una variable, com [POZO2013].

a) La propietat $P(n)$ que es vol demostrar és:

   "La suma de $n \geq 2$ funcions derivables qualssevol (reals de variable real) és derivable i la seva derivada és la suma de les derivades."

   Si es vol un més gran nivell de formalització, aleshores és convenient introduir, per exemple, el conjunt $D = \{f | f : \mathbb{R} \to \mathbb{R}$ i és derivable$\}$.

   I aleshores, suposant n nombre natural:

$$\forall n (n \geq 2 \to \forall f_1 \cdots \forall f_n ((f_1 \in D \wedge \cdots \wedge f_n \in D) \to (\sum_{k=1}^{n} f_k \in D \wedge (\sum_{k=1}^{n} f_k)' = \sum_{k=1}^{n} f_k')))$$

   La demostració serà per inducció sobre n, amb $n_0 = 2$.

   Pas bàsic, $P(2)$. Cal veure que, per a qualsevol parella ($n = 2$) de funcions derivables f_1, f_2, es compleix que $(f_1 + f_2)$ és derivable i $(f_1 + f_2)' = f_1' + f_2'$. És justament el "resultat auxiliar 1". La demostració és estàndard ([POZO2013]).

   Pas inductiu, $P(n) \Rightarrow P(n+1), \forall n \geq 2$.

   Fixem $n \geq 2$ arbitrari. Cal veure que:

   "Si la suma de n funcions derivables és derivable i la derivada de la suma és suma de derivades, aleshores la suma de $n+1$ funcions derivables és derivable i la derivada de la suma és la suma de les derivades".

Formalment, i per a expressar exactament el que es vol dir:

$P(n)$ (hipòtesi d'inducció):

$\forall f_1 \cdots \forall f_n (\forall i((i \in \mathbb{N} \wedge 1 \leq i \leq n) \to f_i \in D) \to (f_1 + \cdots + f_n \in D \wedge (f_1 + \cdots + f_n)' = f_1' + \cdots + f_n'))$ (HI).

$P(n+1)$ ((tesi d'inducció)):

$\forall g_1 \cdots \forall g_{n+1} (\forall i((i \in \mathbb{N} \wedge 1 \leq i \leq n+1) \to g_i \in D) \to (g_1 + \cdots + g_{n+1} \in D \wedge (g_1 + \cdots + g_{n+1})' = g_1' + \cdots + g_{n+1}'))$.

Formalització alternativa:

$P(n)$ (hipòtesi d'inducció):

$\forall f_1 \cdots \forall f_n ((f_1 \in D \wedge \cdots \wedge f_n \in D) \to (f_1 + \cdots + f_n \in D \wedge (f_1 + \cdots + f_n)' = f_1' + \cdots + f_n'))$ (HI).

$P(n+1)$ (tesi d'inducció):

$\forall g_1 \cdots \forall g_{n+1} ((g_1 \in D \wedge \cdots \wedge g_{n+1} \in D) \to (g_1 + \cdots + g_{n+1} \in D \wedge (g_1 + \cdots + g_{n+1})' = g_1' + \cdots + g_{n+1}'))$.

Demostració del pas inductiu. Cal provar: $P(n) \Rightarrow P(n+1), \forall n \geq 2$.

Siguin $g_1, \cdots, g_{n+1}$ funcions de D (derivables). Per associativitat, podem escriure:

$g_1 + \cdots + g_{n+1} = (g_1 + \cdots + g_n) + g_{n+1}$, expressió com a suma de dues funcions. La primera és suma de n funcions derivables: esperem així poder establir la connexió amb la HI.

Escollint $f_1 = g_1, \cdots, f_n = g_n$ tenim que $f_1, \cdots, f_n$ són derivables i, per HI, $f_1 + \cdots + f_n$ és derivable, amb $(f_1 + \cdots + f_n)' = f_1' + \cdots + f_n'$. Per la "propietat auxiliar 1", la suma de les dues funcions $(g_1 + \cdots + g_n) + g_{n+1}$ és derivable i $[(g_1 + \cdots + g_n) + g_{n+1}]' = (g_1 + \cdots + g_n)' + g_{n+1}' = (f_1 + \cdots + f_n)' + g_{n+1}' \overset{(HI)}{=} (f_1' + \cdots + f_n') + g_{n+1}' = (g_1' + \cdots + g_n') + g_{n+1}' = g_1' + \cdots + g_n' + g_{n+1}'$.

Observació. Si no utilitzem el "resultat auxiliar 1", demostrat externament, aleshores cal demostrar-lo en el pas bàsic. Però aleshores, en el pas inductiu, fem servir novament $P(2)$, de manera que es pot considerar que l'esquema demostratiu és $(P(2) \wedge P(n)) \Rightarrow P(n+1)$, o fins i tot inducció completa.

b) La resolució és anàloga a l'apartat anterior. Atès això, en donarem només les idees bàsiques.

Pas bàsic. Cal demostrar l'afirmació per a $n = 2$, que és precisament el "resultat auxiliar 2".

Pas inductiu. Siguin $g_1, \cdots, g_{n+1}$ funcions derivables.

Sigui $g_1 \cdots g_{n+1} = (g_1 \cdots g_n) \cdot g_{n+1}$, expressió com a producte de dues funcions. Denotem $h = g_1 \cdots g_n$, de manera que $g_1 \cdots g_{n+1} = h \cdot g_{n+1}$.

Ara h és el producte de n funcions derivables i li és aplicable, per tant, la hipòtesi d'inducció. Aplicant la HI a la funció $h = g_1 \cdots g_n$, podem afirmar que

– h és derivable (conseqüència 1) i que:

– $h' = (g_1 \cdots g_n)' = (g_1' g_2 \cdots g_n) + (g_1 g_2' \cdots g_n) + \cdots + (g_1 g_2 \cdots g_n')$ (conseqüència 2).

Essent h derivable (conseqüència 1 de la HI) i, pel "resultat auxiliar 2", és $(g_1 \cdots g_n) \cdot g_{n+1} = hg_{n+1}$ derivable i

$[(g_1 \cdots g_n) \cdot g_{n+1}]' = (hg_{n+1})' = h'g_{n+1} + hg_{n+1}'$. I així resulta que $g_1 \cdots g_{n+1}$ és derivable, amb derivada $(g_1 \cdots g_{n+1})' = h'g_{n+1} + hg_{n+1}'$.

Aplicant novament la HI (conseqüència 2):

$$\begin{aligned}
&(g_1 \cdots g_{n+1})' = h'g_{n+1} + hg_{n+1}' \stackrel{(HI)}{=} \\
&= (g_1' g_2 \cdots g_n + g_1 g_2' \cdots g_n + \cdots + g_1 g_2 \cdots g_n') g_{n+1} + (g_1 \cdots g_n) g_{n+1}' = \\
&= (g_1' g_2 \cdots g_n g_{n+1} + g_1 g_2' \cdots g_n g_{n+1} + \cdots + g_1 g_2 \cdots g_n' g_{n+1}) + g_1 \cdots g_n g_{n+1}' = \\
&= g_1' g_2 \cdots g_n g_{n+1} + g_1 g_2' \cdots g_n g_{n+1} + \cdots + g_1 g_2 \cdots g_n' g_{n+1} + g_1 \cdots g_n g_{n+1}',
\end{aligned}$$

com s'havia de veure.

Si $g(x) = \sin x$, les derivades successives (d'ordre n) són:

$g'(x) = \cos x$ $(n = 1)$,
$g''(x) = -\sin x$ $(n = 2)$,
$g'''(x) = -\cos x$ $(n = 3)$,
$g''''(x) = \sin x$ $(n = 4)$,

amb repetició cada quatre vegades. Es pot expressar en termes del residu de la divisió entera de n entre 4 en què tenim quatre casos possibles: $n = 4q = 4q + 0$ o $n = 4q + 1$ o $n = 4q + 2$ o $n = 4q + 3$. Tot nombre enter és d'alguna d'aquestes formes, per a algun enter q convenient.

Anàlogament per a d'altres funcions: $\cos x$, $x \cos x$. Per exemple, si $f(x) = x \cos x$:

$$\begin{aligned}
f'(x) &= \cos x - x \sin x \\
f''(x) &= -\sin x - (\sin x + x \cos x) = -2\sin x - x \cos x \\
f'''(x) &= -2\cos x - (\cos x - x \sin x) = -3\cos x + x \sin x \\
f''''(x) &= 3\sin x + (\sin x + x \cos x) = 4\sin x + x \cos x
\end{aligned}$$

Observem que, amb $f^{(5)}$, tornem a obtenir el mateix patró que f' (i així successivament):

$$f^{(5)}(x) = 4\cos x + (\cos x - x\sin x) = 5\cos x - x\sin x$$
$$f^{(6)}(x) = -5\sin x - (\sin x + x\cos x) = -6\sin x - x\cos x$$

Aquest és un exemple en què es mostra que és possible haver de demostrar el pas inductiu per mètodes no directes. En particular, convé fer la demostració per casos, en aquest exemple.

PROBLEMA 7.44

Sigui $f(x) = x\cos x$. Demostreu per inducció que les derivades successives de f són, per a $n \geq 1$:

$$f^{(n)}(x) = \begin{cases} n\sin x + x\cos x & \textit{si } n = 4q+0 \textit{ per a algun } q \textit{ enter} \\ n\cos x - x\sin x & \textit{si } n = 4q+1 \textit{ per a algun } q \textit{ enter} \\ -n\sin x - x\cos x & \textit{si } n = 4q+2 \textit{ per a algun } q \textit{ enter} \\ -n\cos x + x\sin x & \textit{si } n = 4q+3 \textit{ per a algun } q \textit{ enter} \end{cases}$$

Solució. La propietat $P(n)$ és la igualtat anterior, per a tot $n \geq 1$. Vegeu que hi ha diversos casos o tipus:

Tipus 1. Suposem $n = 4q$ per a un q enter adequat.

Tipus 2. Suposem $n = 4q+1$ per a un q enter adequat.

Tipus 3. Suposem $n = 4q+2$ per a un q enter adequat.

Tipus 4. Suposem $n = 4q+3$ per a un q enter adequat.

Pas bàsic. Cal provar la propietat per a $n = n_0 = 1$. És $1 = 0 \cdot 4 + 1$, de manera que correspon al tipus segon, i hem de veure, doncs, que $f'(x) = n\cos x - x\sin x$, per a $n = 1$. En efecte, $f'(x) = (x\cos x)' = \cos x - x\sin x = 1 \cdot \cos x - x\sin x$.

Pas inductiu. Cal demostrar $P(n) \Rightarrow P(n+1)$, per a tot $n \geq 1$ ($n_0 = 1$). Fem la demostració per casos, atesa la formulació en termes de casos:

Cas 1. Suposem $n = 4q$ per a un q enter adequat. Aleshores, $n+1 = 4q+1$ (segon tipus). Per tant, hem de veure:

$f^{(n)}(x) \overset{HI}{=} n\sin x + x\cos x \Rightarrow f^{(n+1)}(x) = (n+1)\cos x - x\sin x$. En efecte:

$f^{n+1}(x) = (f^n)'(x) = (f^n(x))' \overset{HI}{=} (n\sin x + x\cos x)' = n\cos x + (\cos x - x\sin x) = (n+1)\cos x - x\sin x$.

Cas 2. Suposem $n = 4q + 1$ per a un q enter adequat. Aleshores $n + 1 = 4q + 2$ (tercer tipus). Per tant, hem de veure:

$f^n(x) \overset{HI}{=} n\cos x - x\sin x \Rightarrow f^{n+1}(x) = -(n+1)\sin x - x\cos x$. En efecte:

$f^{n+1}(x) = (f^n)'(x) = (f^n(x))' \overset{HI}{=} (n\cos x - x\sin x)'$
$= -n\sin x - (\sin x + x\cos x) = -(n+1)\sin x - x\cos x$.

Cas 3. Suposem $n = 4q + 2$ per a un q enter adequat. Aleshores $n + 1 = 4q + 3$ (quart tipus). Per tant, hem de veure:

$f^n(x) \overset{HI}{=} -n\sin x - x\cos x \Rightarrow f^{n+1}(x) = -(n+1)\cos x - x\sin x$. En efecte:

$f^{n+1}(x) = (f^n)'(x) = (f^n(x))' \overset{HI}{=} (-n\sin x - x\cos x)'$
$= -n\cos x - (\cos x - x\sin x) = -(n+1)\cos x - x\sin x$.

Cas 4. Suposem $n = 4q + 3$ per a un q enter adequat. Aleshores $n + 1 = 4q + 4 = 4t$ (primer tipus). Per tant, hem de veure:

$f^n(x) \overset{HI}{=} -n\cos x + x\sin x \Rightarrow f^{n+1}(x) = -(n+1)\sin x - x\cos x$. En efecte,

$f^{n+1}(x) = (f^n)'(x) = (f^n(x))' \overset{HI}{=} (-n\cos x + x\sin x)'$
$= n\sin x + (\sin x + x\cos x) = (n+1)\sin x + x\cos x$.

Exercici/exemple addicional similar. Considereu $h(x) = x\sin x$. Tenim algunes derivades successives:

$h'(x) = \sin x + x\cos x$
$h''(x) = \cos x + (\cos x - x\sin x) = 2\cos x - x\sin x$
$h'''(x) = -2\sin x - (\sin x + x\cos x) = -3\sin x - x\cos x$
$h^{(iv)}(x) = -3\cos x - (\cos x - x\sin x) = -4\cos x + x\sin x\, h^{(v)}(x) = 4\sin x + (\sin x + x\cos x) =$
$5\sin x + x\cos x$

Aleshores, si n és un natural positiu, quina és la fórmula general de la derivada d'ordre n i com es pot demostrar?

Podeu trobar altres demostracions per inducció en diversos exercicis de la resta de capítols.

→ 8

Conjunts

8.1. Conjunts i elements, relació de pertinença

Què és un conjunt (noció intuïtiva)

Donem la idea de conjunt de manera intuïtiva.

> Un conjunt és:
>
> – una col·lecció d'objectes de manera que
> – l'ordre no importa i
> – no s'admeten repeticions.

Els objectes que el formen són els ***elements*** d'un conjunt. Un conjunt el determinen els seus elements. Allò que caracteritza un conjunt són els seus elements, encara que el conjunt es pugui definir de maneres diverses.

La notació per a expressar un conjunt és $\{\ldots\}$.

Exemple 8.1

▷ $\{0,1,2,3,4,5,6,7,8,9\}$ és el conjunt dels dígits decimals,

▷ $\{a,e,i,o,u\}$ és el conjunt de les vocals del nostre alfabet. ■

No hi ha repeticions, de manera que són el mateix conjunt els següents: $\{a,a,b\}$ i $\{a,b\}$ (són iguals, cosa que expressem com $\{a,a,b\} = \{a,b\}$). Així, les eventuals repeticions d'objectes s'identifiquen a un únic objecte o element.

L'ordre no importa: els conjunts $\{2,-2\}$, $\{-2,2\}$ són el mateix (són iguals, cosa que expressem $\{2,-2\} = \{-2,2\}$). Només importa quins elements el formen, no en quin ordre. Això no és contradictori amb el fet que, per a descriure un conjunt, de vegades s'hagi de donar ordenadament en una llista: conceptualment, no hi ha cap ordre i qualsevol reordenació produeix el mateix conjunt.

Observeu que hi ha objectes (o, pensant més en el terreny de la informàtica, de les estructures de dades) que no són conjunts, com per exemple les llistes o les cadenes de caràcters. Per exemple, en una cadena binària 1100011100, l'ordre importa i s'admeten repeticions. També a les paraules ordinàries sobre un alfabet: a "MISSISSIPPI" no podem suprimir les repeticions ni canviar l'ordre. No tota llista és un conjunt: per exemple, un polígon pot descriure's mitjançant una llista ordenada dels seus vèrtexs: $[P_1, P_2, \cdots, P_n]$, en què l'ordre importa.

Hi ha d'altres situacions en què no hi ha repeticions, però importa l'ordre, com en el cas de les permutacions. Una permutació no és, doncs, un conjunt.

Resulta útil fer assignacions com

$A = \{1,2,4\}$

$B = \{a,b,c\}$

i així poder-nos-hi referir.

Recordem que disposem de notacions estàndard per als conjunts numèrics:

$\mathbb{N}$: el conjunt dels nombres naturals,

$\mathbb{Z}$: el conjunt dels nombres enters,

$\mathbb{Q}$: el conjunt dels nombres racionals,

$\mathbb{R}$: el conjunt dels nombres reals,

$\mathbb{C}$: el conjunt dels nombres complexos.

Element, pertinença a un conjunt, no-pertinença

Els objectes que formen un conjunt són els seus *elements*. La notació per a expressar que *a és un element del conjunt A* és $a \in A$; es diu també que *a pertany a A*. Així, si $A = \{1,2,w,z\}$, tindrem que $1 \in A$, $2 \in A$, $w \in A$, $z \in A$.

Si un objecte *x no és element d'un conjunt C*, és a dir, no hi pertany, ho expressem amb la notació $x \notin C$. A l'exemple anterior, $4 \notin A$, $t \notin A$. Altres exemples: $-2 \notin \mathbb{N}$, $\sqrt{2} \notin \mathbb{Q}$, però $\sqrt{2} \in \mathbb{R}$.

Vegem-ne alguns exemples addicionals:

Exemples 8.2

Exemple 1. Considerem $A = \{1,2,\{3,5,a\},w,z,\{\{t\}\}\}$.

Observem que hi ha elements a A que, per la seva banda, són conjunts; per exemple $\{3,5,a\}$. Però ara això no importa: el paper que juga aquí $\{3,5,a\}$ és el d'element del conjunt A.

Tenim:

$1 \in A$, $2 \in A$, $\{3,5,a\} \in A$, $w \in A$, $z \in A$, $\{\{t\}\} \in A$,
$3 \notin A$, $5 \notin A$, $a \notin A$, $t \notin A$, $\{t\} \notin A$.

Aquest conjunt té sis elements: $1, 2, \{3,5,a\}, w, z, \{\{t\}\}$.

De fet, podria ser perfectament "opac":

$$A = \{1, 2, \boxed{\text{CAIXA1}}, w, z, \boxed{\text{CAIXA2}}\}$$

$$A = \{1, 2, \boxed{\phantom{\text{element1}}}, w, z, \boxed{\phantom{\text{element2}}}\}$$
$$A = \{1, 2, \boxed{\text{element1}}, w, z, \boxed{\text{element2}}\}$$

Exemple 2. $t \notin \{\{t\}\}$,

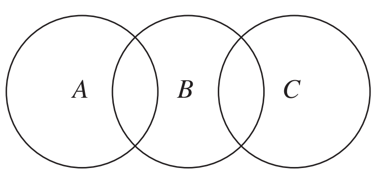
Exemple 3. $\{t\} \in \{\{t\}\}$.

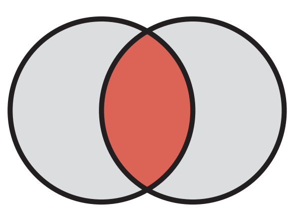
Exemple 4. $x \notin \{\{x, \{x, \{x\}\}\}, \{x\}, \{x, y\}\}$.

Exemple 5. Quants i quins elements té $\{\{\{\{\{a\}\}\}\}\}$? Un únic element, $\{\{\{\{a\}\}\}\}$. ■

Diagrames de Venn

Una possible representació esquemàtica per a conjunts és la dels diagrames de Venn. Cada conjunt es representa per una "rodona" o similar. No és demostratiu, gairebé només expositiu, i encara per a dos, tres i pocs conjunts més. Vegem-ne alguns exemples.





El conjunt buit

Un conjunt especial és el que no conté elements.

Es denota per $\emptyset$ (de fet, $\emptyset = \{\}$). És $\forall x (x \notin \emptyset)$.

Exemple 8.3 Sigui $A = \{1,2,\emptyset,\{\emptyset\}\}$. Aleshores:

$A \neq \emptyset$,

$\emptyset \in A$,

$\{\emptyset\} \in A$,

(vegeu inclusió) $\emptyset \subseteq A$. ■

Exemple 8.4 Indiqueu si són certes les afirmacions següents (formalitzeu-les):

a) Tots els elements del conjunt buit són de color blau.
b) Tots els elements del conjunt buit no són de color blau (o: cap element del conjunt buit és blau).

Per a la formalització, introduïm el predicat $B =$ "ser de color blau" ($B(x)$: "x és de color blau").

Les afirmacions són certes, ja que cap element és de $\emptyset$ i, per tant, és cert que qualsevol element de $\emptyset$ satisfà la propietat (buidament).

També es pot donar un argument formal a través de les simbolitzacions:

a) $\forall x(x \in \emptyset \rightarrow B(x))$.

   Fixat un x (i per a cada x), vegem que $x \in \emptyset \rightarrow B(x)$ és cert. L'afirmació $x \in \emptyset$ és falsa i, per tant, d'acord amb la taula de veritat del condicional, on és $0 \rightarrow *$ és cert, resulta $x \in \emptyset \rightarrow B(x)$ cert. Com que així és per a qualsevol x, l'afirmació $\forall x(x \in \emptyset \rightarrow B(x))$ és certa.

b) $\forall x(x \in \emptyset \rightarrow \neg B(x))$. És cert, exactament per la mateixa argumentació de l'apartat anterior. ■

Definició o descripció de conjunts

Es poden definir conjunts de diverses maneres:

– per extensió, explicitant els elements que formen el conjunt.
– per comprensió, mitjançant la propietat que satisfan els elements del conjunt i només ells, és a dir, la propietat que els caracteritza.

Exemple 8.5 El conjunt dels nombres senars es pot expressar com:

$\{m | \exists k(k \in \mathbb{Z} \wedge m = 2k+1)\}$

o bé (també s'admet) $\{2k+1 | k \in \mathbb{Z}\}$. ■

Vegem un exemple addicional d'aquesta última forma.

Exemple 8.6 Amb

$A = \{(-1)^{2n+2} + (-1)^{5n+2} | n \in \mathbb{N}\}$

volem definir el conjunt dels “elements de la forma $(-1)^{2n+2} + (-1)^{5n+2}$ variant n en el conjunt de (tots) els nombre naturals”. O també:

$A = \{m|$ existeix $n \in \mathbb{N}$ tal que $m = (-1)^{2n+2} + (-1)^{5n+2}\}$ o, més formalitzadament:

$A = \{m | \exists n (n \in \mathbb{N} \wedge m = (-1)^{2n+2} + (-1)^{5n+2})\}$.

$A = \{m | \exists n \in \mathbb{N} (m = (-1)^{2n+2} + (-1)^{5n+2})\}$.

$A = \{m | \exists n \in \mathbb{N}\ m = (-1)^{2n+2} + (-1)^{5n+2}\}$. ■

A la pràctica, encara hi ha altres formes de definir conjunts:

– per recursió, que no tractarem,
– per operacions conjuntistes a partir de conjunts preexistents, i mitjançant fórmules conjuntistes: per exemple, donats A, B, C, formem un nou conjunt mitjançant: $A - (B - C)$ o $A \cup (B \cap C)$, per exemple.

A l’exercici posterior, es presenten exemples de definició per comprensió i es demana la descripció per extensió.

PROBLEMA 8.1

Descriviu els conjunts següents per extensió (és a dir, indicant quins són els seus elements).

a) $\{x \in \mathbb{R} | x^2 = 2\}$
b) $\{x \in \mathbb{R} | x^2 - 3x + 2 = 0\}$
c) $\{x \in \mathbb{R} | x^2 + 2 = 0\}$
d) $\{x \in \mathbb{N} | x^2 = 15\}$
e) $\{x \in \mathbb{N} | x^2 = 4\}$
f) $\{x \in \mathbb{Z} | x^2 = 4\}$
g) $\{1 + (-1)^n | n \in \mathbb{N}\}$
h) $\{3 + (-2)^n | n \in \mathbb{N}\}$
i) $\{n^2 | n \in \{-2, 5, 0, 3\}\}$
j) $\{\frac{1}{n} | n \in \mathbb{N}, 3 < n < 13\}$
k) $\{x \in \mathbb{Q} | x^2 = 7\}$
l) $\{x \in \mathbb{R} | x^2 < -3\}$
m) $\{\frac{1}{n} | n \in \mathbb{N}, 2|n, 4 < n < 16\}$
n) $\{(-1)^n | n \in \mathbb{N}\}$
o) $\{(-1)^n(-1)^{2n} + (-1)^{2n+9} | n \in \mathbb{N}\}$
p) $\{(-1)^n(-1)^{3n+1} + (-1)^{n+2} | n \in \mathbb{N}\}$
q) $\{(-1)^{2n+2} + (-1)^{5n+2} | n \in \mathbb{N}\}$

r) $\{\frac{1}{n} | n \in \mathbb{N}, 2|n, 3 \nmid n, 5 \nmid n, 4 < n < 16\}$

Solució

a) $\{x \in \mathbb{R} | x^2 = 2\} = \{-\sqrt{2}, \sqrt{2}\}$.
b) Es resol l’equació de segon grau en $\mathbb{R}$; el conjunt de les solucions és el que es demana: $\{x \in \mathbb{R} | x^2 - 3x + 2 = 0\} = \{1, 2\}$.

c) $\{x \in \mathbb{R} | x^2 + 2 = 0\} = \emptyset$. En efecte, per a tot nombre real x, és $x^2 \geq 0$. Per tant, $x^2 + 2 \geq 2 > 0$, d'on $x^2 + 2 \neq 0$ per a cada $x \in \mathbb{R}$.

d) $\{x \in \mathbb{N} | x^2 = 15\} = \emptyset$. Les úniques solucions són $\pm\sqrt{15}$, que no són nombres naturals.

e) $\{x \in \mathbb{N} | x^2 = 4\} = \{2\}$.

f) $\{x \in \mathbb{Z} | x^2 = 4\} = \{-2, 2\}$.

g) $\{1 + (-1)^n | n \in \mathbb{N}\}$.

Fem una distinció de paritat per a n: si n és parell, aleshores $(-1)^n = 1$ i serà, per tant, $1 + (-1)^n = 2$; si n és senar, aleshores $(-1)^n = -1$, d'on $1 + (-1)^n = 1 - 1 = 0$. Així, $\{1 + (-1)^n | n \in \mathbb{N}\} = \{0, 2\}$.

h) $\{3 + (-2)^n | n \in \mathbb{N}\}$.

Segons la paritat de n: $(-2)^n = (-1)^n 2^n = 2^n$ si n és parell; $(-2)^n = (-1)^n 2^n = -2^n$ si n és senar. Per tant:

$\{3 + (-2)^n | n \in \mathbb{N}\} = \{3 + 2^n | n \in \mathbb{N}\} \cup \{3 - 2^n | n \in \mathbb{N}\}$ (vegeu l'operació conjuntista de reunió).

i) $\{n^2 | n \in \{-2, 5, 0, 3\}\} = \{(-2)^2, 5^2, 0^2, 3^2\} = \{4, 25, 0, 9\}$.

j) $\{\frac{1}{n} | n \in \mathbb{N}, 4 \leq n \leq 10\} = \{\frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}, \frac{1}{9}, \frac{1}{10}\}$.

k) $\{x \in \mathbb{Q} | x^2 = 7\} = \emptyset$. Les solucions reals $-\sqrt{7}, \sqrt{7}$ són irracionals.

l) $\{x \in \mathbb{R} | x^2 < -3\} = \emptyset$, ja que, per a tot nombre real x, es compleix: $x^2 \geq 0 > -3$.

m) $\{\frac{1}{n} | n \in \mathbb{N}, 2 | n, 3 < n < 13\}$.

Els possibles valors de n són els parells d'entre $4, 5, 6, 7, 8, 9, 10, 11, 12$, és a dir, $4, 6, 8, 10, 12$. Per tant, el conjunt és $\{\frac{1}{4}, \frac{1}{6}, \frac{1}{8}, \frac{1}{10}, \frac{1}{12}\}$.

n) $\{(-1)^n | n \in \mathbb{N}\} = \{-1, 1\}$.

Considerant la paritat de n, si n és parell, $(-1)^n = 1$; si n és senar, $(-1)^n = -1$; d'aquí el resultat.

o) $\{(-1)^n (-1)^{2n} + (-1)^{2n+9} | n \in \mathbb{N}\}$.

El nombre $2n + 9$, suma de parell i senar, és senar. El nombre $2n$ és parell per a qualsevol n. Per tant, $(-1)^n (-1)^{2n} + (-1)^{2n+9} = (-1)^n + 1 + (-1) = (-1)^n$. Segons la paritat de n: $(-1)^n = 1$ si n és parell, i $(-1)^n = -1$ si n és senar. Per tant, $\{(-1)^n (-1)^{2n} + (-1)^{2n+9} | n \in \mathbb{N}\} = \{-1, 1\}$.

p) $\{(-1)^n(-1)^{3n+1}+(-1)^{n+2}|n\in\mathbb{N}\}$.

Si n és parell, $3n+1$ és senar i $n+2$ és parell; per tant, $(-1)^n(-1)^{3n+1}+(-1)^{n+2}=1\cdot(-1)+1=0$. Si n és senar, aleshores $3n+1$ és parell, $n+2$ és senar; per tant, $(-1)^n(-1)^{3n+1}+(-1)^{n+2}=(-1)1+(-1)=-2$.

Finalment, $\{(-1)^n(-1)^{3n+1}+(-1)^{n+2}|n\in\mathbb{N}\}=\{0,-2\}$.

També es poden sumar els exponents, $(-1)^n(-1)^{3n+1}=(-1)^{n+(3n+1)}=(-1)^{4n+1}$; l'exponent $4n+1$ és sempre senar i, per tant, $(-1)^n(-1)^{3n+1}=(-1)^{4n+1}=-1$.

q) $\{(-1)^{2n+2}+(-1)^{5n+2}|n\in\mathbb{N}\}$.

L'exponent $2n+2$ és sempre parell i, per tant, $(-1)^{2n+2}=1$. Si n és parell, aleshores $5n+2$ és parell, d'on $(-1)^{5n+2}=1$, i si n és senar, aleshores $5n+2$ és senar i, en conseqüència, $(-1)^{5n+2}=1$.
Resulta finalment, d'acord amb els casos considerats:

$\{(-1)^{2n+2}+(-1)^{5n+2}|n\in\mathbb{N}\}=\{0,2\}$.

r) $\{\dfrac{1}{n}|n\in\mathbb{N},2|n,3\nmid n,5\nmid n,4<n<16\}$.

Per la quarta condició, els possibles valors de n són: $5,6,7,8,9,10,11,12,13,14,15$. Per la primera condició, resten $6,8,10,12,14$. Per la segona, resta $8,10,14$. Per la tercera, resten $8,14$. Per tant:

$\{\frac{1}{n}|n\in\mathbb{N},2|n,3\nmid n,5\nmid n,4<n<16\}=\{\frac{1}{n}|n\in\{8,14\}\}=\{\frac{1}{8},\frac{1}{14}\}$.

És possible que un conjunt pugui ser definit per comprensió (per propietats) de més d'una manera:

Exemple 8.7 Considerem el conjunt dels enters no múltiples de 3, és a dir: $A=\{n\in\mathbb{Z}|3\nmid n\}=\{n|n\in\mathbb{Z}\wedge 3\nmid n\}$.

Com pot ser un nombre enter no divisible per 3? Per la divisió entera de n entre 3, resulta que existeixen enters q,r tals que $n=3q+r$, amb $r=1$ o $r=2$ (no múltiple de 3). És a dir $n=3q+1$ o $n=3q+2$. També es pot expressar com $\{n|\exists q(q\in\mathbb{Z}\wedge n=3q+1)\vee\exists t(t\in\mathbb{Z}\wedge n=3t+2)\}$.

Observació. També es pot expressar (vegeu l'operació conjuntista d'unió) com:

$A=\{3a+1|a\in\mathbb{Z}\}\cup\{3b+2|b\in\mathbb{Z}\}$. ■

Conjunts finits, infinits

Un conjunt és finit si té un nombre finit d'elements, és a dir, si en podem comptar el nombre d'elements. Per exemple, $C=\{1,2,3,6\}$ és finit i té 4 elements. El nombre d'elements d'un conjunt finit és el *cardinal* del conjunt. La notació habitual és $|C|$; així, $|C| = 4$. En canvi, $\mathbb{N}$ no és finit: és infinit. És *infinit* tot conjunt que no sigui finit (no en podem comptar el nombre dels seus elements). També ho són el conjunt dels enters parells, el conjunt dels enters senars, el conjunt dels múltiples de 3, el conjunt dels enters, dels racionals, dels nombres reals i dels complexos. És $|\emptyset| = 0$. De fet, $C = \emptyset \Leftrightarrow |C| = 0$.

8.2. Igualtat i desigualtat de conjunts

8.2.1. Igualtat de dos conjunts

Abans s'ha dit que el que importa d'un conjunt, el que el defineix, són els elements que el formen. Per aquest motiu, és natural la definició (conceptual) següent:

Definició 8.1 *Dos conjunts són iguals si tenen els mateixos elements.*

Els elements de qualsevol dels dos també són de l'altre. En cas contrari, són diferents.

Notació. Si A i B són conjunts, $A = B$ denota que són iguals i $A \neq B$ denota que són diferents.

Exemples 8.8

Exemple 1. Abans s'ha dit que l'ordre no importa; així que els conjunts

$\{x,\{1,2,\{y\}\},a,\emptyset\}$, $\{\emptyset,a,x,\{1,2,\{y\}\}\}$ i $\{\emptyset,a,x,\{2,1,\{y\}\}\}$ són iguals. D'acord amb la notació anterior ($A = B$), és $\{x,\{1,2,\{y\}\},a,\emptyset\} = \{\emptyset,a,x,\{1,2,\{y\}\}\}$.

Exemple 2. Els conjunts $A = \{1,2,3\}$ i $B = \{2,4,7,9\}$ no són iguals (són diferents). Per exemple, perquè $3 \in A$ i $3 \notin B$. Per tant, $A \neq B$.

Exemple 3. Els conjunts $\mathbb{N}$ i $\mathbb{Z}$ no són iguals. Per exemple, $-3 \in \mathbb{Z}$ i, en canvi, $-3 \notin \mathbb{N}$. Per tant, $\mathbb{N} \neq \mathbb{Z}$. ■

Expressió de la igualtat de dos conjunts mitjançant fórmules de predicat: Tot element de A ho és de B i tot element de B ho és de A. Per tant, podem escriure

$(x \in A \rightarrow x \in B)$ i $(x \in B \rightarrow x \in A)$, és a dir:

$(x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)$

Equivalentment:

$(x \in A \leftrightarrow x \in B)$

I això és per a un x arbitrari, de manera que les fórmules de predicat concretes (equivalents) que corresponen a la igualtat són:

$\forall x((x \in A \to x \in B) \wedge (x \in B \to x \in A))$

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

També: $\forall x(x \in A \to x \in B) \wedge \forall y(y \in B \to y \in A))$.

Què hem de demostrar per a provar la igualtat dels conjunts A i B?

▷ Hem de considerar un x arbitrari, però fix per a la demostració, i provar

$x \in A \Rightarrow x \in B$ i

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

o bé, equivalentment, si es pot aconseguir, provar:

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

▷ També es pot considerar

$x \notin A \Leftrightarrow x \notin B$

Això és degut al fet que $(F \leftrightarrow G) \equiv (\neg F \leftrightarrow \neg G)$

▷ En comptes de provar

$x \in A \Rightarrow x \in B$ i

$x \in B \Rightarrow x \in A$,

podem provar, equivalentment, els contrarecíprocs respectius:

$x \notin B \Rightarrow x \notin A$ i

$x \notin A \Rightarrow x \notin B$

Per exemple, per a l'esquema:

$x \in A \Rightarrow x \in B$ i

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

es podria procedir de la manera següent (esquema demostratiu general).

Per a la primera implicació, és a dir, per a $x \in A \Rightarrow x \in B$:

Estructura de l'enunciat:

Hipòtesi: $x \in A$

Tesi: $x \in B$

Se suposa x arbitrari, però fix per a tota l'argumentació.

Anàlogament, per a $x \in B \Rightarrow x \in A$.

Demostració

Part 1: $x \in A \Rightarrow x \in B$

Sigui $x \in A$ (se suposa x arbitrari, però fix per a la resta de l'argumentació).

...

(arguments) ...

Aleshores $x \in B$.

Per tant, $x \in A \Rightarrow x \in B$.

Així, $\forall x(x \in A \rightarrow x \in B)$ és cert.

Part 2: $y \in B \Rightarrow y \in A$

Sigui $y \in B$ (se suposa y arbitrari, però fix per a la resta de l'argumentació).

...

(arguments)

...

Aleshores $y \in A$.

Per tant, $y \in B \Rightarrow y \in A$.

Així, $\forall y(y \in B \rightarrow y \in A)$ és cert. *Conclusió*: $A = B$

Més detall (arguments):

$x \in A$

...

Aleshores P_1 ...

Per tant, P_2 ...

En conseqüència, P_3

...

$x \in B$

$x \in A \Rightarrow P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow \ldots \Rightarrow x \in B$.

Veurem que el problema també es pot formular en termes d'inclusió de conjunts (secció 8.3).

El que s'ha descrit anteriorment és genèric, tot i que en el fons és això. Hi ha altres situacions possibles, com per exemple aquella en la qual definim un conjunt a través de fórmules conjuntistes (secció 8.10). En aquest cas, pot ser possible demostrar la igualtat “a alt nivell”, sense haver d’argumentar amb elements, mitjançant operacions conjuntistes, i fins i tot amb mètodes específics, com el de les taules de pertinença. Amb aquest mètode, també podem demostrar no igualtat.

Exemples i exercicis de demostració de la igualtat de dos conjunts

Exemple 8.9 Conjunt dels enters senars.

Provem que $A = B$ si $A = \{n \in \mathbb{Z} | 2 \nmid n\}$ i $B = \{2k+1 | k \in \mathbb{Z}\}$.

En efecte, vegem:

$\forall n(n \in A \rightarrow n \in B)$

Sigui $n \in A$. Aleshores no és divisible per 2.

Efectuant la divisió entera de n per 2, existeixen enters k, r tals que $n = 2k + r$, amb $0 \leq r < 2$, és a dir, $0 \leq r \leq 1$. Essent n no divisible per 2, el residu r de la divisió entera de n per 2 ha de ser $r \neq 0$, d’on $r = 1$.

Per tant, $n = 2k + 1$ per a algun k enter. Així, $n \in B$.

Recíprocament, vegem:

$\forall m(m \in B \rightarrow m \in A)$

Sigui $m \in B$. Aleshores existeix $k \in \mathbb{Z}$ tal que $m = 2k + 1$.

Vegem que m és senar, és a dir, no múltiple de 2, és a dir, $m \in A$.

Ho demostrarem per *reducció a l’absurd*. Suposem que m no és senar. Per tant, és parell, és a dir $m = 2q$ per a algun enter q. Per consegüent, $2q = m = 2k+1$, és a dir, $2q = 2k+1$, d’on $1 = 2q - 2k = 2(q-k)$, que és parell. En conseqüència, 1 és parell, que és absurd.

Finalment, doncs, $m \in A$. ■

Exemple 8.10 $\{x \in \mathbb{Z}|\ 6|x\} = \{x \in \mathbb{Z}|\ 2|x \wedge 3|x\}$ $(= \{6k | k \in \mathbb{Z}\})$.

Sigui $A = \{x \in \mathbb{Z}|\ 6|x\}$ i $B = \{x \in \mathbb{Z}|\ 2|x \wedge 3|x\}$.

1. Vegem que, per a tot x, $x \in A \Rightarrow x \in B$:

   Sigui $x \in A$.

   Aleshores $6|x$, és a dir, existeix un enter q tal que $x = 6q$. Per tant, $x = 6q = 3(2q)$, d’on $3|x$. També podem escriure $x = 2(3q)$, d’on $2|x$. Per tant, $2|x$ i $3|x$.

   En conseqüència, $x \in B$.

2. Vegem que, per a tot x, $x \in B \Rightarrow x \in A$:

   Sigui $x \in B$.

   Aleshores $2|x$ i $3|x$. Per $3|x$, x és de la forma $x = 3q$ per a algun q enter. Per l’altra hipòtesi, és $2|x = 3q$. Vegem que podem deduir $2|q$, i així tindríem $q = 2t$, per a algun t enter i, per tant, $x = 3(2t) = 6t$, d’on $x \in B$, i això conclouria la demostració. Vegem, doncs, $2|3q \Rightarrow 2|q$.

Demostrem-ho per *reducció a l'absurd*. Suposem que la implicació no és certa, és a dir que és cert: $2|3q$ i $2\nmid q$. Vegem que arribem a alguna contradicció. Si $2\nmid q$, per divisió entera és $q=2w+1$ per a algun enter w, d'on $3q=3(2w+1)=6w+3$. Ara bé, és $2|3q$ i, per tant, $2|6w+3$, d'on $6w+3=2s$ per a s enter convenient. Així, resulta $2s-6w=3=3$, és a dir, $2(s-3w)=3$. I, atès que $2|2(s-3w)$, resulta $2|3$, d'on resulta que 3 és múltiple de 2, que és absurd.

Finalment, $x\in A$. ■

Exemple 8.11 Provem que els conjunts següents són iguals (dues expressions dels senars):

$S_1=\{n|n\in\mathbb{Z}\wedge\exists k(k\in\mathbb{Z}\wedge n=2k+1)\}$

$S_2=\{m|m\in\mathbb{Z}$ i existeix un nombre enter t tal que $m=2t-1\}$

O bé $\{2k+1|k\in\mathbb{Z}\}=\{2t-1|t\in\mathbb{Z}\}$.

Observem que S_2 es pot expressar amb fórmules de predicat com a expressió de les propietats:

$S_1=\{n|n\in\mathbb{Z}\wedge\exists k(k\in\mathbb{Z}\wedge n=2k+1)\}$

$S_2=\{m|m\in\mathbb{Z}\wedge\exists t(t\in\mathbb{Z}\wedge m=2t-1)\}$

Demostrarem la igualtat provant les dues implicacions

$x\in S_1\Rightarrow x\in S_2$ i

$x\in S_2\Rightarrow x\in S_1$,

per a tot x, dos subproblemes que resoldrem independentment.

Subproblema 1. Vegem que és cert:

$\forall x(x\in S_1\rightarrow x\in S_2)$

Hipòtesi: $x\in S_1$

Tesi: $x\in S_2$

Fixem x de S_1. Aleshores, hem de veure que $x\in S_1\Rightarrow x\in S_2$.

Si $x\in S_1$, aleshores $x=2k+1$ per a un determinat k enter (i x també és enter).

Vegem que $\exists t(t\in\mathbb{Z}\wedge x=2t-1)$. Imposem $2t-1=x=2k+1$. Operant, resulta $t=k+1$, d'on $k=t-1$. Per tant, i com a comprovació $x=2k+1=2(t-1)+1=2t-1$. Així doncs, existeix un nombre enter t tal que $x=2t-1$ (és suficient prendre $t=k+1$), és a dir, $x\in S_2$.

Subproblema 2. Anàlogament, demostrem que és cert:

$\forall x(x \in S_2 \to x \in S_1)$

Hipòtesi: $x \in S_2$

Tesi: $x \in S_1$

Fixem x de S_2. Vegem que $x \in S_2 \Rightarrow x \in S_1$.

Si $x \in S_2$, aleshores $x = 2t - 1$ per a un determinat t enter (i x també és enter).

Vegem que $\exists k(t \in \mathbb{Z} \wedge x = 2k+1)$. Imposem $2t-1 = x = 2k+1$. Operant resulta $t = k+1$, d'on $k = t-1$. Per tant, i com a comprovació, $x = 2t-1 = 2(k+1)-1 = 2k+1$. Així doncs, existeix un nombre enter k tal que $x = 2k+1$ (és suficient prendre $k = t-1$), és a dir, $x \in S_1$. ■

Tot seguit, veiem més exercicis en què s'ha de demostrar la igualtat de dos conjunts.

PROBLEMA 8.2

Proveu que els enters senars múltiples de 5 *són de la forma* $10n+5$ *per a* n *enter. En termes de conjunts:*

$\{m \in \mathbb{Z} | \; 2 \nmid m \wedge 5|m\} = \{10n+5| \; n \in \mathbb{Z}\}$.

Solució. Hem de veure dues implicacions:

a) $x \in \{m \in \mathbb{Z} | 2 \nmid m \wedge 5|m\} \Rightarrow x \in \{10n+5|n \in \mathbb{Z}\}$?
Sigui $x \in \{m \in \mathbb{Z} | 2 \nmid m \wedge 5|m\}$.

En efecte, si x és múltiple de 5, és $x = 5k$ per a algun k enter. Ara bé, si $5k$ ha de ser senar, ho ha de ser també k (ja que, en cas contrari, seria x parell). Per tant, $k = 2t+1$ (una altra versió: $2t-1$). En conseqüència, $x = 5(2t+1) = 10t+5$.

Per tant, $x \in \{10n+5|n \in \mathbb{Z}\}$.

Observació. Fent servir l'altra possible expressió per a senars, s'arriba a la mateixa conclusió (és una comprovació, no podia ser d'altra manera): $k = 2t'-1$, d'on $x = 5(2t'-1) = 10t'-5 = 10(t'-1)+5$.

b) $x \in \{10n+5|n \in \mathbb{Z}\} \Rightarrow x \in \{m \in \mathbb{Z} | 2 \nmid m \wedge 5|m\}$?

Sigui $x \in \{10n+5|n \in \mathbb{Z}\}$.

Llavors $x = 10n+5$ per a algun n enter. Ara tenim $x = 2(5n)+5$, suma d'un nombre parell i un de senar, que és senar. Per tant, $2 \nmid x$. D'altra banda, $x = 10n+5 = 5(2n+1)$, que és múltiple de 5. Així, $2 \nmid x \wedge 5|x$. Per tant,

$x \in \{m \in \mathbb{Z} | 2 \nmid m \wedge 5|m\}$.

PROBLEMA 8.3

Proveu que els enters parells múltiples de 5 *són de la forma* $10n$ *per a* n *enter. En termes de conjunts:*

$\{m \in \mathbb{Z} |\ 2|m \wedge 5|m\} = \{10n|\ n \in \mathbb{Z}\}$.

Solució. Siguin $A = \{m \in \mathbb{Z}|\ 2|m \wedge 5|m\}$, $B = \{10n|\ n \in \mathbb{Z}\}$. Volem demostrar $A = B$.

a) Vegem que $x \in B \Rightarrow x \in A$. Sigui $x \in B$.

   Aleshores existeix $n \in \mathbb{Z}$ tal que $x = 10n$. Ara bé, es pot expressar de dues formes: $x = 10n = 5(2n)$, d'on $5|n$ i com $x = 2(5n)$, d'on $2|n$.

   Per tant, $x \in A$.

b) Vegem que $x \in A \Rightarrow x \in B$. Sigui $x \in A$.

   Aleshores és $x = 5r$ i també $x = 2s$, amb r, s enters, d'on $5r = 2s$ i així resulta que $2|2s$ i, per tant, $2|5r$.

   Podem utilitzar el lema d'Euclides o el lema de Gauss per deduir $2|r$, d'on $r = 2r'$, amb r' enter convenient, i així $x = 5r = 10r'$.

   Per tant, $x \in A$.

   També es pot fer una argumentació que no utilitzi cap dels lemes anteriors. Si, a partir de $2|5r$, volem deduir $2|r$, podem suposar que $2 \nmid r$. Aleshores, considerant la divisió entera de r per 2, és $r = 2\alpha + 1$, per a un enter α. Com que $5r = 2\beta$, per a un enter β adequat és $5(2\alpha + 1) = 2\beta$, d'on $2\beta - 10\alpha = 5$ i, per tant, $2(\beta - 5\alpha) = 5$. Com que 2 divideix el membre de l'esquerra de la igualtat anterior, també divideix el de la dreta, és a dir, $2|5$, absurd. Per tant, $2|r$.

PROBLEMA 8.4

Proveu que els conjunts següents són iguals:

$\{10n + 5|n \in \mathbb{Z}\} = \{10n - 5|n \in \mathbb{Z}\} = \{10n - 15|n \in \mathbb{Z}\} = \{10n + 15|n \in \mathbb{Z}\}$.

Solució. Provem només $A = B$ si $A = \{10n+5|n \in \mathbb{Z}\}$ i $B = \{10n-5|n \in \mathbb{Z}\}$. Les altres igualtats es poden demostrar anàlogament (exercici).

Quina relació hi ha entre n, n' (enters) si $10n + 5 = 10n' - 5$? De la igualtat en resulta $10n - 10n' + 10 = 0$, que equival a $n - n' + 1 = 0$, que equival a $n' = n + 1$. Per tant:

$x \in A \Leftrightarrow$

$\exists n \in \mathbb{Z}(x = 10n + 5) \Rightarrow (*)$

$\exists n' \in \mathbb{Z}(x = 10n' - 5) \Leftrightarrow$ (prenent $n' = n + 1$ resulta $x = 10n + 5 = 10(n' - 1) + 5 = 10n' - 5$), que equival a

$x \in B$.

Ara bé, la implicació anterior (*) és, de fet, una equivalència, ja que:

$\exists n' \in \mathbb{Z}(x = 10n' - 5)$ implica $\exists n \in \mathbb{Z}(x = 10n + 5)$, prenent $n = n' - 1$; en efecte, $x = 10n' - 5 = 10(n+1) - 5 = 10n + 10 - 5 = 10n + 5$.

Per tant, refent l'argumentació:

$x \in A \Leftrightarrow \exists n \in \mathbb{Z}(x = 10n + 5) \Leftrightarrow \exists n' \in \mathbb{Z}(x = 10n' - 5) \Leftrightarrow x \in B$.

Així, doncs, aquesta seqüència d'equivalències prova $x \in A \Leftrightarrow x \in B$. Per tant, $\forall x(x \in A \leftrightarrow x \in B)$ és cert, és a dir, $A = B$.

8.2.2. Desigualtat de dos conjunts

És simplement la negació de la igualtat, és a dir, $\neg(A = B)$.

Notació: La notació corresponent és $A \neq B$.

Així:

Exemples 8.12

Exemple 1. Els conjunts $A = \{1,2,3\}$ i $B = \{\emptyset,4,5,*\}$ no són iguals (són diferents). Per exemple, perquè $3 \in A$ i $3 \notin B$. O també perquè $4 \in B$ i, en canvi, $4 \notin A$. És $\{1,2,3\} \neq \{\emptyset,4,5,*\}$ (és $A \neq B$). ■

Exemple 2. Els conjunts $\mathbb{Q}$ i $\mathbb{R}$ no són iguals. Per exemple, $\sqrt{2} \in \mathbb{R}$ i, en canvi, $\sqrt{2} \notin \mathbb{Q}$. Per tant, $\mathbb{Q} \neq \mathbb{R}$. ■

Expressió de la desigualtat de dos conjunts mitjançant fórmules de predicat. Intuïtivament, es veu clar. Vegem una obtenció "automatitzada" amb la negació de

$\forall x((x \in A \to x \in B) \wedge (x \in B \to x \in A))$

En efecte, escrivim diverses equivalències:

$\neg\forall x((x \in A \to x \in B) \wedge (x \in B \to x \in A))$

$\exists x \neg((x \in A \to x \in B) \wedge (x \in B \to x \in A))$ (per negació del quantificador universal)

$\exists x(\neg(x \in A \to x \in B) \vee \neg(x \in B \to x \in A))$ (per De Morgan, lògica)

$\exists x((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A))$ (per negació del condicional)

$A \neq B$ si, i només si, $\exists x((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A))$

Per tant, "hi ha algun element que és d'un conjunt i no de l'altre".

Es pot reescriure la fórmula anterior per a obtenir-ne una d'equivalent:

$\exists x((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A))$, que equival a

$\exists x(x \in A \wedge x \notin B) \vee \exists x(x \in B \wedge x \notin A)$, que reescrivim com

$\exists x(x \in A \wedge x \notin B) \vee \exists y(y \in B \wedge y \notin A)$

Vegem casos diferents de desigualtat, per diferents motius:

Exemples 8.13

Exemple 1. $A = \{1,2,3\}$, $B = \{7,8\}$ (no tenen cap element en comú) ($A \neq B$). ■

Exemple 2. $A = \{1,2,3\}$, $B = \{1,2,3,4,5\}$ (tots els elements de A són de B, però no a l'inrevés) (n'hi ha prou que existeixi un element de A que no sigui de B o a l'inrevés) ($A \neq B$). ■

Exemple 3. $A = \{1,2,3,a,b,c\}$, $B = \{1,2,y\}$ (alguns elements de A no són de B i alguns elements de B no són de A; n'hi ha prou amb la primera part o la segona) ($A \neq B$). ■

Què hem de fer per tal de provar la desigualtat dels conjunts A i B? Bàsicament, i genèricament, hem de mostrar que existeix un element de A que no és de B, o bé que existeix algun element de B que no és de A.

Hi pot haver algun cas especial en què es pugui procedir de manera diferent. Per exemple, si els conjunts A,B estan definits per fórmules conjuntistes, aleshores es pot veure a través de les taules de pertinença (vegeu secció 8.10); en aquest cas, cal veure que les taules de pertinença són diferents.

A part dels exemples anteriors, vegem-ne algun altre:

Exemple 8.14 Vegem que el conjunt dels enters múltiples de 3 i els enters múltiples de 6 són diferents.

Formalitzem: siguin $A = \{3q | q \in \mathbb{Z}\}$ i $B = \{6q | q \in \mathbb{Z}\}$. Veiem que $3 \in A$ i, en canvi, $3 \notin B$, ja que 3 no és múltiple de 6. Es compleix, doncs, $\exists x(x \in A \wedge x \in B)$. En aquest cas, atès que $6k = 3(2k)$, resulta que tot múltiple de 6 també és múltiple de 3, de manera que $\forall x(x \in B \rightarrow x \in A)$ és cert. ■

8.3. La relació d'inclusió. Subconjunts

Definició 8.2 *Es diu que un conjunt A és un* ***subconjunt*** *del conjunt B si, i només si, tot element de A és també element de B. També es diu que A* ***està inclòs*** *en B o que "B conté A".*

Notació: $A \subseteq B$ és la notació corresponent a "A és subconjunt de B".

$A \nsubseteq B$ és la notació corresponent a "A no és subconjunt de B" (negació del concepte anterior, $\neg(A \subseteq B)$).

Exemples 8.15

Exemple 1. $\{1,2,3\} \subseteq \{-1,x,\{x\},1,2,z,3,6\}$. En efecte:

$1 \in \{1,2,3\}$ i també $1 \in \{-1,x,\{x\},1,2,z,3,6\}$

$2 \in \{1,2,3\}$ i també $2 \in \{-1,x,\{x\},1,2,z,3,6\}$

$3 \in \{1,2,3\}$ i també $3 \in \{-1,x,\{x\},1,2,z,3,6\}$. ■

Exemple 2. Siguin $A = \{y,z\}$, $B = \{x,\{y,z\},\{1,y\},z,\{y\},y\}$. Aleshores és $A \subseteq B$.

En efecte, $\{\,y\,,\,z\,\} \subseteq \{x,\{y,z\},\{1,y\},\,z\,,\{y\},\,y\,\}$. ■

Exemple 3. $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$ (fent $m = \frac{m}{1}$). ■

Exemple 4. $(2,3) \subseteq [2,3]$, $(2,3) \subseteq [-4,5]$ (intervals en els reals). ■

Exemple 5. Siguin C el conjunt dels enters múltiples de 7 i D el conjunt dels enters múltiples de 21. És $C = \{7n | n \in \mathbb{Z}\}$ i $D = \{21n | n \in \mathbb{Z}\}$.

Vegem que es compleix $D \subseteq C$.

Vegem que tot element de D és també de C.

En efecte, si $x \in D$, aleshores és de la forma $x = 21k$ per a algun k enter convenient. Vegem que $x \in C$. Tenim $x = 21k = 7(3k) = 7k'$, amb $k' = 3k \in \mathbb{Z}$. Així, x és múltiple de 7, d'on $x \in C$. ■

Expressió de la inclusió mitjançant fórmules de predicat: Formalitzant la definició anterior, $A \subseteq B$ s'expressa com:

$$\forall x (x \in A \rightarrow x \in B)$$

Expressió equivalent pel contrarecíproc: Expressem la relació d'inclusió en termes del contrarecíproc:

$(p \rightarrow q \equiv \neg q \rightarrow \neg p)$:

De la fórmula $\forall x (x \in A \rightarrow x \in B)$, considerem:

$(x \in A \rightarrow x \in B)$, que és equivalent al contrarecíproc: $(x \notin B \rightarrow x \notin A)$

Generalitzant:

$\forall x (x \notin B \rightarrow x \notin A)$

Resumint:

$A \subseteq B$ si, i només si, $\forall x (x \in A \rightarrow x \in B)$

$A \subseteq B$ si, i només si, $\forall x (x \notin B \rightarrow x \notin A)$

***Com demostrar** $A \subseteq B$?*

D'acord amb les dues expressions anteriors, cal considerar un x arbitrari, però fix per a la demostració, i provar **una qualsevol** de les implicacions següents:

$x \in A \Rightarrow x \in B$ (*directa*)

Sigui $x \in A$.

... (argumentacions)

Per tant, $x \in B$.

Conclusió: $A \subseteq B$.

$x \notin B \Rightarrow x \notin A$ (*contrarecíproc*)

També es pot demostrar *per reducció a l'absurd*, a partir de suposar certa la negació de $x \in A \Rightarrow x \in B$, és a dir, $x \in A \wedge x \notin B$.

De manera completa: neguem $\forall x(x \in A \rightarrow x \in B)$:

$\exists x \neg(x \in A \rightarrow x \in B)$

$\exists x(x \in A \wedge x \notin B)$

i arribem a alguna contradicció.

Vegem uns exemples on es demostra la inclusió per diversos mètodes.

Exemple 8.16 Sigui $A = \{15k | k \in \mathbb{Z}\}$ (conjunt dels múltiples de 15) i sigui $B = \{5t | t \in \mathbb{Z}\}$ (conjunt dels múltiples de 5). Vegem que $A \subseteq B$, és a dir, que $\forall x(x \in A \rightarrow x \in B)$ és cert.

Hem de provar $x \in A \Rightarrow x \in B$ per a un element x qualsevol fixat.

Sigui $x \in A$.

Aleshores es pot escriure com $x = 15k$, per a un cert enter k. Vegem que $x \in B$, és a dir, que es pot expressar com $x = 5t$ per a algun t enter. Ara bé, $x = 15k = 5(3k)$ i és suficient prendre $t = 3k \in \mathbb{Z}$.

Per tant, $x \in B$.

Així, $x \in A \Rightarrow x \in B$. Per tant, $A \subseteq B$. ■

Exemple 8.17 Siguin D_6 el conjunt dels enters múltiples de 6 i D_3 el conjunt dels enters múltiples de 3.

Volem provar que $D_6 \subseteq D_3$.

Recordem que $D_6 = \{6k | k \in \mathbb{Z}\}$ i $D_3 = \{3k | k \in \mathbb{Z}\}$.

Mètode 1. Hi ha una demostració directa i senzilla del resultat:

Hem de provar $x \in D_6 \Rightarrow x \in D_3$, amb x arbitrari. És a dir, que és cert: $\forall x(x \in D_6 \to x \in D_3)$

Sigui $x \in D_6$. Aleshores existeix un enter k tal que $x = 6k$. Volem veure que x és de la forma dels elements de D_3, és a dir, $x = 3k'$ per a algun enter k'. En efecte, $x = 6k = 3(2k)$ i és suficient prendre $k' = 2k$. Per tant, $x \in D_3$. Així, $D_6 \subseteq D_3$.

Mètode 2. Vegem una demostració per reducció a l'absurd.

S'ha vist una demostració directa i senzilla del resultat al mètode 1. Vegem la demostració per reducció a l'absurd, més complicada, però amb propòsit d'exercitació i de mostrar una metodologia demostrativa:

Suposem fals l'enunciat $\forall x(x \in D_6 \to x \in D_3)$.

I, per tant, certa la negació de l'anterior, $\exists x(x \in D_6 \wedge x \notin D_3)$.

Suposem, doncs, que existeix x tal que $x \in D_6$ i $x \notin D_3$. Vegem que arribem a una contradicció.

Si x no és múltiple de 3 i si $x = 3q + r$, $0 \leq r \leq 2$ és la divisió entera de x per r, aleshores $r \neq 0$. Per tant, són possibles *dos casos* (resolució per casos):

Cas 1: $x = 3q + 1$

Cas 2: $x = 3q + 2$

Si $x \in D_6$, aleshores $x = 6k$ per a algun enter k.

En el cas 1, és $3q + 1 = x = 6k$, d'on $3(2k - q) = 1$. Atès que $3|(3(2k - q))$, resulta que $3|1$, que és absurd.

En el cas 2, és $3q + 2 = x = 6k$, d'on $3(2k - q) = 2$. Atès que $3|(3(2k - q))$, resulta que $3|2$, que és absurd.

S'ha arribat a una contradicció. Per tant, és cert: $\forall x(x \in D_6 \to x \in D_3)$, d'on $D_6 \subseteq D_3$.

Mètode 3. Pel contrarecíproc (encara que n'hem vist una demostració directa més simple).

Volem demostrar $D_6 \subseteq D_3$. Pel mètode escollit, vegem que $\forall x(x \notin D_3 \to x \notin D_6)$ és cert. Sigui, doncs, x arbitrari. Volem veure que $x \notin D_3 \Rightarrow x \notin D_6$.

Si $x \notin D_3$, aleshores x no és múltiple de 3. Efectuant la divisió entera de x entre 3, el residu és no nul i, per tant, és $x = 3q + 1$ o $x = 3q + 2$. Efectuem la divisió entera de x per 6; resulta $x = 6t + r$, amb $0 \leq r \leq 5$. Volem veure que $r \neq 0$.

Argumentant per casos:

En el cas que sigui $x = 3q + 1$, tenim $x = 6t + r$, d'on $3q + 1 = 6t + r$, d'on $3(q - 2t) = r - 1$, d'on $3|r - 1$. Si fos $r = 0$, seria $3| - 1$, absurd.

En el cas que sigui $x = 3q+2$, tenim $x = 6t+r$, d'on $3q+2 = 6t+r$, d'on $3(q-2t) = r-2$, d'on $3|r-2$. Si fos $r = 0$, seria $3|-2$, absurd.

Per tant, $r \neq 0$ i, en conseqüència, $x \notin D_6$. ■

Per a dos conjunts, no és certa l'afirmació "$A \subseteq B$ o $B \subseteq A$". Pot ser que fins i tot cap de les dues inclusions es compleixi. Per exemple, amb $A = \{1,2,3,4\}$ i $B = \{3,4,5,6,7\}$.

De $A \subseteq B$ no se'n deriva $B \subseteq A$, ni viceversa.

Negació de la inclusió $A \subseteq B$. Quan $A \not\subseteq B$? La no inclusió de A en B és simplement la negació de $A \subseteq B$. També es diu que "A no és subconjunt de B", o que "B no conté A" (com a subconjunt). La notació que utilitzem és $A \not\subseteq B$, que no és més que $\neg(A \subseteq B)$.

Es veu immediatament que $\neg(A \subseteq B)$ si, i només si, algun element de A no ho és de B. Es pot obtenir formalment, "automatitzadament", per negació de la corresponent fórmula de predicat:

$\neg\forall x(x \in A \to x \in B)$, que equival a (per negació del quantificador universal)

$\exists x\neg(x \in A \to x \in B)$, que equival a

$\exists x(x \in A \wedge \neg x \in B)$, per l'equivalència de negació del condicional.

$\exists x(x \in A \wedge x \notin B)$, per reescriptura.

Si neguem la fórmula amb contrarecíproc, n'obtenim lògicament el mateix (seqüència d'equivalències):

$\neg\forall x(x \notin B \to x \notin A)$

$\exists x\neg(x \notin B \to x \notin A)$ (negació del quantificador universal)

$\exists x(x \notin B \wedge \neg x \notin A)$ (negació del condicional)

$\exists x(x \notin B \wedge \neg\neg x \in A)$ (reescriptura)

$\exists x(x \notin B \wedge x \in A)$ (doble negació)

$\exists x(x \in A \wedge x \notin B)$, res de nou.

Exemples 8.18

Exemple 1. $\{1,2,3,4\} \not\subseteq \{2,3\}$. En efecte: $1 \in \{1,2,3,4\}$ i, en canvi, $1 \notin \{2,3\}$. Amb $x = 1$, veiem la no-inclusió. També podríem utilitzar $x = 4$, però amb un element n'hi ha prou. ■

Exemple 2. Siguin $A = \{y,z\}$, $B = \{x,\{y,z\},\{1,y\},z,\{y\},\{\{y\}\},\emptyset\}$. Aleshores, $A \not\subseteq B$.

En efecte, és $y \in A$ i, en canvi, $y \notin B$ (i també per a z). ■

Exemple 3. $(-2,3) \not\subseteq (0,7)$. És $-1 \in (-2,3)$ i, en canvi, $-1 \notin (-2,3)$. ■

Exemple 4. $\{y,z\} \not\subseteq \{\{z\},\{y,z\},\{3,y,z\},\{y\}\}$. Efectivament, $y \in \{y,z\}$ i, en canvi, $y \notin \{\{z\},\{y,z\},\{3,y,z\},\{y\}\}$. ■

Exemple 5. $\{1,2,3\} \not\subseteq \{1,\{2\},3,4,5\}$. ■

Exemple 8.19 Siguin A el conjunt dels enters múltiples de 7 i B el conjunt dels enters múltiples de 35. Vegem que $A \not\subseteq B$. Hem de veure que $\exists x(x \in A \wedge x \notin B)$ és cert. Considerem $x = 14$. És $x = 14 \in A$ i, en canvi, $x = 14 \notin B$. Observeu que $B \subseteq A$ (ja que $35k = 7(5k)$; o bé l'exemple similar que hem vist anteriorment).

En resum:

***Com demostrar** $A \not\subseteq B$?*

$A \not\subseteq B$ si, i només si, $\exists x(x \in A \wedge x \notin B)$

És suficient mostrar algun element de A que no sigui de B.

Igualtat de conjunts en termes d'inclusió. Recordem que la igualtat dels conjunts A i B és equivalent que sigui cert

$\forall x((x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A))$

i és cert si són certs:

$\forall x(x \in A \rightarrow x \in B)$
$\forall x(x \in B \rightarrow x \in A)$

o bé, per a qualsevol x:

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

Es pot reformular en termes de la relació d'inclusió. És a dir, respectivament, $A \subseteq B$ i $B \subseteq A$.

Així, $A = B$ si, i només si, $A \subseteq B \wedge B \subseteq A$.

Per tant, demostrarem la igualtat de conjunts $A = B$ si demostrem equivalentment la doble inclusió: $A \subseteq B$ i $B \subseteq A$.

La igualtat és un cas especial d'inclusió. La notació $A \subseteq B$ no exclou la igualtat (però pot ser que no es produeixi).

En resum: $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$

Provar la igualtat de conjunts (per doble inclusió). Així doncs, per a demostrar la igualtat de dos conjunts hem de demostrar separadament dues inclusions, i així descomponem el problema en dos subproblemes, que resoldrem separadament.

Subproblema 1: Provar $A \subseteq B$.

Subproblema 2: Provar $B \subseteq A$.

Exemple 8.20

Sigui $A = \{2p-3 | p \in \mathbb{Z}\}$.

Sigui $B = \{2q+5 | q \in \mathbb{Z}\}$.

Vegem que $A = B$.

Subproblema 1: Provar $A \subseteq B$.

Sigui $x \in A$.

Aleshores és $x = 2p-3$ per a algun p enter. Per a veure que és $x \in B$, hem de veure que existeix un enter q tal que $x = 2q+5$. Imposem $2p-3 = x = 2q+5$. Serà $2(p-q) = 8$, d'on $q = p-4$ o $p = q+4$. Efectivament, i com a comprovació, $2q+5 = 2(p-4)+5 = 2p-8+5 = 2p-3 = x$ (o a l'inrevés: $x = 2p-3 = 2(q+4)-3 = 2q+8-3 = 2q+5$).

Per tant, $x \in B$.

Subproblema 2: Provar $B \subseteq A$.

Sigui $x \in B$.

Aleshores és $x = 2q+5$ per a algun enter q. Vegem que existeix un enter p tal que $x = 2p-3$. S'ha de complir $2q+5 = 2p-3$, d'on $p = q+4$, $q = p-4$ i per a aquest p serà $x = 2p-3$, és a dir, $x \in A$. Es fa una comprovació com abans.

Per tant, $x \in A$. ■

Exemples 8.21 El lector pot provar diverses igualtats de conjunts (alguna ja s'ha vist a l'exemple anterior):

$$\{2k+1 | k \in \mathbb{Z}\} = \{2k-1 | k \in \mathbb{Z}\} = \{2k+3 | k \in \mathbb{Z}\} = \{2k-3 | k \in \mathbb{Z}\} =$$
$$= \{2k+5 | k \in \mathbb{Z}\} = \{2k-5 | k \in \mathbb{Z}\} = \{2k+7 | k \in \mathbb{Z}\} = \{2k-7 | k \in \mathbb{Z}\}$$

Vegem-ne alguna:

Exemple 1. $\{2k+1 | k \in \mathbb{Z}\} = \{2k'+3 | k' \in \mathbb{Z}\}$. Hem de veure que tot enter de la forma $2k+1$ és també de la forma $2k'+3$ i recíprocament. És a dir:

$\forall k \in \mathbb{Z}\ \exists k' \in \mathbb{Z}\ (2k+1 = 2k'+3)$ i

$\forall k' \in \mathbb{Z}\ \exists k \in \mathbb{Z}\ (2k'+3 = 2k+1)$

Estudiem quina relació hi ha d'haver entre k, k': $2k+1 = 2k'+3 \Rightarrow 2(k-k') = 3-1 \Rightarrow k-k' = 1$.

Així, donat k, escollim $k' = k-1$ i, donat k', escollim $k = k'+1$.
Això permet demostrar la doble inclusió i, per tant, la igualtat dels conjunts.

I similarment per als altres exemples.

Exemple 2. Per a provar $\{2k+1|k\in\mathbb{Z}\}=\{2k'-3|k'\in\mathbb{Z}\}$ fem un estudi similar: $2k+1=2k'-3\Rightarrow 2(k'-k)=4$, d'on $k'-k=2$.

I similarment per als altres exemples. ■

Exemple 3. Igualtats addicionals:

$\{2k|k\in\mathbb{Z}\}=\{2k+2|k\in\mathbb{Z}\}=\{2k-2|k\in\mathbb{Z}\}=\{2k+4|k\in\mathbb{Z}\}=$

$=\{2k-4|k\in\mathbb{Z}\}=\{2k+6|k\in\mathbb{Z}\}=\{2k-6|k\in\mathbb{Z}\}=\{2k+8|k\in\mathbb{Z}\}=\{2k-8|k\in\mathbb{Z}\}=....$ ■

Desigualtat de conjunts en termes d'inclusió. Quan dos conjunts són diferents? Volem contestar aquesta pregunta en termes de la relació d'inclusió.

A partir de

$A=B\leftrightarrow(A\subseteq B\wedge B\subseteq A)$

resulta (per $F\leftrightarrow G\equiv\neg F\leftrightarrow\neg G$)

$\neg(A=B)\leftrightarrow\neg(A\subseteq B\wedge B\subseteq A)$. Reescrivim:

$A\neq B\leftrightarrow\neg(A\subseteq B\wedge B\subseteq A)$. Per De Morgan (lògica), equival a:

$A\neq B\leftrightarrow(\neg(A\subseteq B)\vee\neg(B\subseteq A))$. Reescriptura:

$A\neq B\leftrightarrow((A\not\subseteq B)\vee(B\not\subseteq A))$

Veiem, doncs, que, per a la desigualtat de conjunts, n'hi ha prou que una de les inclusions no sigui certa; no cal que no ho siguin totes dues.

Exemple 8.22 Siguin A el conjunt dels enters múltiples de 5 i B el conjunt dels enters múltiples de 10. És compleix $B\subseteq A$, però $A\not\subseteq B$. Així que $A\neq B$. ■

Exemple 8.23 Siguin $A=\{2k|k\in\mathbb{Z}\}$ i $B=\{4p|p\in\mathbb{Z}\}$. Vegem que $\{2k|k\in\mathbb{Z}\}\neq\{4p|p\in\mathbb{Z}\}$. Serà suficient veure que alguna de les dues inclusions possibles no és certa. En efecte, vegem que $\{2k|k\in\mathbb{Z}\}\not\subseteq\{4p|p\in\mathbb{Z}\}$. Hem de veure que existeix $x\in A$ tal que $x\notin B$. És a dir, $\exists k\in\mathbb{Z}\forall k'\in\mathbb{Z}(2k\neq 4k')$. És suficient prendre $k=1$, o bé $k=3$ o $k=5$ o infinits més possibles. Els elements corresponents a aquests valors de k són de A però no de B. En canvi, $B\subseteq A$. A més de la resolució formal detallada anterior, el problema s'hauria pogut resoldre simplement considerant que 6 és múltiple de 2 i, en canvi, no de 4. ■

Observeu que la negació de $A\subseteq B$ ni equival a $B\subseteq A$ ni ho implica.

Propietats bàsiques de la inclusió

Teorema 8.1 *Si A,B,C són conjunts:*

a) $\emptyset\subseteq A$, *per a tot conjunt* A.

b) $A\subseteq A$, *per a qualsevol conjunt* A.

c) $((A\subseteq B)\wedge(B\subseteq C))\Rightarrow A\subseteq C$.

Demostracions

Donem demostracions com a exemple o exercici de treball amb conjunts.

$\emptyset \subseteq A$, per a tot conjunt A.

Demostració. Es compleix buidament $\forall x(x \in \emptyset \to x \in A)$ (ja que $\emptyset$ no té elements; l'afirmació es compleix per a tots els seus elements). Formalment, és un cas de propietat sempre certa ja que lògicament és $\forall x(F \to x \in A)$ o $\forall x(0 \to x \in A)$ sempre cert. "Tots els elements del $\emptyset$ són de A", cert, ja que no n'hi ha cap.

$A \subseteq A$, per a qualsevol conjunt A.

Demostració. Trivialment, ja que $\forall x(x \in A \to x \in A)$. És el cas $0 \to 0$ o $1 \to 1$, certs formalment en ambdós casos. És una obvietat, ja que "tot element de A és de A" és cert.

Propietat de transitivitat de la inclusió per als conjunts A, B, C:

$$\left.\begin{array}{l} A \subseteq B \\ B \subseteq C \end{array}\right\} \Rightarrow A \subseteq C$$

Demostració. La hipòtesi està formada per dues afirmacions:

$H_1 : A \subseteq B$ (és a dir, $x \in A \Rightarrow x \in B$) ($x$ arbitrari),

$H_2 : B \subseteq C$ (és a dir, $x \in B \Rightarrow x \in C$) ($x$ arbitrari).

La tesi és $T : A \subseteq C$.

L'estructura és: $(H_1 \wedge H_2) \Rightarrow T$.

Hem de provar que

si x és un element qualsevol de A, també ho és de C,

és a dir, $x \in A \Rightarrow x \in C$.

Sigui, doncs, $x \in A$. Aplicant H_1 (i "MP", *modus ponens*), resulta $x \in B$.

Aplicant $x \in B$ i H_2, deduïm $x \in C$.

Inclusió estricta/subconjunts propis:

Definició 8.3 *Es diu que el conjunt A és* ***subconjunt propi*** *de B si $A \subseteq B$ i $A \neq B$. La notació corresponent a aquest concepte és $A \subset B$. També es diu que "B conté estrictament A", o que "la inclusió de A a B és estricta".*

De fet, és equivalent a dir: $A \subseteq B$ i $B \nsubseteq A$.

Per tant, podem expressar la inclusió estricta mitjançant la fórmula de predicat següent:

$\forall x(x \in A \rightarrow x \in B) \wedge \exists y(y \in B \wedge y \notin A)$

Exemples 8.24

Exemple 1. $\mathbb{N} \subset \mathbb{Z}$.

Exemple 2. $\mathbb{Q} \subset \mathbb{R}$.

Exemple 3. $\{2n|n \in \mathbb{Z}\} \subset \mathbb{Z}$.

Exemple 4. El conjunt dels múltiples de 14 és un subconjunt propi del conjunt dels múltiples de 7.

Exemple 5. $\{6k|k \in \mathbb{Z}\} \subset \{3k|k \in \mathbb{Z}\}$, ja que $6k = 3(2k) = 3k'$.

Exemple 6. $(2,3) \subset [2,3]$ (intervals en els reals).

Exemple 7. $\{2,3\} \subset \{1,2,3,4\}$. ■

Naturalment, $A \subset B \Rightarrow A \neq B$.

Conjunts finits, cardinal i inclusió. Recordem que un conjunt és finit si podem comptar el nombre dels seus elements. El nombre d'elements del conjunt finit A és el cardinal de A i es denota $|A|$.

En el cas dels conjunts finits, tenim:

Si A, B són conjunts finits i $A \subseteq B$, aleshores $|A| \leq |B|$. Així, si $|A| \nleq |B|$, aleshores $A \nsubseteq B$. O bé $|A| > |B| \Rightarrow A \nsubseteq B$.

Per tant, només per un argument de cardinals, ja tenim $\{1,2,3,4,5\} \not\subset \{1,2,3,4\}$.

Exemples i problemes de demostració de la igualtat de dos conjunts per la doble inclusió

Exemple 8.25 Aquest exemple ja l'hem presentat a "igualtat de conjunts", però sense explicitar que es demostrava la doble inclusió.

Proveu que són iguals els conjunts (dues expressions dels nombres senars):

$S_1 = \{n|n \in \mathbb{Z} \wedge \exists k(k \in \mathbb{Z} \wedge n = 2k+1)\}$

$S_2 = \{m|m \in \mathbb{Z}$ i existeix un nombre enter t tal que $m = 2t-1\}$

Què cal veure? Ho demostrarem provant les dues inclusions $S_1 \subseteq S_2$ i $S_2 \subseteq S_1$, dos subproblemes que resoldrem independentment.

Subproblema 1. Demostrem que $S_1 \subseteq S_2$.

Això vol dir que $\forall x(x \in S_1 \to x \in S_2)$ és cert.

Fixat x (arbitrari), hem de veure que $x \in S_1 \Rightarrow x \in S_2$.

Si $x \in S_1$, aleshores és $x = 2k+1$ per a un cert k enter (i x també és enter).

Vegem que existeix un enter t tal que $x = 2t-1$ ($\exists t(t \in \mathbb{Z} \wedge x = 2t-1)$). Imposem $2t-1 = x = 2k+1$. Operant, resulta $t = k+1$, d'on $k = t-1$. Per tant, i com a comprovació, $x = 2k+1 = 2(t-1)+1 = 2t-1$. En conseqüència, existeix un nombre enter t tal que $x = 2t-1$ (és suficient prendre $t = k+1$), és a dir, $x \in S_2$.

Subproblema 2. Anàlogament, demostrem que $S_2 \subseteq S_1$.

Això vol dir que $\forall x(x \in S_2 \to x \in S_1)$ és cert.

Fixem x, un element arbitrari. Hem de provar que $x \in S_2 \Rightarrow x \in S_1$.

Si $x \in S_2$, aleshores $x = 2t-1$ per a un determinat t enter (i x també és enter).

Vegem que existeix un enter k tal que $x = 2k+1$ ($\exists k(k \in \mathbb{Z} \wedge x = 2k+1)$). Imposem $2t-1 = x = 2k+1$. Operant resulta $t = k+1$, d'on $k = t-1$. Per tant, i com a comprovació, $x = 2t-1 = 2(k+1)-1 = 2k+1$. En conseqüència, existeix un nombre enter k tal que $x = 2k+1$ (és suficient prendre $k = t-1$), és a dir, $x \in S_1$.

Així, queden demostrades les dues inclusions i, en conseqüència, la igualtat dels conjunts. ■

Exemple 8.26 Proveu que $\{4p+6 | p \in \mathbb{Z}\} = \{4q-10 | q \in \mathbb{Z}\}$.

Denotem $A = \{4p+6 | p \in \mathbb{Z}\}$, $B = \{4q-10 | q \in \mathbb{Z}\}$.

Hem de demostrar que qualsevol element de A és de B i recíprocament, és a dir, qualsevol element de B és de A.

Equivalentment, hem de veure:

$\forall k(k \in \mathbb{Z} \to \exists k'(k' \in \mathbb{Z} \wedge 4k+6 = 4k'-10))$

$\forall k'(k' \in \mathbb{Z} \to \exists k(k \in \mathbb{Z} \wedge 4k'-10 = 4k+6))$

O bé:

$\forall p \in \mathbb{Z}\ \exists q \in \mathbb{Z}(4p+6 = 4q-10)$

$\forall q \in \mathbb{Z}\ \exists p \in \mathbb{Z}(4q-10 = 4p+6)$

Comencem estudiant quina relació hi ha entre p,q per a un element comú als dos conjunts:

$4p+6=4q-10 \Rightarrow 4(q-p)=16 \Rightarrow q-p=4.$

$A \subseteq B$: Vegem que $x \in A \Rightarrow x \in B$. Si $x \in A$, és $x=4p+6$ per a algun enter p. Prenent $q=4+p$ (relació anterior) és $p=q-4$ i, substituint, resulta $x=4(q-4)+6=4q+10$ i, per tant, $x \in B$.

$B \subseteq A$: Vegem que $x \in B \Rightarrow x \in A$. Si $x \in B$, és $x=4q-10$ per a algun enter q. Prenent $p=q-4$ (relació anterior) és $q=p+4$ i, substituint, resulta $x=4(p+4)-10=4p+6$ i, per tant, $x \in A$.

Això conclou la demostració de les dues inclusions i, per tant, la igualtat dels conjunts. ■

PROBLEMA 8.5

Proveu que són iguals els conjunts:

$A=\{n|n \in \mathbb{Z} \wedge n \text{ és senar} \wedge 3|n\}$

$B=\{6k+3|k \in \mathbb{Z}\}.$

Solució. Són dos subproblemes, que resoldrem separadament.

▷ Vegem $B \subseteq A$ (*subproblema 1*). Vegem que $x \in B \Rightarrow x \in A$.

Sigui $x \in B$ (hipòtesi). Cal veure $x \in A$ (tesi). Aleshores x és de la forma $x=6k+3$ per a algun k enter convenient. Vegem que x satisfà les propietats dels elements de A. En primer lloc, x és un enter. En segon lloc, és múltiple de 3, ja que $x=6k+3=3(2k+1)$. Finalment, $x=2(3k)+3$ és senar, ja que la suma d'un parell i un senar és senar. També es pot veure això últim directament: $x=2(3k)+3=2(3k+1)+1=2k'+1$, senar (amb $k'=3k+1$).

Per tant, $x \in A$.

▷ Vegem $A \subseteq B$ (*subproblema 2*). Vegem que $x \in A \Rightarrow x \in B$.

Sigui $x \in A$ (hipòtesi). Cal veure $x \in B$ (tesi). Aleshores x és enter, senar i múltiple de 3. Com que és múltiple de 3, és $x=3q$, per a algun q enter convenient.

Vegem que q és senar (per reducció a l'absurd o pel contrarecíproc). Si q no fos senar, és a dir, si fos parell, aleshores seria $3q$ parell, d'on x seria parell. Per tant, q és senar.

Hem de veure que $x=6k+3$ per a algun k enter convenient. Vegem que podem obtenir k tal que la igualtat anterior es compleixi. Imposem-ho: $6k+3=x=3q$, d'on $2k=q-1$. Essent q senar, $q-1$ és parell i, per tant, $k=\frac{q-1}{2} \in \mathbb{Z}$. Escollint, doncs, $k=\frac{q-1}{2}$, resulta el que ens cal: $6k+3=6(\frac{q-1}{2})+3=3(q-1)+3=3q$, com volíem veure.

Demostrada la doble inclusió, resulta demostrada la igualtat.

PROBLEMA 8.6

Proveu que són iguals els conjunts:

$A = \{x \in \mathbb{Z} | 2 | (13x+7)\}$

$B = \{x \in \mathbb{Z} | 2 \nmid x\}$

Solució. Observeu que es pot reformular:

$A = \{x \in \mathbb{Z} | 13x+7 \text{ és parell}\}$

$B = \{x \in \mathbb{Z} | x \text{ és senar}\}$

Què cal veure? Resolem dos subproblemes separadament: $A \subseteq B$ i $B \subseteq A$. Això vol dir que hem de demostrar $x \in A \Rightarrow x \in B$ i recíprocament, $x \in B \Rightarrow x \in A$.

▷ Vegem $A \subseteq B$ (*subproblema 1*). Vegem que $x \in A \Rightarrow x \in B$. Sigui $x \in A$ (hipòtesi). Vegem que $x \in B$ (tesi).

Per la hipòtesi, $13x+7$ és parell, és a dir, $13x+7 = 2k$, per a cert k enter, d'on $13x = 2k-7$, que és senar perquè és la diferència d'un parell i un senar (o també perquè $13x = 2(k-3)11$, senar). Ara bé, $13x$ és senar $\Rightarrow x$ és senar. En efecte, vegem-ho pel contrarecíproc: si x fos parell, seria $x = 2t$, per a un cert enter t i, per tant, $13x = 2(13t)$, parell (o directament: si x fos parell, $13x$ seria parell, la qual cosa és una contradicció). Així, doncs, $x \in B$.

▷ Vegem $B \subseteq A$ (*subproblema 1*). Vegem que $x \in B \Rightarrow x \in A$. Sigui $x \in B$ (hipòtesi). Provem que $x \in A$ (tesi).

Aleshores, per la hipòtesi, és $x = 2k+1$, per a un cert k enter. Hem de provar que $13x+7$ és parell. En efecte, $13x+7 = 13(2k+1)+7 = 2(13k)+20 = 2(13k+10) = 2k'$, que és parell (amb $k' = 13k+10$, enter). També es pot raonar dient: $13x$ és senar per ser producte de dos nombres senars; $13x+7$ és parell per ser suma de dos nombres senars.

PROBLEMA 8.7

Demostreu que els conjunts:

$A = \{3k | k \in \mathbb{Z}\}$ *(els múltiples de 3)*

$B = \{3(k+1) | k \in \mathbb{Z}\}$

$C = \{3(k+2) | k \in \mathbb{Z}\}$

$D = \{3k+9 | k \in \mathbb{Z}\}$

són iguals.

Solució. S'ha de demostrar per parelles. Primer, per exemple, $A = B$. Per transitivitat de la igualtat, no cal demostrar totes les igualtats possibles. Per exemple, provant les igualtats $A = B = C = D$ (és a dir, $A = B$, $B = C$, $C = D$), resoldríem el problema.

El conjunt D també es pot expressar com $D = \{3(k+3)|k \in \mathbb{Z}\}$ i es podria demostrar la igualtat amb A de manera similar als altres casos.

Vegem, doncs, $A = B$. Per exemple, veient les dues inclusions separadament:

$A \subseteq B$?

Sigui $x \in A$.

Aleshores $x = 3k$ per a un cert k enter. Vegem que es pot escriure de la forma $3(q+1)$, per a un q enter convenient. L'obtindrem imposant la igualtat: $3k = 3(q+1)$. Aleshores és $k = q+1$, d'on $q = k-1$, en funció de k. Tot i que no cal, podem comprovar que $3(q+1) = 3(k-1+1) = 3k$.

Per tant, $x \in B$.

Hem vist, doncs, que, per a un x arbitrari:

$x \in A \to x \in B$, d'on $\forall x(x \in A \to x \in B)$ és cert.

$B \subseteq A$?

Sigui $x \in B$.

Existeix un k enter tal que $x = 3(k+1)$, que és de la forma $3k'$, amb $k' = k+1 \in \mathbb{Z}$.
Per tant, $x \in A$.

Hem provat, doncs, que per a un x qualsevol,

$x \in B \to x \in A$, d'on $\forall x(x \in B \to x \in A)$.

De forma similar, es poden demostrar les altres igualtats, cosa que es deixa com a exercici.

8.4. El conjunt potència. Conjunt de les parts

Definició 8.4 (El conjunt dels subconjunts d'un conjunt) *Donat un conjunt A, el **conjunt de les parts de** A és el conjunt de tots els subconjunts de A. La notació corresponent és $\mathscr{P}(A)$. Així:*

$$\mathscr{P}(A) = \{B|B \subseteq A\}$$

Així, $B \subseteq A$ si, i només si, $B \in \mathscr{P}(A)$ (inclusió en termes de pertinença al conjunt de les parts).

El conjunt de les parts d'un conjunt A també s'anomena **conjunt potència** de A.

Sempre és no buit? Efectivament, sempre és no buit, ja que:

$\emptyset \subseteq A \Rightarrow \emptyset \in \mathscr{P}(A)$

$A \subseteq A \Rightarrow A \in \mathscr{P}(A)$

Per tant, $\mathscr{P}(A) \neq \emptyset$.

Malgrat que es pugui afirmar que $\emptyset \in \mathscr{P}(A)$ i $A \in \mathscr{P}(A)$, això no implica que hi hagi un mínim de dos elements, ja que pot ser que $A = \emptyset$.

$\mathscr{P}(\emptyset) = \{\emptyset\}$

Exemples 8.27

Exemple 1. $A = \emptyset$. És $\mathscr{P}(A) = \emptyset$

Exemple 2. $A = \{a\}$. És $\mathscr{P}(A) = \{\emptyset, \{a\}\} = \{\emptyset, A\}$

Exemple 3. $A = \{a,b\}$. És $\mathscr{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\} = \{\emptyset, \{a\}, \{b\}, A\}$

Exemple 4. $A = \{a,b,c\}$. Podem obtenir els conjunts de manera sistemàtica, considerant subconjunts dels diversos cardinals possibles:

Conjunts de 0 elements: $\emptyset$

Conjunts d'1 element: $\{a\}$, $\{b\}$, $\{c\}$

Conjunts de 2 elements: $\{a,b\}$, $\{a,c\}$, $\{b,c\}$

Conjunts de 3 elements: $\{a,b,c\}$ (el total)

Finalment, $\mathscr{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
També $\mathscr{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, A\}$.

Exemple 5. $\mathscr{P}(\{\ \{\{\{x\}\}\}\ \}) = \{\emptyset, \{\ \{\{\{x\}\}\}\ \}\}$. ■

8.5. Operacions conjuntistes: unió de conjunts

Definició 8.5 (Unió de dos conjunts) *Siguin A i B dos conjunts. Es defineix la **unió** de A i B com el conjunt dels elements que pertanyen a A o a B. És a dir, qualsevol dels següents:*

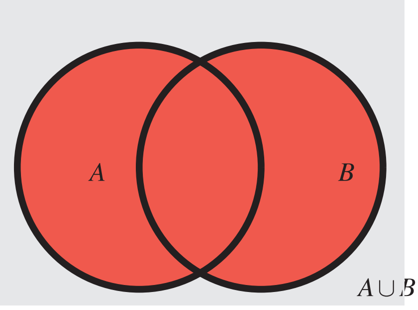
$A \cup B = \{x |\ x \in A \text{ o } x \in B\}$

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

$A \cup B = \{x :\ x \in A \text{ o } x \in B\}$

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

Observeu que la "o" o disjunció de la definició no és exclusiva, de manera que un element de la unió pot pertànyer a ambdós conjunts.



També s'anomena **reunió**.

Descrivim equivalentment la unió amb una fórmula de predicats:
$\forall x(x \in A \cup B \leftrightarrow (x \in A \vee x \in B))$.

Com obtenir la unió de dos conjunts?
A la pràctica, agafem tots els elements d'un conjunt, tots els de l'altre i formem un nou conjunt, eliminant les repeticions si n'hi ha.

Exemples 8.28

Exemple 1. $A = \{0,1,2,3\}$, $B = \{2,3,4,a,b\}$.

$A \cup B = \{0,1,2,3,4,a,b\}$.

Exemple 2. $A = \{0,1,2,3\}$, $B = \{2,3,4,a,\{0\},\emptyset\}$.

$A \cup B = \{0,1,2,3,4,a,\{0\},\emptyset\}$.

Exemple 3. $\{a,b,\{3\}\} \cup \{3,\{a\}\} = \{a,b,3,\{3\},\{a\}\}$.

Exemple 4. $\{x \in \mathbb{R} | 3 \leq x \leq 9\} \cup \{x \in \mathbb{R} | 6 \leq x \leq 12\} = \{x \in \mathbb{R} | 3 \leq x \leq 12\}$. En una altra notació, la d'intervals tancats en el conjunts dels nombres reals,

$[3,9] \cup [6,12] = [3,12]$.

Exemple 5. $\{x \in \mathbb{R} | x > 0\} \cup \{x \in \mathbb{R} | x \leq 0\} = \mathbb{R}$.

Exemple 6. $\{2k | k \in \mathbb{Z}\} \cup \{m \in \mathbb{Z} | \exists w(w \in \mathbb{Z} \wedge m = 2w+1)\} = \mathbb{Z}$.

Exemple 7. Com traduir en termes de conjunts que tot nombre enter és parell o senar?

$\mathbb{Z} = \{2k | k \in \mathbb{Z}\} \cup \{2q+1 | q \in \mathbb{Z}\}$.

Observeu que no diem aquí que només pot ser una de les dues coses (encara que sigui així).

Exemple 8. $(a,b) \cup \{a,b\} = [a,b]$ (intervals en $\mathbb{R}$).

Exemple 9. $A = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 < 1\}$ (cercle de centre $(0,0)$ i radi $R = 1$, sense el contorn circular, és a dir, sense la circumferència $x^2 + y^2 = 1$).

$B = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$ (circumferència de centre $(0,0)$ i radi $R = 1$).

$A \cup B = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 1\}$ (cercle de centre $(0,0)$ i radi $R = 1$, amb el contorn circular).

Exemple 10. $A = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 < 25\}$ (cercle de centre $(0,0)$ i radi $R = 5$, sense el contorn circular, és a dir, sense la circumferència $x^2 + y^2 = 25$).

$B = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 > 25\}$ (l'exterior de la circumferència de centre $(0,0)$ i radi $R = 5$).

$A \cup B$ és el conjunt de punts del pla bidimensional sense la circumferència $x^2 + y^2 = 25$. També $A \cup B = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \neq 25\}$.

Exemple 11. $[2,3] = \{2,3\} \cup (2,3) = \{2\} \cup (2,3) \cup \{3\}$.

Exemple 12. $[2,4] = [2,3] \cup [3,4]$. ■

Exemple 8.29 Considerem $A = \{x \in \mathbb{R} | x^2 - x + 2 \geq 0\}$.

Vegem com el podem expressar com a unió de dos conjunts. Resolent l'equació de segon grau $x^2 - x + 2 = 0$, en resulten les solucions $x = -1$ i $x = 2$. La gràfica de $y = x^2 - x + 2$ és una paràbola, oberta cap al semiplà de les $y \geq 0$, que interseca l'eix x en els punts $(-1,0)$ i $(2,0)$. Per tant:

$A = \{x \in \mathbb{R} | x \leq -1\} \cup \{x \in \mathbb{R} | x \geq 2\} = (-\infty, -1] \cup [2, \infty)$. ■

Ser de la unió

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

$x \in A \cup B$ si, i només si, $x \in A \vee x \in B$

Negació de ser de la unió (no ser de la unió). És intuïtiu: un element que no sigui de la unió no pot ser de cap dels dos conjunts, ja que si fos d'algun, aleshores pertanyeria a la unió, per definició d'unió. Es pot obtenir automatitzadament: la condició equivalent s'obté per negació de $x \in A \vee x \in B$, és a dir:

$\neg(x \in A \vee x \in B)$, que equival a (per De Morgan, lògica)

$\neg(x \in A) \wedge \neg(x \in B)$, és a dir,

$x \notin A \wedge x \notin B$

És a dir, $x \notin A \cup B \Leftrightarrow (x \notin A \wedge x \notin B)$.

Es pot generalitzar a tres conjunts o més, com veurem a continuació i al final.

Propietats bàsiques de la unió

Teorema 8.2 *Siguin A,B,C conjunts. Es compleix:*

a) $A \cup A = A$.

b) $A \cup B = B \cup A$ *(propietat commutativa de la unió).*

c) $(A \cup B) \cup C = A \cup (B \cup C)$ *(propietat associativa de la unió).*

d) $A \cup \emptyset = A$.

e) $A \subseteq A \cup B$, $B \subseteq A \cup B$.

f) $A \subseteq B$ *si, i només si,* $A \cup B = B$.

g) $A \cup B \subseteq C$ *si, i només si,* $A \subseteq C$ *i* $B \subseteq C$.

Comentari sobre la propietat associativa. Com a conseqüència de la propietat associativa, podem escriure $A \cup B \cup C$ sense cap ambigüitat, ja que és qualsevol de les anteriors.

Exemple 8.30

$A = \{4, a, x, y\}$

$B = \{x, z, t, w, 3\}$

$C = \{-1, 3, \{\emptyset\}\}$

$A \cup B \cup C = \{4, a, x, y, z, t, w, 3, -1, \{\emptyset\}\}$

$A \cup B \cup C = (A \cup B) \cup C = \{4, a, x, y, z, t, w, 3\} \cup \{-1, 3, \{\emptyset\}\} = \{4, a, x, y, z, t, w, 3, -1, \{\emptyset\}\}$

$A \cup B \cup C = A \cup (B \cup C) = \{4, a, x, y\} \cup \{x, z, t, w, 3, -1, \{\emptyset\}\} = \{4, a, x, y, z, t, w, 3, -1, \{\emptyset\}\}$

■

Per associativitat, podríem definir la reunió de més de dos, sempre reduint-la al cas de dos.

Per exemple, $A \cup B \cup C = (A \cup B) \cup C$. Per associativitat, no hi ha el problema potencial de si amb $A \cup (B \cup C)$ n'obtindríem un conjunt diferent, ja que ambdós han de coincidir.

Vegem, com a exemple d'aquesta manera de procedir:

$A \cup B \cup C \cup D =$

$= A \cup (B \cup C \cup D)$

$= A \cup (B \cup (C \cup D))$

En general, per a n conjunts, la definició es pot fer recursivament ("inductivament") en dos passos:

1. Pas inicial, definint la reunió per a dos conjunts, tal com s'ha fet anteriorment:

   $A_1 \cup A_2 = \{x \mid x \in A_1 \vee x \in A_2\}$

2. Fórmula recurrent:

   $A_1 \cup \cdots \cup A_n = (A_1 \cup \cdots \cup A_{n-1}) \cup A_n$, reunió de dos conjunts, ja definida.

Al final de la secció, donarem una definició directa de la unió de n conjunts (de fet, d'una col·lecció arbitrària de conjunts).

Demostracions

(**Vegem-les com a aplicació dels conceptes i les tècniques de demostració**. Algunes són pràcticament òbvies, però procurarem donar-ne argumentacions formals).

> Quan tenim dos conjunts definits per fórmules lògiques (fórmules de predicat), els conjunts són iguals si les fórmules lògiques són equivalents.

$A \cup A = A$ ("Reunir un conjunt amb si mateix és no fer res").

Demostració. És l'expressió conjuntista de l'equivalència $p \vee p \equiv p$, on substituïm $p = x \in A$. És a dir, $(x \in A \vee x \in A) \equiv x \in A$, cosa que, d'altra banda, és completament intuïtiva.

Cal veure que $\forall x(x \in A \cup A \leftrightarrow x \in A)$ és cert.

Hem de veure que, per a tot x arbitrari:

$x \in A \cup A \Leftrightarrow x \in A$, és a dir,

$(x \in A \vee x \in A) \Leftrightarrow x \in A$, que és òbviament cert.

$A \cup B = B \cup A$ (propietat commutativa de la unió)

Demostració. És conseqüència de $p \vee q \equiv q \vee p$, que, per substitució, dóna l'equivalència $x \in A \vee x \in B \equiv x \in B \vee x \in A$.

Tenim la igualtat dels conjunts si, i només si, $\forall x(x \in A \cup B \leftrightarrow x \in B \cup A)$, la qual cosa és òbvia.

$(A \cup B) \cup C = A \cup (B \cup C)$ (propietat associativa de la unió)

Demostració. Hem de veure que $\forall x(x \in (A \cup B) \cup C \leftrightarrow x \in A \cup (B \cup C))$ és cert.

És l'expressió conjuntista de la propietat associativa de la disjunció per a fórmules de proposició i predicats. De l'equivalència

$(p \vee q) \vee t \equiv p \vee (q \vee t)$ resulta que són equivalents:

$(x \in A \vee x \in B) \vee x \in C$ i $x \in A \vee (x \in B \vee x \in C)$ (per a x arbitrari).

Per tant:

$(A \cup B) \cup C =$

$= \{x | x \in (A \cup B) \vee x \in C\}$ (per definició de la unió de dos conjunts)

$= \{x|(x \in A \vee x \in B) \vee x \in C\}$ (per definició de la unió de dos conjunts)

$= \{x|x \in A \vee (x \in B \vee x \in C)\}$ (per associativitat de $\vee$)

$= \{x|x \in A \vee (x \in B \cup C)\}$ (per definició de la unió de dos conjunts)

$= \{x|x \in A \cup (B \cup C)\}$ (per definició de la unió de dos conjunts)

$= A \cup (B \cup C)$.

També es pot expressar d'una altra manera:

$x \in (A \cup B) \cup C \Leftrightarrow$

$\Leftrightarrow x \in (A \cup B) \vee x \in C$

$\Leftrightarrow (x \in A \vee x \in B) \vee x \in C$

$\Leftrightarrow x \in A \vee (x \in B \vee x \in C)$

$\Leftrightarrow x \in A \vee (x \in B \cup C)$

$\Leftrightarrow x \in A \cup (B \cup C)$

Així, $\forall x(x \in (A \cup B) \cup C \leftrightarrow x \in A \cup (B \cup C))$ és cert. O bé:

$x \in (A \cup B) \cup C \Rightarrow x \in A \cup (B \cup C)$ i, recíprocament:

$x \in A \cup (B \cup C) \Rightarrow x \in (A \cup B) \cup C$.

$A \cup \emptyset = A$ ("Reunir un conjunt amb si mateix és no fer res")

Demostració. Intuïtivament, fer la reunió amb el buit és no afegir cap element a A, amb la qual cosa la igualtat és evident.

$x \in A \vee x \in \emptyset$ equival a $x \in A$, ja que $x \in \emptyset$ sempre és fals. Alternativament:

$x \in A \vee x \in \emptyset$, que equival a $x \in A \vee \mathbb{F}$, que equival a $x \in A$.

$A \subseteq A \cup B$, $B \subseteq A \cup B$ ("La unió de dos conjunts sempre conté com a subconjunts els dos conjunts que la defineixen")

Demostració. Per a veure $A \subseteq A \cup B$, hem de veure que per a un x arbitrari, $x \in A \Rightarrow x \in A \cup B$, és a dir, $x \in A \Rightarrow (x \in A \vee x \in B)$, que és obvi, o bé, més formalment, perquè $p \rightarrow (p \vee q)$ és tautologia. També, més senzillament, per la pròpia definició d'unió.

Alternativament, pel contrarecíproc, podem intentar veure que

$x \notin A \cup B \Rightarrow x \notin A$, és a dir, equivalentment, que $(x \notin A \wedge x \notin B) \Rightarrow x \notin A$, que és obvi. També, més formalment, perquè $(p \wedge q) \rightarrow p$ és una tautologia.

Anàlogament, per $B \subseteq A \cup B$. Cal veure que $\forall x(x \in B \rightarrow x \in A \cup B)$ és cert.

$A \subseteq B$ si, i només si, $A \cup B = B$

Demostració. Hem de provar $A \subseteq B \Leftrightarrow A \cup B = B$, és a dir, que

$\forall x(x \in A \to x \in B) \leftrightarrow \forall y(y \in A \cup B \leftrightarrow y \in B)$ és cert.

Cal provar dues implicacions:

$A \subseteq B \Rightarrow A \cup B = B$

$A \cup B = B \Rightarrow A \subseteq B$

$\Rightarrow$)? ($A \subseteq B \Rightarrow A \cup B = B$).

Hipòtesi: $A \subseteq B$

Tesi: $A \cup B = B$.

Per a demostrar $A \cup B = B$, hem de demostrar dues inclusions. Sempre es compleix la inclusió $B \subseteq A \cup B$, per definició d'unió (o per la propietat demostrada anteriorment). Vegem, doncs, l'altra inclusió:

$A \subseteq B \Rightarrow A \cup B \subseteq B$.

Cal, doncs, veure que, aplicant la hipòtesi, és $x \in A \cup B \Rightarrow x \in B$.

Sigui $x \in A \cup B$, arbitrari però fix. Tenim que $x \in A$ o $x \in B$. Aleshores, si $x \in B$, hem acabat; si $x \in A$, s'aplica la hipòtesi i resulta $x \in B$.

Exposició alternativa. Vegeu una altra forma d'exposar:

$$x \in A \cup B \Rightarrow \left\{ \begin{array}{l} x \in A \overset{A \subseteq B}{\Rightarrow} x \in B \\ \text{o} \\ x \in B \end{array} \right\} \Rightarrow x \in B$$

$\Leftarrow$)? ($A \cup B = B \Rightarrow A \subseteq B$).

Hipòtesi: $A \cup B = B$

Tesi: $A \subseteq B$

Cal, doncs, veure:

$\forall x(x \in A \cup B \leftrightarrow x \in B) \Rightarrow \forall y(y \in A \to y \in B)$.

Sigui $y \in A$. Vegem que $y \in B$ aplicant la hipòtesi $A \cup B = B$. És a dir, cal provar que, aplicant la hipòtesi, $y \in A \Rightarrow y \in B$.

En efecte, si $y \in A$, aleshores $y \in A \cup B$, d'on, per hipòtesi, $y \in B$.

$A \cup B \subseteq C$ si, i només si, $A \subseteq C$ i $B \subseteq C$

És el mateix que dir que $A \cup B \subseteq C \Leftrightarrow (A \subseteq C \text{ i } B \subseteq C)$

Demostració. (explicitem detalladament l'*estructura demostrativa* en els diversos mètodes):

Mètode 1. Observeu que:

- a l'esquerra (de $\Leftrightarrow$) estem dient, per a tot x: $(x \in A \vee x \in B) \rightarrow x \in C$
- a la dreta (de $\Leftrightarrow$) estem dient, per a tot x: $(x \in A \rightarrow x \in C) \wedge (x \in B \rightarrow x \in C)$

Són equivalents, cosa que deriva de l'equivalència:

$(p \vee q) \rightarrow t \equiv ((p \rightarrow t) \wedge (q \rightarrow t))$.

Mètode 2. També es pot explicar d'altres maneres. Per a demostrar l'equivalència hem de demostrar dues implicacions:

$A \cup B \subseteq C \Rightarrow ((A \subseteq C) \wedge (B \subseteq C))$

$((A \subseteq C) \wedge (B \subseteq C)) \Rightarrow A \cup B \subseteq C$.

Primera implicació. Vegem $A \cup B \subseteq C \Rightarrow ((A \subseteq C) \wedge (B \subseteq C))$.

Hipòtesi [H]: $A \cup B \subseteq C$

Tesi: $(A \subseteq C) \wedge (B \subseteq C)$

Primera part de la tesi (T1): $A \subseteq C$

Segona part de la tesi (T2): $B \subseteq C$

Cal provar: $H \Rightarrow T1$ i $H \Rightarrow T2$.

$(H \Rightarrow T1)$: $x \in A \Rightarrow x \in A \cup B \overset{Hip}{\Rightarrow} x \in C$

$(H \Rightarrow T2)$: $x \in B \Rightarrow x \in A \cup B \overset{Hip}{\Rightarrow} x \in C$

Segona implicació. Vegem $((A \subseteq C) \wedge (B \subseteq C)) \Rightarrow A \cup B \subseteq C$.

Hipòtesi: $(A \subseteq C) \wedge (B \subseteq C)$

H1 [hipòtesi (part 1)]: $A \subseteq C$

H2 [hipòtesi (part 2)]: $B \subseteq C$

Tesi: $A \cup B \subseteq C$

Sigui $x \in A \cup B$. Vegem que $x \in C$, és a dir, $x \in A \cup B \Rightarrow x \in C$.

Per ser $x \in A \cup B$, és $x \in A$ o $x \in B$. Si $x \in A$, aplicant que $A \subseteq C$ (H1), $x \in C$. Si $x \in B$, aplicant que $B \subseteq C$ (H2), aleshores $x \in C$.

De manera alternativa, directament:

$A \subseteq A \cup B \subseteq C$, $B \subseteq A \cup B \subseteq C$; per tant,

$(A \subseteq C \wedge B \subseteq C) \Rightarrow A \cup B \subseteq C \cup C = C$.

Observacions

1. Podem expressar $(A \cup B \subseteq C) \Rightarrow A \subseteq C$ mitjançant la fórmula

$\forall x(x \in A \cup B \rightarrow x \in C) \Rightarrow \forall y(y \in A \rightarrow y \in C)$.

1a. Contrarecíproc a l'interior de la fórmula (dreta):

$\forall x(x \in A \cup B \rightarrow x \in C) \Rightarrow \forall y(y \notin C \rightarrow y \notin A)$.

Vegem la prova: $y \notin C \Rightarrow y \notin A \cup B$ (aplicant la hipòtesi)

$y \notin A \cup B \Rightarrow y \notin A$, ja que sempre tenim $A \subseteq A \cup B$. Resumint:

$y \notin C \Rightarrow y \notin A \cup B \Rightarrow y \notin A$. Per tant,

$y \notin C \Rightarrow y \notin A$.

1b. Contrarecíproc global (tota la fórmula):

$\neg\forall y(y \in A \rightarrow y \in C) \rightarrow \neg\forall x(x \in A \cup B \rightarrow x \in C)$

$\exists y\neg(y \in A \rightarrow y \in C) \rightarrow \exists x\neg(x \in A \cup B \rightarrow x \in C)$

$\exists y(y \in A \wedge y \notin C) \rightarrow \exists x(x \in A \cup B \wedge x \notin C)$

És suficient escollir $x = y$, ja que $x = y \in A \Rightarrow x \in A \cup B$.

O bé es pot continuar amb el desenvolupament, convertint així la demostració en gairebé un automatisme:

$\exists y(y \in A \wedge y \notin C) \rightarrow \exists x(x \in A \cup B \wedge x \notin C)$

$\exists y(y \in A \wedge y \notin C) \rightarrow \exists x((x \in A \vee x \in B) \wedge x \notin C)$

$\exists y(y \in A \wedge y \notin C) \rightarrow \exists x((x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C))$

Observem la disjunció a la dreta (certa si un operand és cert):

$\exists y(y \in A \wedge y \notin C) \rightarrow \exists x((x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C))$

Agafem $x = y$.

1b (reformulat). Contrarecíproc en termes de conjunts:

$\neg(A \subseteq C) \Rightarrow \neg(A \cup B \subseteq C)$

Hipòtesi: $\neg(A \subseteq C)$

Tesi: $\neg(A \cup B \subseteq C)$

Per la hipòtesi, existeix $z \in A$ tal que $z \notin C$. Hem de veure que existeix $x \in A \cup B$ tal que $x \notin C$. Prenent $x = z$ se satisfà la condició $x \in A \cup B$, ja que $A \subseteq A \cup B$.

2. Es pot demostrar $((A \subseteq C) \wedge (B \subseteq C)) \Rightarrow A \cup B \subseteq C$ pel contrarecíproc. Cal provar: $\neg(A \cup B \subseteq C) \Rightarrow \neg((A \subseteq C) \wedge (B \subseteq C))$.

$\neg(A \cup B \subseteq C) \Rightarrow (\neg(A \subseteq C) \vee \neg(B \subseteq C))$

Existeix $x \in A \cup B$ tal que $x \notin C$, és a dir,

existeix x tal que $x \in A \vee x \in B$, i tal que $x \notin C$, és a dir (per distributivitat de $\wedge$ respecte de $\vee$),

existeix x tal que $x \in A \wedge x \notin C$, o tal que $x \in B \wedge \notin C$, és a dir,

$\neg(A \subseteq C) \vee \neg(B \subseteq C)$.

De manera alternativa, directament, cal veure que és cert:

$(\forall x(x \in A \rightarrow x \in C) \wedge \forall y(x \in B \rightarrow x \in C)) \rightarrow \forall z(z \in A \cup B \rightarrow z \in C)$.

Escrivim fórmules equivalents al contrarecíproc que pràcticament automatitzen l'argumentació:

$\neg\forall z(z \in A \cup B \rightarrow z \in C) \rightarrow \neg[\forall x(x \in A \rightarrow x \in C) \wedge \forall y(x \in B \rightarrow x \in C)]$

$\exists z \neg(z \in A \cup B \rightarrow z \in C) \rightarrow [\neg\forall x(x \in A \rightarrow x \in C) \vee \neg\forall y(x \in B \rightarrow x \in C)]$

$\exists z \neg(z \in A \cup B \rightarrow z \in C) \rightarrow [\exists x \neg(x \in A \rightarrow x \in C) \vee \exists y \neg(x \in B \rightarrow x \in C)]$

$\exists z(z \in A \cup B \wedge z \notin C) \rightarrow [\exists x(x \in A \wedge x \notin C) \vee \exists y(x \in B \wedge x \notin C)]$

$\exists z((z \in A \vee z \in B) \wedge z \notin C) \rightarrow [\exists x(x \in A \wedge x \notin C) \vee \exists y(x \in B \wedge x \notin C)]$

$\exists z((z \in A \wedge z \notin C) \vee (z \in B \wedge z \notin C)) \rightarrow [\exists x(x \in A \wedge x \notin C) \vee \exists y(x \in B \wedge x \notin C)]$

És suficient prendre $x = z, y = z$.

Generalització: unió de *n* conjunts i d'una col·lecció arbitrària de conjunts

Sigui $A_1, \cdots, A_n$ conjunts. Definim:

$A_1 \cup \cdots \cup A_n = \{x | x \in A_1 \vee \cdots \vee x \in A_n\}$

O bé, segons diverses variants:

$A_1 \cup \cdots \cup A_n = \{x | x \in A_{i_0} \text{ per a algun } i_0 \in \{1, \cdots, n\}\}$

$A_1 \cup \cdots \cup A_n = \{x | x \in A_{i_0} \text{ per a algun nombre natural } i_0 \text{ tal que } 1 \leq i_0 \leq n\}\}$

$A_1 \cup \cdots \cup A_n = \{x | \exists k (k \in \{1, \cdots, n\} \wedge x \in A_k)\}$

$A_1 \cup \cdots \cup A_n = \{x | \exists i_0 (i_0 \in \mathbb{N} \wedge 1 \leq i_0 \leq n \wedge x \in A_{i_0})\}$

En aquest cas, podem considerar un conjunt, el dels índexs, $J = \{1, \cdots, n\}$, i podríem reexpressar els anteriors en termes de J, i també introduir-hi la notació:

$\bigcup_{i \in J} A_i$, o bé $\bigcup_{i=1}^{n} A_i$, i també $\bigcup_{1 \leq i \leq n} A_i$.

Exemple 8.31

$A = \{1, -2, t\}$
$B = \{3, a, z, \{z\}, t\}$
$C = \{a, 3, 4, 5, 6\}$
$A \cup B \cup C = \{1, -2, 3, 4, 5, 6, a, z, t, \{z\}\}$. ■

▷ Què vol dir que $x \in A \cup B \cup C$? Que $x \in A \vee x \in B \vee x \in C$.

▷ Què vol dir que $x \notin A \cup B \cup C$? Que $x \notin A \wedge x \notin B \wedge x \notin C$.

En general, $x \in A_1 \cup \cdots \cup A_n$ si, i només si, $x \in A_1 \vee \cdots \vee x \in A_n$.

Equivalentment:

$x \in A_1 \cup \cdots \cup A_n$ si, i només si, existeix i_0 tal que $1 \leq i_0 \leq n$ i $x \in A_{i_0}$.

En termes d'una fórmula de predicats:

$\exists k (k \in \mathbb{N} \wedge 1 \leq k \leq n \wedge x \in A_k)$

▷ Què vol dir que $x \notin A_1 \cup \cdots \cup A_n$?

Equival a dir que x no pertany a cap dels conjunts. La negació corresponent seria:

$\neg(x \in A_1 \vee \cdots \vee x \in A_n)$, que equival, per De Morgan (lògica) generalitzat, a:

$(\neg x \in A_1 \wedge \cdots \wedge \neg x \in A_n)$

$x \notin A_1 \wedge \cdots \wedge x \notin A_n$

És a dir, també, $\forall i ((i \in \mathbb{N} \wedge 1 \leq i \leq n) \rightarrow x \notin A_i)$.

Està clar, però també es pot deduir de forma automatitzada per la negació de

$\exists k(k \in \mathbb{N} \wedge 1 \leq k \leq n \wedge x \in A_k)$.

És a dir, tenim diverses equivalències:

$\neg\exists k(k \in \mathbb{N} \wedge 1 \leq k \leq n \wedge x \in A_k)$

$\forall k \neg(k \in \mathbb{N} \wedge 1 \leq k \leq n \wedge x \in A_k)$ (per negació del quantificador existencial)

$\forall k(\neg(k \in \mathbb{N} \wedge 1 \leq k \leq n) \vee \neg(x \in A_k))$ (per De Morgan (lògica))

$\forall k(\neg(k \in \mathbb{N} \wedge 1 \leq k \leq n) \vee x \notin A_k)$

$\forall k((k \in \mathbb{N} \wedge 1 \leq k \leq n) \rightarrow x \notin A_k)$ (per equivalència del condicional).

El conjunt dels índexs J pot no ser finit, ni tan sols format per naturals. Aleshores:

$$\bigcup_{i \in J} A_i = \{x | \exists k(k \in J \wedge x \in A_k)\}$$

Aquesta notació la necessitarem en el tema del conjunt quocient i particions.

Exemples 8.32 Per exemple, per a intervals en $\mathbb{R}$:

Exemple 1. $\bigcup_{n \in \mathbb{N}} [0,n] = \{x | x \in \mathbb{R} \wedge x \geq 0\}$

Exemple 2. $\bigcup_{x \in \mathbb{R}} [0,x] = \{w | w \in \mathbb{R} \wedge w \geq 0\}$

Exemple 3. $\bigcup_{x \in \mathbb{R}^+} [-x,x] = \mathbb{R}$

Exemple 4. $\bigcup_{n \in \mathbb{N}} [-2^n, 2^n] = \mathbb{R}$

Exemple 5. $\bigcup_{n \in \mathbb{N}} [-2^n, 3^n] = \mathbb{R}$

Exemple 6. $\bigcup_{m \in \mathbb{Z}} [m, m+1] = \mathbb{R}$ ■

8.6. Operacions conjuntistes: intersecció de conjunts

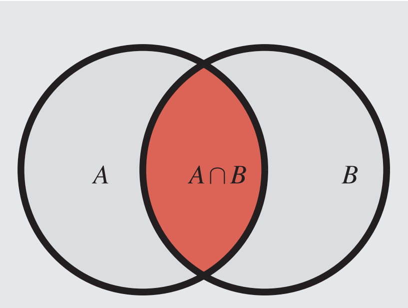
Definició 8.6 (intersecció de dos conjunts) *Siguin A i B dos conjunts. Es defineix la* ***intersecció*** *d'A i B com el conjunt dels elements que pertanyen a A i a B. És a dir, qualsevol de les següents:*

$A \cap B = \{x|\ x \in A \text{ i } x \in B\}$

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

$A \cap B = \{x :\ x \in A \text{ i } x \in B\}$

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



Equivalentment, amb una fórmula de predicats, tenim:

$\forall x(x \in A \cap B \leftrightarrow (x \in A \wedge x \in B)).$

Com obtenir la intersecció de dos conjunts?
A la pràctica, reunim tots els elements que són comuns als dos conjunts i en formem un de nou.

Exemples 8.33

Exemple 1. $A = \{0,1,2,3,b\}$, $B = \{2,3,4,a,b\}$.
$A \cap B = \{2,3,b\}$.

Exemple 2. $A = \{0,1,2,3\}$, $B = \{4,a,\{0\},\emptyset\}$, $A \cap B = \emptyset$ (disjunts).

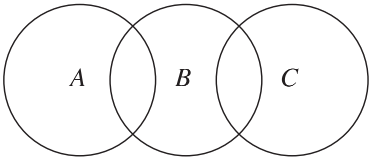
Exemple 3. $\{3,-1,z,x\} \cap \{z,t,w,\pi\} = \{z\}$.

Exemple 4. $\{\{x\},\{y,z\}\} \cap \{x,y,z\} = \emptyset$ (disjunts).

Exemple 5. $\{x \in \mathbb{R}|3 \leq x \leq 9\} \cap \{x \in \mathbb{R}|6 \leq x \leq 12\} = \{x \in \mathbb{R}|6 \leq x \leq 9\} = [6,9]$.

Exemple 6. $[-1,5] \cap [-3,0] = [-1,0]$ (intervals reals).

Exemple 7. La intersecció dels conjunts següents és buida: $A \cap B \cap C = \emptyset$ (disjunts).



Exemple 8. $\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 4\} \cap \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \geq 1\} =$
$= \{(x,y) \in \mathbb{R}^2 | 1 \leq x^2 + y^2 \leq 4\}$, una corona circular, determinada per les circumferències de centre $(0,0)$ i radis $R_1 = 1$ i $R_2 = 2$.

Exemple 9. $\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 4\} \cap \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \geq 4\} =$

$= \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 4\}$, circumferència de centre l'origen i de radi 2. El conjunt $\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 4\}$ és el cercle del pla bidimensional, de centre $C = (0,0)$ i de radi $R = 4$.

Exemple 10. $[a,b] \cap [b,c] = \{b\}$ (intervals reals).

Exemple 11. $[a,b] \cap (b,c) = \emptyset$ (intervals reals).

Exemple 12. $\{x \in \mathbb{Q} | x \geq 0\} \cap \{x \in \mathbb{Q} | x \leq 0\} = \{0\}$. ■

Exemple 8.34

$A = \{(x,y) \in \mathbb{R}^2 | y = x\}$ (bisectriu del 1r i el 3r quadrants del pla bidimensional).

$B = \{(x,y) \in \mathbb{R}^2 | y = -x\}$ (bisectriu del 2n i el 4t quadrants del pla bidimensional).

És $A \cap B = \{(x,y) \in \mathbb{R}^2 | y = x \wedge y = -x\} = \{(0,0)\}$.

Analíticament, cal resoldre el sistema $y = x$; $y = -x$, d'on $x = -x$, de manera que $x = 0$ i, per tant, $y = 0$. Així, l'única solució és $(0,0)$. En conseqüència, $A \cap B = \{(0,0)\}$. En aquest cas, també s'arriba a la mateixa conclusió atenent el significat geomètric (intersecció de les dues rectes). ■

Exemple 8.35

$A = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$ és el conjunt de punts del pla format per la circumferència de centre $(0,0)$ i de radi $R = 1$.

$B = \{(x,y) \in \mathbb{R}^2 | (x-1)^2 + y^2 = 2\}$ és el conjunt de punts del pla format per la circumferència de centre $(1,0)$ i de radi $R = \sqrt{2}$.

La intersecció $A \cap B = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 1 \wedge (x-1)^2 + y^2 = 2\}$ s'obté resolent el sistema d'equacions:

$$\begin{cases} x^2 + y^2 = 1 \\ (x-1)^2 + y^2 = 2 \end{cases}$$

per a obtenir els punts d'intersecció de les circumferències.

Es desenvolupa el quadrat a la segona ($x^2 - 2x + 1 + y^2 = 2$) i se substitueix $x^2 + y^2$ per 1 (primera); se n'obté $x = 0$, que substituïm a la primera. Resulta $x = 0$, d'on $y = \pm 1$ i, per tant, els punts són $(0,1)$ i $(0,-1)$.

Així, $A \cap B = \{(0,1),(0,-1)\}$. ■

Exemple 8.36 Demostreu:

$\{3n|n \in \mathbb{Z}\} \cap \{5m|m \in \mathbb{Z}\} = \{15r|r \in \mathbb{Z}\}$.

Observeu que:

$A = \{3n|n \in \mathbb{Z}\} = \{x \in \mathbb{Z}|\ 3|x\}$ (conjunt dels múltiples de 3).

$B = \{5n|n \in \mathbb{Z}\} = \{x \in \mathbb{Z}|\ 5|x\}$ (conjunt dels múltiples de 5).

$C = \{15n|n \in \mathbb{Z}\} = \{x \in \mathbb{Z}|\ 15|x\}$ (conjunt dels múltiples de 15).

$A \cap B = \{x \in \mathbb{Z}|\ 3|x \wedge 5|x\}$.

Veure que $A \cap B = C$ equival a veure $(3|x \wedge 5|x) \Leftrightarrow 15|x$, és a dir, que $\forall x(x \in A \cap B \leftrightarrow x \in C)$ és cert, o sigui que $\forall x((3|x \wedge 5|x) \leftrightarrow 15|x)$ és cert.

Cal provar dues inclusions:

Part 1. $C \subseteq A \cap B$?. Volem veure $x \in C \Rightarrow x \in A \cap B$.

Hipòtesi: $x \in C$

Tesi: $x \in A \cap B$

Sigui $x \in C$. (Què cal veure?: $x \in A \cap B$).

Aleshores existeix $k \in \mathbb{Z}$ tal que $x = 15k$. D'una banda, és $x = 3(5k)$, múltiple de 3 i, per tant, $x \in A$; d'altra banda, és $x = 5(3k)$, múltiple de 5 i, per tant, $x \in B$.

Així, $x \in A \cap B$.

Part 2. $A \cap B \subseteq C$? Cal veure $x \in A \cap B \Rightarrow x \in C$.

Hipòtesi: $x \in A \cap B$.

Tesi: $x \in C$.

Sigui $x \in A \cap B$. (Què cal veure?: $x \in C$).

Per ser $x \in A$, és $x = 3k$ per a algun k enter. Per ser $x \in B$, és $x = 5t$ per a algun t enter. Així, $3k = 5t$. Tenim $3|3k$ i, per tant, $3|5t$. Per aplicació d'un teorema ben conegut d'Euclides, que afirma que, si p primer i $p|ab$, aleshores $p|a$ o $p|b$; en aquest cas, $p = 3$, $a = 5$, $b = t$. Per tant, $3|t$, és a dir, $t = 3t'$ per a cert t' enter, i així $x = 5t = 5(3t') = 15t'$, d'on

$x \in C$.

Argument alternatiu. També es pot arribar a la mateixa conclusió sense aplicar el teorema esmentat, fent una demostració *per reducció a l'absurd*: partim de $3k = 5t$; afirmem que $3|t$. Suposem $3 \nmid t$. Si t no és múltiple de 3, aleshores, considerant la divisió entera (de t entre 3) $t = 3q + r$, amb $0 \leq r < 3$, és $1 \leq r \leq 2$. I ara, *per casos*. Es consideren dos casos segons els valors de r possibles:

Cas 1: $r = 1$. És $t = 3q + 1$. Substituint, $3k = 5t = 5(3q + 1)$, d'on $3k - 3(5q) = 5$, d'on $3(k - 5q) = 5$. Com que $3|3(k - 5q)$, seria $3|5$, absurd.

Cas 2: $r = 2$. És $t = 3q + 2$. Substituint, $3k = 5t = 5(3q + 2)$, d'on $3k - 3(5q + 3) = 1$, d'on $3(k - 5q - 3) = 1$. Atès que $3|3(k - 5q - 3)$, seria $3|1$, absurd.

Per tant, $3|t$ i l'argumentació es completa com abans. ■

Definició 8.7 (Conjunts disjunts) *Dos conjunts són disjunts si la seva intersecció és buida. Els conjunts A i B són disjunts si $A \cap B = \emptyset$.*

El concepte es pot estendre a més conjunts.

Exemples 8.37

Exemple 1. $[-1,0] \cap [4,7] = \emptyset$ (intervals reals).

Exemple 2. $\{2n | n \in \mathbb{Z}\} \cap \{2m + 1 | m \in \mathbb{Z}\} = \emptyset$ (intersecció de parells i senars). Vegem per què mitjançant una demostració *per reducció a l'absurd*. Estem afirmant (n, m enters) $\forall n \forall m (2n \neq 2m + 1)$, és a dir, que no hi ha cap element comú de la intersecció. Si ho neguem, tindrem $\exists n \exists m (2n = 2m + 1)$; vegem que arribem a una contradicció. Tenim $2n - 2m = 1$, d'on $2(n - m) = 1$. Ara bé, $2|2(n - m)$; per tant, $2|1$, absurd.

Exemple 3. $\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 4\} \cap \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 1\} = \emptyset$ (dues circumferències disjuntes: ambdues de centre $C = (0,0)$), la primera de radi $R = 2$, la segona de radi $R' = 1$. Recordi el lector que l'equació de la circumferència del pla de centre (a,b) i radi R és $(x - a)^2 + (y - b)^2 = R^2$.

Per *reducció a l'absurd*. Si, per a algun (x,y) fos $x^2 + y^2 = 4$ i $x^2 + y^2 = 1$, seria $4 = x^2 + y^2 = 1$, absurd.

Exemple 4. $\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 4\} \cap \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \geq 9\} = \emptyset$.

Exemple 5. $\{x \in \mathbb{Q} | x > 0\} \cap \{x \in \mathbb{Q} | x < 0\} = \emptyset$. ■

Exemple 8.38 Siguin:

$A = \{4p + 6 | p \in \mathbb{Z}\}$

$B = \{4q - 12 | q \in \mathbb{Z}\}$.

Vegem que són disjunts.

En fem la demostració *per reducció a l'absurd*. Suposem que $A \cap B \neq \emptyset$. Vegem que arribem a alguna contradicció.

Sigui $x \in A \cap B$.

Essent de A, es pot expressar $x = 4p + 6$ per a algun p enter; essent de B, és $x = 4q - 12$, per a algun enter q. Així, $4p + 6 = 4q - 12$. Aleshores $4(q - p) = 12 + 6 = 18$, d'on $2(q - p) = 9$. Atès que $2|2(q - p)$, resulta $2|9$, absurd. ■

Definició 8.8 (Conjunts disjunts dos a dos o mútuament disjunts) *Siguin $A_1, \cdots, A_n$ conjunts. Es diu que són dos a dos disjunts, si ho són cada dos. És a dir:*

Per a tot i, j, $i \neq j$, $1 \leq i \leq n$, $1 \leq j \leq n$, és $A_i \cap A_j = \emptyset$.

Més formalment:

$\forall i \forall j((1 \leq i \leq n \wedge 1 \leq j \leq n \wedge i \neq j) \rightarrow A_i \cap A_j = \emptyset)$

Es pot generalitzar a una col·lecció arbitrària de conjunts no necessàriament finita.

Com negar aquesta propietat?

Exemple 8.39 $[-1, 1]$, $[2, 3]$, $[4, 6]$ són conjunts dos a dos disjunts. ■

Ser de la intersecció de dos conjunts

$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$

$x \in A \cap B$ si, i només si, $x \in A \wedge x \in B$

Negació de ser de la intersecció (no ser de la intersecció de dos conjunts). És intuïtiu: un element no és de la intersecció si, i només si, no és d'algun dels dos ja que si fos de tots dos, aleshores pertanyeria a la intersecció, per definició d'intersecció. Es pot obtenir automatitzadament la fórmula corresponent de predicats: la condició equivalent s'obté per negació de $x \in A \wedge x \in B$, és a dir:

$\neg(x \in A \wedge x \in B)$, que equival a (per De Morgan, lògica)

$\neg(x \in A) \vee \neg(x \in B)$, és a dir:

$x \notin A \vee x \notin B$ (canvi de notació).

Per tant:

$x \notin A \cap B$ si, i només si, $x \notin A \vee x \notin B$.

$x \notin A \cap B \Leftrightarrow x \notin A \vee x \notin B$

$\forall x(x \notin A \cap B \leftrightarrow x \notin A \vee x \notin B)$

Es pot generalitzar a tres conjunts o més, com veurem al final.

Propietats bàsiques de la intersecció

Teorema 8.3 *Siguin A, B, C conjunts. Aleshores:*

a) $A \cap A = A$

b) $A \cap B = B \cap A$ *(propietat commutativa de la intersecció)*

c) $(A \cap B) \cap C = A \cap (B \cap C)$ *(propietat associativa de la intersecció)*

d) $A \cap \emptyset = \emptyset$

e) $A \cap B \subseteq A$, $A \cap B \subseteq B$

f) $A \subset B \Leftrightarrow A \cap B = A$

g) $C \subseteq A \cap B$ *si, i només si,* $C \subseteq A$ *i* $C \subseteq B$

Com a conseqüència de la propietat associativa, podem escriure $A \cap B \cap C$ sense cap ambigüitat, ja que és qualsevol de les anteriors.

Exemple 8.40

$A = \{4, a, x, y, 3, b\}$, $B = \{x, z, t, w, 3, b\}$, $C = \{-1, 3, x, \{\emptyset\}\}$

$A \cap B \cap C = \{3, x\}$
$A \cap B \cap C = (A \cap B) \cap C = \{x, 3, b\} \cap \{-1, 3, x, \{\emptyset\}\} = \{x, 3\}$

$A \cap B \cap C = A \cap (B \cap C) = \{4, a, x, y, 3, b\} \cap \{x, 3\} = \{x, 3\}$. ■

Per associativitat, podríem definir la intersecció de més de dos conjunts, sempre reduint-la al cas de dos. Per exemple, $A \cap B \cap C = (A \cap B) \cap C$. Per l'associativitat, no hi ha el problema potencial de si amb $A \cap (B \cap C)$ obtindríem un conjunt diferent, ja que ambdós han de coincidir.

Vegem, com a exemple d'aquesta manera de procedir:

$A \cap B \cap C \cap D =$

$= A \cap (B \cap C \cap D)$

$= A \cap (B \cap (C \cap D))$

En general, per a n conjunts, la definició es pot fer recursivament ("inductivament") en dos passos:

1. Pas inicial, definint la intersecció per a dos conjunts, tal com s'ha fer anteriorment:

$A_1 \cap A_2 = \{x |\ x \in A_1 \wedge x \in A_2\}$

2. Fórmula recurrent:

$A_1 \cap \cdots \cap A_n = (A_1 \cap \cdots \cap A_{n-1}) \cap A_n$ (intersecció de dos conjunts, ja definida)

Al final de la secció, donarem una definició directa de la intersecció de n conjunts (de fet, d'una col·lecció arbitrària de conjunts).

Demostracions (exercicis de demostració i de tècniques demostratives)

$A \cap A = A$

$\forall x(x \in A \cap A \leftrightarrow x \in A)$, que equival a

$\forall x((x \in A \wedge x \in A) \leftrightarrow x \in A)$.

Demostració. És una obvietat, però es pot justificar formalment.

Tenim $(p \wedge p) \equiv p$ o bé $(p \wedge p) \leftrightarrow p$ és cert o bé $(p \wedge p) \Leftrightarrow p$.

Així, $(x \in A \wedge x \in A) \Leftrightarrow x \in A$.

Per tant, $\forall x((x \in A \wedge x \in A) \leftrightarrow x \in A)$ és cert.

Una altra argumentació: $A \cap A = \{x|x \in A \wedge x \in A\} = \{x|x \in A\} = A$, ja que $x \in A \wedge x \in A \equiv x \in A$.

$A \cap B = B \cap A$ (propietat commutativa de la intersecció)

$\forall x(x \in A \cap B \leftrightarrow x \in B \cap A)$, que equival a

$\forall x((x \in A \wedge x \in B) \leftrightarrow (x \in B \wedge x \in A))$.

Demostració. És una obvietat; conceptualment és clar. Però es pot justificar formalment:

És conseqüència de $p \wedge q \equiv q \wedge p$, d'on l'equivalència de $x \in A \wedge x \in B$ i de $x \in B \wedge x \in A$. Per tant:

$A \cap B =$

$= \{x|x \in A \wedge x \in B\}$ (per definició de $\cap$)

$= \{x|x \in B \wedge x \in A\}$ (per equivalència de commutativitat de $\wedge$)

$= B \cap A$ (per definició de $\cap$)

$(A \cap B) \cap C = A \cap (B \cap C)$ (propietat associativa de la intersecció)

Hem de veure $\forall x(x \in (A \cap B) \cap C \leftrightarrow x \in A \cap (B \cap C))$, que equival a

$\forall x(((x \in A \wedge x \in B) \wedge x \in C) \leftrightarrow (x \in A \wedge (x \in B \wedge x \in C)))$.

Demostració

– És l'expressió conjuntista de la propietat associativa de la conjunció lògica per a fórmules de proposició i predicats. De l'equivalència

  $(p \wedge q) \wedge t \equiv p \wedge (q \wedge t)$

  resulta que són equivalents:

  $(x \in A \wedge x \in B) \wedge x \in C$ i $x \in A \wedge (x \in B \wedge x \in C)$. Per tant, els conjunts anteriors coincideixen.

– També ho podem expressar de la manera següent:

  $(A \cap B) \cap C = \{x|x \in (A \cap B) \wedge x \in C\}$ (per definició de $\cap$)

$= \{x | (x \in A \wedge x \in B) \wedge x \in C\}$ (per definició de $\cap$)

$= \{x | x \in A \wedge (x \in B \wedge x \in C)\}$ (per associativitat de $\wedge$)

$= \{x | x \in A \wedge (x \in B \cap C)\}$ (per definició de $\cap$)

$= \{x | x \in A \cap (B \cup C)\}$ (per definició de $\cap$)

$= A \cap (B \cap C)$.

– També es pot expressar d'una altra manera, per definició de la intersecció i per l'equivalència d'associativitat de la conjunció:

$x \in (A \cap B) \cap C \Leftrightarrow$

$\Leftrightarrow x \in (A \cap B) \wedge x \in C$

$\Leftrightarrow (x \in A \wedge x \in B) \wedge x \in C$

$\Leftrightarrow x \in A \wedge (x \in B \wedge x \in C)$

$\Leftrightarrow x \in A \wedge (x \in B \cap C)$

$\Leftrightarrow x \in A \cap (B \cap C)$

$A \cap \emptyset = \emptyset$

$\forall x(x \in A \cap \emptyset \leftrightarrow x \in \emptyset)$, que és equivalent a

$\forall x((x \in A \wedge x \in \emptyset) \leftrightarrow x \in \emptyset)$.

Demostració. Conceptualment, és clar i evident, per la definició de $\cap$ i pel fet que $\emptyset$ no conté cap element.

Per reducció a l'absurd, suposem que $A \cap \emptyset \neq \emptyset$. Si fos $A \cap \emptyset \neq \emptyset$, existiria algun x tal que $x \in A \cap \emptyset$, d'on $x \in A$ i $x \in \emptyset$, que és fals. Arribem a la contradicció que el conjunt buit té algun element (és a dir, que el conjunt buit és no buit!). Per tant, ha de ser $A \cap \emptyset = \emptyset$.

Mètode alternatiu. Si utilitzem el resultat que es demostra a l'apartat següent, es pot demostrar així:

$\emptyset \subseteq A \cap \emptyset$ (sempre: el buit és subconjunt de qualsevol conjunt)

$A \cap \emptyset \subseteq \emptyset$ (per la propietat de l'apartat següent)

Per la doble inclusió anterior, en resulta la igualtat ($\emptyset \subseteq A \cap \emptyset \subseteq \emptyset$, d'on la igualtat $A \cap \emptyset = \emptyset$).

$A \cap B \subseteq A$, $A \cap B \subseteq B$

Demostració. Conceptualment, és clar, ja que els elements de la intersecció pertanyen als dos conjunts i, per tant, a qualsevol dels dos. Formalment, vegem, per exemple, la primera. La segona es justificaria anàlogament.

$A \cap B \subseteq A$?

Cal veure que $x \in A \cap B \Rightarrow x \in A$, o bé:

$\forall x(x \in A \cap B \rightarrow x \in A)$.

Hipòtesi: $x \in A \cap B$

Tesi: $x \in A$

És $x \in A \cap B \Rightarrow (x \in A \wedge x \in B) \Rightarrow x \in A$, ja que:

$(p \wedge q) \rightarrow p$
$(p \wedge q) \rightarrow q$

són certes sempre (tautologies) i, per tant, $(p \wedge q) \Rightarrow p$ i $(p \wedge q) \Rightarrow q$.

Així, $A \cap B \subseteq A$.

Alternativament, per reducció a l'absurd. Cal veure que $\forall x(x \in A \cap B \rightarrow x \in A)$. Partim de la negació $\exists x \neg(x \in A \cap B \rightarrow x \in A)$ i arribem a una contradicció:

$\exists x(x \in A \cap B \wedge x \notin A)$

$\exists x(x \in A \wedge x \in B \wedge x \notin A)$,

que és absurd, ja que s'afirma que, per a algun x, és $x \in A$ i $x \notin A$.

L'anterior demostració per reducció a l'absurd també es por formular segons una altra variant, en termes del complementari:

$\exists x(x \in A \cap B \wedge x \in A^c)$

$\exists x(x \in A \cap B \cap A^c)$

$\exists x(x \in (A \cap A^c) \cap B)$

$\exists x(x \in \emptyset \cap B)$

$\exists x(x \in \emptyset)$, que és absurd.

Anàlogament per a $A \cap B \subseteq B$.

$A \subseteq B$ si, i només si, $A \cap B = A$, és a dir:

$A \subseteq B \Leftrightarrow A \cap B = A$

Demostració (cal demostrar dues implicacions)

Part 1 (subproblema 1)

$\Leftarrow$) És a dir, $A \cap B = A \Rightarrow A \subseteq B$.

En altres termes:

$\forall x(x \in A \cap B \leftrightarrow x \in A) \rightarrow \forall y(y \in A \rightarrow y \in B)$ és cert.

Ara, la hipòtesi [H] és $A \cap B = A$.

Tesi: $A \subseteq B$

Volem veure $x \in A \Rightarrow x \in B$, per a tot x.

En efecte, $x \in A \overset{[H]}{\Rightarrow} x \in A \cap B \overset{A \cap B \subseteq B}{\Rightarrow} x \in B$.

Part 2 (subproblema 2)

$\Rightarrow$) És a dir, $A \subseteq B \Rightarrow A \cap B = A$.

Ara, la hipòtesi $[H]$ és $A \subseteq B$.

I la tesi és $A \cap B = A$, és a dir, $A \cap B \subseteq A$ i $A \subseteq A \cap B$.

Sempre és $A \cap B \subseteq A$, de manera que només cal provar $A \subseteq A \cap B$, aplicant la hipòtesi. Vegem, doncs, que

$x \in A \overset{A \subseteq B [H]}{\Longrightarrow} x \in A \cap B$.

En efecte, sigui $x \in A$. Per $A \subseteq B$ ([H]), és $x \in B$ (i continuem tenint $x \in A$). Per tant, $x \in A \cap B$.

$C \subseteq A \cap B$ si, i només si, $C \subseteq A$ i $C \subseteq B$

$C \subseteq A \cap B \Leftrightarrow (C \subseteq A \text{ i } C \subseteq B)$

Demostració (cal demostrar dues implicacions)

Subproblema 1 ($\Rightarrow$)

$C \subseteq A \cap B \subseteq A$, d'on $C \subseteq A$

$C \subseteq A \cap B \subseteq B$, d'on $C \subseteq B$.

Subproblema 2 ($\Leftarrow$)

Hipòtesi: $(C \subseteq A \text{ i } C \subseteq B)$

H1: $C \subseteq A$

H2: $C \subseteq B$

Tesi T: $C \subseteq A \cap B$

Estructura: $(H1 \wedge H2) \rightarrow T$

Sigui $x \in C$. Vegem que $x \in A \cap B$, aplicant la hipòtesi ($C \subseteq A$ i $C \subseteq B$).

Per H1, és $x \in A$; per H2, és $x \in B$. Per tant, $x \in A \cap B$. Queda demostrat.

Alternativament: Sigui $x \in C$. Amb aquest supòsit, despleguem la hipòtesi:

$(x \in C \rightarrow x \in A) \wedge (x \in C \rightarrow x \in B)$, que equival a

$(x \notin C \vee x \in A) \wedge (x \notin C \vee x \in B)$, que equival a

$x \notin C \vee (x \in A \wedge x \in B)$, que equival a

$x \in C \rightarrow (x \in A \wedge x \in B)$, que equival a

$x \in C \rightarrow x \in A \cap B$

Generalització: intersecció de *n* conjunts i d'una col·lecció arbitrària de conjunts

Sigui $A_1, \cdots, A_n$ conjunts. Definim:

$A_1 \cap \cdots \cap A_n = \{x | x \in A_1 \wedge \cdots \wedge x \in A_n\}$

Els elements de la intersecció són els que són comuns a tots els conjunts.

O bé:

$A_1 \cap \cdots \cap A_n = \{x | x \in A_i$ per a tot $i \in \{1, \cdots, n\}\}$

$A_1 \cap \cdots \cap A_n = \{x | x \in A_i$ per a tot nombre natural i tal que $1 \leq i \leq n\}\}$

$A_1 \cap \cdots \cap A_n = \{x | \forall k (k \in \{1, \cdots, n\} \rightarrow x \in A_k)\}$

$A_1 \cap \cdots \cap A_n = \{x | \forall i ((i \in \mathbb{N} \wedge 1 \leq i \leq n) \rightarrow x \in A_i)\}$

En aquest cas, podem considerar un conjunt, el dels índexs, $J = \{1, \cdots, n\}$, i podríem reexpressar els anteriors en termes de J, i també introduir la notació:

$\bigcap_{i \in J} A_i$, o bé $\bigcap_{i=1}^{n} A_i$, i també $\bigcap_{1 \leq i \leq n} A_i$.

Exemple 8.41

$A = \{1, -2, t, a\}$

$B = \{3, a, z, \{z\}, t\}$

$C = \{a, 3, 4, 5, 6\}$

$A \cap B \cap C = \{a\}$. ■

▷ Què vol dir que $x \in A \cap B \cap C$? Que $x \in A \wedge x \in B \wedge x \in C$

▷ Què vol dir que $x \notin A \cap B \cap C$? Que $x \notin A \vee x \notin B \vee x \notin C$

En general, $x \in A_1 \cap \cdots \cap A_n$ si, i només si, $x \in A_1 \wedge \cdots \wedge x \in A_n$.

Equivalentment, $x \in A_1 \cap \cdots \cap A_n$ si, i només si, per a tot i tal que $1 \leq i \leq n$, és $x \in A_i$. En termes d'una fórmula de predicats:

$\forall k((k \in \mathbb{N} \wedge 1 \leq k \leq n) \to x \in A_k)$, és a dir:

$(x \in A_1 \cap \cdots \cap A_n) \leftrightarrow \forall k((k \in \mathbb{N} \wedge 1 \leq k \leq n) \to x \in A_k)$. ▷ Què vol dir que $x \notin A_1 \cap \cdots \cap A_n$? Equival a dir que x no pertany a algun dels conjunts. La negació corresponent seria:

$\neg(x \in A_1 \wedge \cdots \wedge x \in A_n)$, que equival, per De Morgan (lògica) generalitzat, a:

$(\neg x \in A_1 \vee \cdots \vee \neg x \in A_n)$

$x \notin A_1 \vee \cdots \vee x \notin A_n$

És a dir, també, $\exists i((i \in \mathbb{N} \wedge 1 \leq i \leq n) \wedge x \notin A_i)$.

Està clar, però també es pot deduir de forma automatitzada per la negació de

$\forall k((k \in \mathbb{N} \wedge 1 \leq k \leq n) \to x \in A_k)$

És a dir:

$\neg \forall k((k \in \mathbb{N} \wedge 1 \leq k \leq n) \to x \in A_k)$

$\exists k \neg((k \in \mathbb{N} \wedge 1 \leq k \leq n) \to x \in A_k)$

$\exists k((k \in \mathbb{N} \wedge 1 \leq k \leq n) \wedge \neg x \in A_k)$

$\exists k(k \in \mathbb{N} \wedge 1 \leq k \leq n \wedge x \notin A_k)$

El conjunt dels índexs J pot no ser finit, ni tan sols format per naturals. Aleshores

$$\bigcap_{i \in J} A_i = \{x | \forall k(k \in J \to x \in A_k)\}$$

Exemples 8.42 Per exemple, per a intervals en $\mathbb{R}$:

Exemple 1. $\bigcap_{n \in \mathbb{N}} [0, n] = \{0\}$

Exemple 2. $\bigcap_{x \in \mathbb{R}^+} [0, x] = \{0\}$

Exemple 3. $\bigcap_{x\in\mathbb{R}^+}[-x,x]=\{0\}$

Exemple 4. $\bigcap_{x\in\mathbb{R}^+}(-x,x)=\emptyset$

Exemple 5. $\bigcap_{n\in\mathbb{N}}[-2^n,2^n]=[-1,1]$

Exemple 6. $\bigcap_{n\in\mathbb{N}}[-2^n,3^n]=[-1,1]$

Exemple 7. $\bigcap_{m\in\mathbb{Z}}[m,m+1]=\emptyset$. ■

8.7. Operacions conjuntistes: diferència de conjunts

Definició 8.9 (diferència de dos conjunts) *Siguin A i B dos conjunts. Es defineix la **diferència** $A-B$ de A i B, en l'ordre indicat, com el conjunt dels elements que pertanyen a A però no a B. És a dir:*

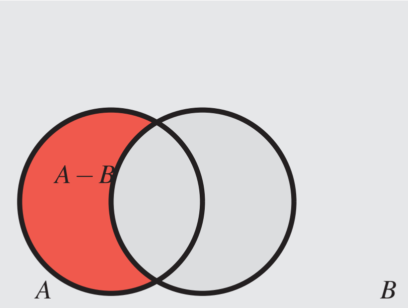
$A-B=\{x|\ x\in A \text{ i } x\notin B\}$, reexpressable com a qualsevol de les següents:

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

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

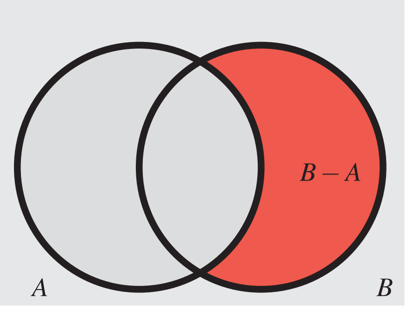
$A-B=\{x:\ x\in A\wedge x\notin B\}$

Notació alternativa: $A\backslash B$



Observem que es pot considerar la diferència de dos conjunts en l'altre ordre possible:

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



Cas particular: el complementari d'un conjunt relativament a un altre. Tot i que hi dediquem una secció específica més endavant, recordem aquí un cas particular de diferència de conjunts, el complementari; així, podrem utilitzar el concepte a partir d'aquí, encara que es tracti posteriorment amb més extensió.

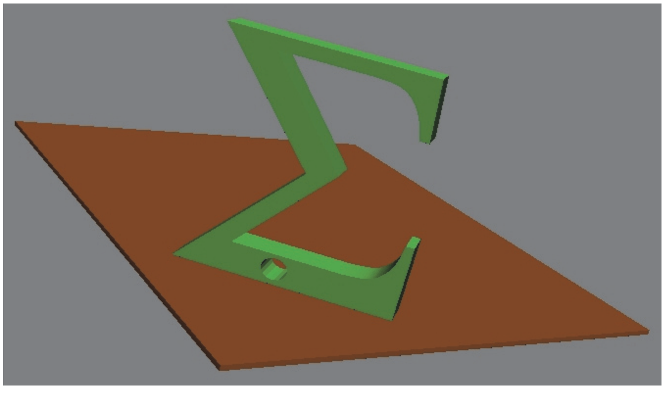
Si $A \subseteq \Omega$, es defineix el **complementari** o el **complement** de A respecte de Ω com la diferència de conjunts $\Omega - A$. Existeixen diverses notacions per al complementari: A^c o $\bar{A}$. Normalment utilitzam la primera, de manera que:

$A^c = \Omega - A.$

Així, $A^c = \Omega - A = \{x : x \in \Omega \wedge x \notin A\} = \{x : x \notin A\} = \{x | x \notin A\}.$

Vegem diversos exemples de diferència de conjunts.

Exemple 8.43



"sumatori perforat sobre rectangle"

Observi el lector que aquesta figura s'ha obtingut com a diferència de conjunts $A - B$, on A és el conjunt de punts del sumatori i B és el conjunt de punts d'un cilindre convenient que ocupa el lloc de la perforació.

Exemples 8.44

Exemple 1. $A = \{0,1,2,3\}$,

$B = \{2,3,4,a,b\}$.

$A - B = \{0,1\}$, $B - A = \{4,a,b\}$.

Exemple 2. $A = \{0,1,2,3\}$,

$B = \{2,3,4,a,\{0\},\emptyset\}$.

$A - B = \{0,1\}$,

$B - A = \{4,a,\{0\},\emptyset\}$.

Exemple 3. $\{1,2,3,4,5\} - \{2,3\} = \{1,4,5\}$,

$\{2,3\} - \{1,2,3,4,5\} = \emptyset$ (observeu que en els dos ordres no són iguals),

$\{2,3\} - \{1,2,4,5\} = \{3\}$.

Exemple 4. $[3,9] - [6,12] = \{x \in \mathbb{R} | 3 \leq x \leq 9\} - \{x \in \mathbb{R} | 6 \leq x \leq 12\}$

$= \{x \in \mathbb{R} | 3 \leq x < 6\} = [3,6)$.

Exemple 5. $[a,b] - (a,b) = \{a,b\}$ (intervals reals).

Exemple 6. $\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 1\} - \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 < 1\} =$

$= \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$.

Exemple 7. $A = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 4\}$,

$B = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 < 1\}$,

$A - B = \{(x,y) \in \mathbb{R}^2 | 1 \leq x^2 + y^2 \leq 4\}$ (corona circular).

Exemple 8. $A = \{1,2,3,4,5,7\}$, $B = \{3,5,6\}$, $C = \{3,4,7\}$,

$B - C = \{5,6\}$, $A - B = \{1,2,4,7\}$.

$A - (B - C) = \{1,2,3,4,5,7\} - \{5,6\} = \{1,2,3,4,7\}$.

$(A - B) - C = \{1,2,4,7\} - \{3,4,7\} = \{1,2\}$. ■

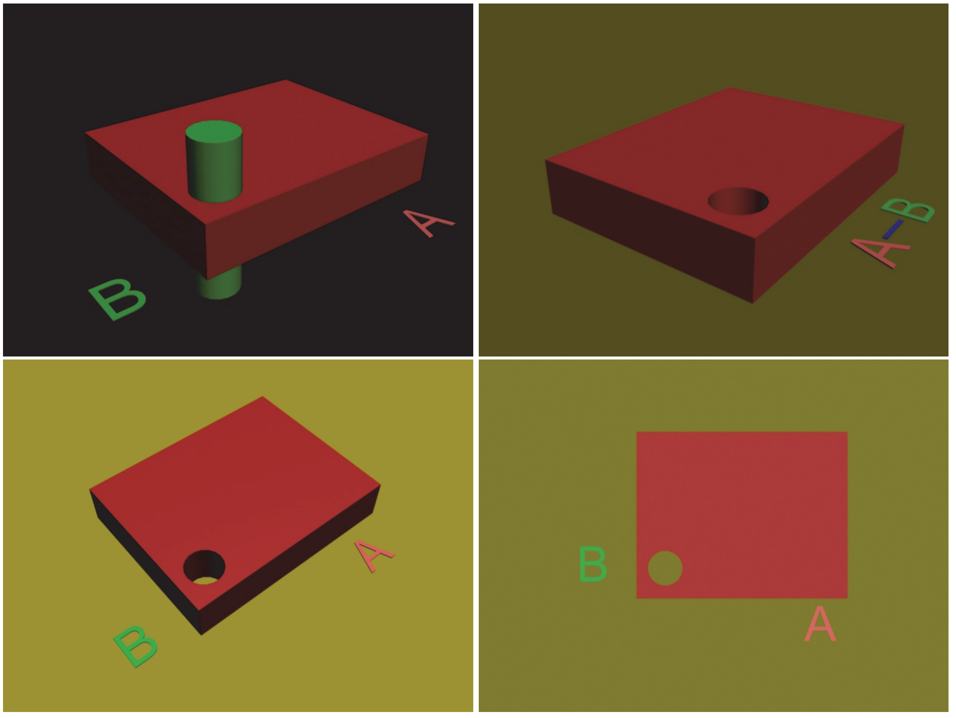
Exemple 8.45 El prisma es descriu com (sense detalls):

$$A = \{(x,y,z) \in \mathbb{R}^3 | x_0 \leq x \leq x_1, y_0 \leq y \leq y_1, z_0 \leq z \leq z_1\} =$$
$$= [x_0,x_1] \times [y_0,y_1] \times [z_0,z_1].$$

El cilindre (de radi R i d'eix paral·lel a l'eix de coordenades Oz):

$$B = \{(x,y,z) \in \mathbb{R}^3 | (x-\alpha)^2 + (y-\beta)^2 < R^2, h_1 \leq z \leq h_2\}.$$

$$A - B = \{(x,y,z) \in \mathbb{R}^3 | x_0 \leq x \leq x_1, y_0 \leq y \leq y_1, z_0 \leq z \leq z_1, x^2 + y^2 \geq R^2\}.$$



També, utilitzant el complementari (vegeu secció posterior):

$B^c = \{(x,y,z) \in \mathbb{R}^3 | x^2 + y^2 \geq R^2\}.$

$A - B = A \cap B^c = \{(x,y,z) \in \mathbb{R}^3 | x_0 \leq x \leq x_1, y_0 \leq y \leq y_1, z_0 \leq z \leq z_1, x^2 + y^2 \geq R^2\}.$ ■

Exemple 8.46 Considereu els conjunts següents:

$A = \{1,2,3,4,5,6,7,8\},$

$B = \{-1,2,5,7,9\},$

$C = \{2,a,b,5\},$

$D = \{7,9,c,d,e\},$

$E = \{9,d,e\}.$

Obteniu $[((A \cap B) - C) \cup D] - E$.

Fem-ne càlculs parcials:

$A \cap B = \{2,5,7\},$

$(A \cap B) - C = \{7\},$

$((A \cap B) - C) \cup D = \{7,9,c,d,e\},$

$[((A \cap B) - C) \cup D] - E = \{7,c,e\}.$ ■

Com expressar ser de la diferència de dos conjunts (en un dels ordres possibles:

$x \in A - B$ equival a $x \in A \wedge x \notin B$, per definició.

També $x \in A - B$, si, i només si,

$x \in A \wedge \neg x \in B$, si, i només si,

$\neg(x \in A \rightarrow x \in B)$.

Com expressar la negació de ser de la diferència (no ser de la diferència de dos conjunts, en un ordre dels dos ordres possibles):

$x \notin A - B$ equival a

$\neg x \in A - B$, que equival a

$\neg(x \in A \wedge x \notin B)$, que equival a

$\neg(x \in A \wedge \neg(x \in B))$, que equival, per De Morgan (lògica), a

$\neg(x \in A) \vee \neg\neg(x \in B)$, que equival (per doble negació) a

$\neg(x \in A) \vee (x \in B)$, és a dir,

$x \notin A \vee x \in B$ (reescriptura).

Per tant, amb

$x \notin A - B$ si, i només si, $x \notin A \vee x \in B$

expressem "no pertànyer a la diferència".

***Com obtenir** $A - B$?*

Els elements de $A - B$ només poden ser de A.

Sigui $x \in A$:

- si $x \in B$, aleshores $x \notin A - B$,
- si $x \notin B$, aleshores $x \in A - B$.

Exemple: $A = \{1,2,3\}$, $B = \{2,4\}$.

$1 \in A$, $1 \notin B$ implica $1 \in A - B$,

$2 \in A$, $2 \in B$ implica $2 \notin A - B$,

$3 \in A$, $3 \notin B$ implica $3 \in A - B$.

No hi ha més elements a A per considerar; per tant, $A - B = \{1,3\}$.

Propietats bàsiques de la diferència de conjunts

Teorema 8.4 *Siguin A,B,C conjunts. Aleshores:*

a) $A - B \subseteq A$

b) $A - \emptyset = A$

c) $\emptyset - A = \emptyset$

d) $A - A = \emptyset$

e) $(A - B) \cap (B - A) = \emptyset$

f) $(A - B) \cap B = \emptyset$

g) $A - B = A - (A \cap B)$

h) $A \subseteq B$ *si, i només si,* $A - B = \emptyset$

i) $C \subseteq A - B$ *si, i només si,* $C \subseteq A$ *i* $C \cap B = \emptyset$

Demostracions (exercicis de demostració i tècnica demostrativa)

$A - B \subseteq A$

$\forall x(x \in A - B \to x \in A)$, equivalent a

$\forall x((x \in A \wedge x \notin B) \to x \in A)$

Demostració

Mètode 1. És conseqüència directa de la definició de diferència de dos conjunts:

$x \in A - B \Rightarrow (x \in A \wedge x \notin B) \Rightarrow x \in A$

Tot i que és una obvietat intuïtiva, molt formalment seria conseqüència de

$(p \wedge q) \Rightarrow p$, ja que $(p \wedge q) \to p$ és sempre cert (tautologia).

Mètode 2. O bé, seguint la idea anterior, concretada, resulta un argument gairebé automatitzat (seqüència d'equivalències):

$(x \in A \wedge x \notin B) \to x \in A$

$\neg(x \in A \wedge x \notin B) \vee x \in A$

$\neg x \in A \vee \neg x \notin B \vee x \in A$

$\neg x \in A \vee x \in B \vee x \in A$

$(\neg x \in A \vee x \in A) \vee x \in B$

$\mathbb{T} \vee x \in B$

$\mathbb{T}$

Per tant, $(x \in A \wedge x \notin B) \to x \in A$ és cert per a tot x; resta la quantificació universal final: $\forall x((x \in A \wedge x \notin B) \to x \in A)$.

$A - \emptyset = A$

$\forall x(x \in A - \emptyset \leftrightarrow x \in A)$

Demostració

Mètode 1 (provant les dues inclusions). Vegem $A - \emptyset \subseteq A$.

Per la definició de diferència de conjunts, sempre és $A - B \subseteq A$, de manera que, en particular, és $A - \emptyset \subseteq A$, per a $B = \emptyset$.

Resta per a veure que $A \subseteq A - \emptyset$.

Si $x \in A$, aleshores $x \notin \emptyset$, per definició de conjunt buit. Per tant, $x \in A \wedge x \notin \emptyset$, és a dir, $x \in A - \emptyset$.

Mètode 2. Alternativament, considerem la seqüència d'*equivalències*:

$x \in A - \emptyset$

$x \in A \wedge x \notin \emptyset$

$x \in A \wedge \mathbb{T}$

$x \in A$

$\emptyset - A = \emptyset$

Demostració. Demostrem les dues inclusions: $\emptyset - A \subseteq \emptyset$ i $\emptyset \subseteq \emptyset - A$.

Sempre és $X - Y \subseteq X$ (primera propietat de la llista del teorema anterior, demostrada prèviament). Per tant, en particular, $\emptyset - A \subseteq \emptyset$. D'altra banda, el conjunt buit és subconjunt de qualsevol conjunt, de manera que, en particular, $\emptyset \subseteq \emptyset - A$. A partir de les *dues* inclusions, obtenim la igualtat dels conjunts.

$A - A = \emptyset$

Demostració. *Per reducció a l'absurd*:

Si $A - A$ fos no buit, existiria un element x tal que $x \in A - A$, és a dir, que $x \in A \wedge x \notin A$, que és fals sempre. Així s'arribaria a un absurd. Per tant, $A - A = \emptyset$.

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

Demostració. En efecte, no hi ha cap element que pugui satisfer

$x \in A \wedge x \notin B \wedge x \in B \wedge x \notin A.$

Es pot veure *per reducció a l'absurd*: suposem que $(A - B) \cap (B - A) \neq \emptyset$ i sigui $x \in A - B$ tal que, al mateix temps, $x \in B - A$. Tenim $x \in A - B \Rightarrow x \in A$. També $x \in B - A \Rightarrow x \notin A$. Per tant, $x \in A$ i $x \notin A$ per a un cert x. És una contradicció: per tant, $(A - B) \cap (B - A) = \emptyset$.

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

Demostració. *Per reducció a l'absurd*:

Si fos $(A - B) \cap B \neq \emptyset$, aleshores existiria x tal que $x \in (A - B) \cap B$. Ara bé,

$x \in (A - B) \cap B \Rightarrow (x \in A - B \wedge x \in B) \Rightarrow (x \in A \wedge x \notin B \wedge x \in B)$.

S'arriba a una contradicció: per a aquest element, $x \notin B \wedge x \in B$. Per tant, $(A - B) \cap B = \emptyset$.

$A - B = A - (A \cap B)$

Demostració

Mètode 1 (demostrem la doble inclusió).

Part 1. $(A - B \subseteq A - (A \cap B))$

$\forall x(x \in A - B \rightarrow x \in A - (A \cap B))$

Fixat x arbitrari, cal veure $x \in A - B \Rightarrow x \in A - (A \cap B)$, és a dir, si $x \in A - B$, vegem que $x \in A - (A \cap B)$

Hipòtesi: $x \in A - B$

Tesi: $x \in A - (A \cap B)$

Sigui $x \in A - B$. Aleshores és $x \in A$ i $x \notin B$. Ara bé, si $x \notin B$, aleshores $x \notin A \cap B$. Per tant, essent $x \in A$, finalment $x \in A - (A \cap B)$.

Part 2. $(A - (A \cap B) \subseteq A - B)$. Si $x \in A - (A \cap B)$, vegem que aleshores $x \in A - B$.

Sigui $x \in A - (A \cap B)$. Llavors $x \in A$ i $x \notin A \cap B$. Aquesta última fórmula equival a $x \notin A$ o $x \notin B$, però, com que $x \in A$, és necessàriament $x \notin B$. En resum, $x \in A$ i $x \notin B$, és a dir, $x \in A - B$.

Mètode 2 (equivalència de fórmules lògiques amb les quals expressem els conjunts).

$\forall x(x \in A - B \leftrightarrow x \in A - (A \cap B))$.

Concretant, escrivim una seqüència d'equivalències (per a x fix arbitrari):

$x \in A - (A \cap B)$

$x \in A \wedge x \notin (A \cap B)$ (per definició de la diferència)

$x \in A \wedge (x \notin A \vee x \notin B)$ (De Morgan, lògica)

$(x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B)$ (distributivitat de $\wedge$ respecte de $\vee$)

$\mathbb{F} \vee (x \in A \wedge x \notin B)$

$x \in A \wedge x \notin B$

$x \in A - B$.

Variant argumental. Un altre mètode consistiria a demostrar que són equivalents

$x \in A - B$ i $x \in A - (A \cap B)$, és a dir, que són equivalents

$x \in A \wedge x \notin B$ i

$x \in A \wedge x \notin A \cap B$, és a dir, $x \in A \wedge (x \notin A \vee \notin B)$. És un cas de l'equivalència $p \wedge \neg q$ i $p \wedge (\neg p \vee \neg q)$. Vegem que $p \wedge \neg q$ i $p \wedge (\neg p \vee \neg q)$ són equivalents (per taules de veritat o desenvolupant la segona: $p \wedge (\neg p \vee \neg q) \equiv (p \wedge \neg p) \vee (p \wedge \neg q) \equiv \mathbb{F} \vee (p \wedge \neg q) \equiv (p \wedge \neg q)$.

Observació: També es pot demostrar la igualtat dels conjunts per taules de pertinença (vegeu secció posterior).

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

És a dir, $A \subseteq B \Leftrightarrow A - B = \emptyset$.

Demostració (amb molt detall):

Vegem-ho formalitzadament (mètodes 1,2 següents):

Mètode 1. Encadenem equivalències:

$A - B = \emptyset$

$\Leftrightarrow \neg\exists x(x \in A - B)$ (és el $\emptyset$)

$\Leftrightarrow \neg\exists x(x \in A \wedge \neg x \in B)$ (definició de $A - B$)

$\Leftrightarrow \forall x \neg(x \in A \wedge \neg x \in B)$ (negació del quantificador existencial)

$\Leftrightarrow \forall x(\neg x \in A \vee \neg\neg x \in B)$ (De Morgan, lògica)

$\Leftrightarrow \forall x(\neg x \in A \vee x \in B)$ (doble negació)

$\Leftrightarrow \forall x(x \in A \rightarrow x \in B)$ (expressió $\rightarrow$ en termes de $\neg, \vee$)

$\Leftrightarrow A \subseteq B$.

Mètode 2. També podríem veure, equivalentment:

$A - B \neq \emptyset \Leftrightarrow A \not\subseteq B$,

ja que $F \Leftrightarrow G$ si, i només si, $\neg F \Leftrightarrow \neg G$,

Encadenem les *equivalències* següents:

$A - B \neq \emptyset$

$\exists x(x \in A - B)$

$\exists x(x \in A \wedge x \notin B)$ (definició de $A - B$)

$\exists x(x \in A \wedge \neg x \in B)$ (reescriptura)

$\exists x(\neg\neg x \in A \wedge \neg x \in B)$ (doble negació)

$\exists x \neg(\neg x \in A \vee x \in B)$ (De Morgan, lògica)

$\exists x \neg(x \in A \to x \in B)$ (expressió $\to$ en termes de $\neg, \vee$)

$\neg\forall x(x \in A \to x \in B)$ (negació del quantificador universal)

$\neg(A \subseteq B)$ (negació de la inclusió)

$A \not\subseteq B$.

Mètode 3. Hem de veure dues implicacions:

$A \subseteq B \Rightarrow A - B = \emptyset$ (subproblema 1)

$A - B = \emptyset \Rightarrow A \subseteq B$ (subproblema 2)

Es demostren separadament.

Subproblema 1 (dintre del mètode 3). $A \subseteq B \Rightarrow A - B = \emptyset$, és a dir,

$\forall x(x \in A \to x \in B) \to \neg\exists y(y \in A - B)$

Hipòtesi: $A \subseteq B$

Tesi: $A - B = \emptyset$

Ho demostrem pel *contrarecíproc*, és a dir, $A - B \neq \emptyset \Rightarrow A \not\subseteq B$.

Per ser $A - B$ no buit, existeix algun element $x \in A - B$. Per definició de diferència de conjunts, és $x \in A$ i $x \notin B$. Però això implica que A no és un subconjunt de B, és a dir, $A \not\subseteq B$.■

Nota: Es pot refer l'argumentació *per reducció a l'absurd*. Neguem la implicació $A - B \neq \emptyset \Rightarrow A \not\subseteq B$ i suposem, per tant, que $A - B \neq \emptyset$ i $A \subseteq B$ és cert. Existeix un element $x \in A - B$, és a dir, tal que $x \in A$ i $x \notin B$. Ara bé, si $A \subseteq B$, de $x \in A$ es deriva $x \in B$, contradicció, ja que resulta $x \in B \wedge x \notin B$. ■

Nota: També podem fer un exercici formal segons una altra presentació: cal veure que és cert:

$\forall x(x \in A \to x \in B) \to \neg\exists y(y \in A - B)$ (de fet, amb $\leftrightarrow$).

Escrivim fórmules equivalents, en seqüència, automatitzant l'argumentació:

$\forall x(x \in A \to x \in B) \to \forall y \neg(y \in A - B)$

$\forall x(x \in A \to x \in B) \to \forall y \neg(y \in A \wedge y \notin B)$

$\forall x(x \in A \to x \in B) \to \forall y(y \notin A \vee y \neg \notin B)$ (De Morgan, lògica)

$\forall x(x \in A \to x \in B) \to \forall y(y \notin A \vee y \in B)$

$\forall x(x \in A \to x \in B) \to \forall y(y \in A \to y \in B)$, que és cert, ja que no és més que $p \to p$. ■

Això acaba la demostració del subproblema 1 (dintre del mètode 3).

Subproblema 2 (dintre del mètode 3). $A - B = \emptyset \Rightarrow A \subseteq B$.

Sigui $x \in A$. Vegem que $x \in B$, aplicant $A - B = \emptyset$. Si fos $x \notin B$, seria $x \in A - B$, cosa impossible, ja que $A - B$ és buit. Per tant, $x \in B$.

Això acaba la demostració del subproblema 2 (dintre del mètode 3). Exercici: quina és l'estructura d'aquesta demostració? ■

Mètode 4

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \neg\exists y(y \in A - B)$.

Escrivim fórmules equivalents, en seqüència, automatitzant l'argumentació:

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \forall y \neg(y \in A - B)$

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \forall y \neg(y \in A \wedge y \notin B)$

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \forall y(y \notin A \vee y \neg \notin B)$ (De Morgan, lògica)

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \forall y(y \notin A \vee y \in B)$

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \forall y(y \in A \rightarrow y \in B)$, que és cert, ja que no és més que $p \leftrightarrow p$. ■

Mètode 5. Aquest mètode requereix el complementari (secció posterior). Suposem que el complementari és relativament a Ω ($A \subseteq \Omega$, $B \subseteq \Omega$).

Fem servir que $A \subseteq B \Leftrightarrow A = A \cap B$ (com hem vist anteriorment).

I hem de provar, doncs, equivalentment:

$A = A \cap B \Leftrightarrow A - B = \emptyset$.

Essent $A - B = A \cap B^c$, és equivalent demostrar, per transitivitat:

$A = A \cap B \Leftrightarrow A \cap B^c = \emptyset$

Hem de demostrar dues implicacions:

Part 1. $\Rightarrow$) ($A = A \cap B \Rightarrow A \cap B^c = \emptyset$)

Hipòtesi: $A = A \cap B$

Tesi: $A \cap B^c = \emptyset$

En efecte:

$A \cap B^c = (A \cap B) \cap B^c$, aplicant la hipòtesi,

$= A \cap (B \cap B^c)$, per associativitat de la intersecció,

$= A \cap \emptyset$, ja que $B \cap B^c = \emptyset$

$= \emptyset$

Part 2. $\Leftarrow$) (recíprocament, $A \cap B^c = \emptyset \Rightarrow A = A \cap B$)

Hipòtesi: $A \cap B^c = \emptyset$

Tesi: $A = A \cap B$

En efecte:

$A = A \cap \Omega = A \cap (B \cup B^c)$, ja que $\Omega = X \cup X^c$,

$= (A \cap B) \cup (A \cap B^c)$, per distributivitat de $\cap$ respecte de $\cup$,

$(A \cap B) \cup \emptyset$, aplicant la hipòtesi,

$= A \cap B$, ja que $X \cup \emptyset = X$.

$C \subseteq A - B$ si, i només si, $C \subseteq A$ i $C \cap B = \emptyset$

Observacions prèvies sobre la condició $C \cap B = \emptyset$

Observeu que demostrem $C \cap B = \emptyset$ si demostrem qualsevol de les dues implicacions següents, per a x arbitrari (són l'una contrarecíproca de l'altra):

$x \in C \Rightarrow x \notin B$

$x \in B \Rightarrow x \notin C$

En efecte, vegem que $\forall x(x \in C \Rightarrow x \notin B)$, cosa que implica $C \cap B = \emptyset$. Per reducció a l'absurd, suposem $C \cap B \neq \emptyset$. Suposant $x \in C \Rightarrow x \notin B$, si existeix $z \in C \cap B$ (és a dir, si $C \cap B$ és no buit), aleshores $z \in C$ i, per tant, $z \notin B$; però, per ser de la intersecció, també $z \in B$, la qual cosa és una contradicció. Per tant, $C \cap B = \emptyset$.

Recíprocament, vegem l'altra implicació: $C \cap B = \emptyset \Rightarrow \forall x(x \in C \rightarrow x \notin B)$.

Sigui $x \in C$, Aleshores $x \notin B$, ja que, si fos $x \in B$, seria $x \in C \cap B$ i, per tant, la contradicció $C \cap B \neq \emptyset$.

Reexpressem-ho d'altres formes: estem afirmant

$C \cap B = \emptyset \Leftrightarrow \forall x(x \in C \rightarrow x \notin B)$

$C \cap B \neq \emptyset \Leftrightarrow \neg\forall x(x \in C \rightarrow x \notin B)$, veracitat que demostrem a continuació:

$\neg\forall x(x \in C \rightarrow x \notin B)$

$\exists x \neg(x \in C \rightarrow x \notin B)$

$\exists x(x \in C \wedge \neg x \notin B)$

$\exists x(x \in C \wedge x \in B)$

$\exists x(x \in C \cap B)$

$C \cap B \neq \emptyset$,

d'on $C \cap B = \emptyset \Leftrightarrow \forall x(x \in C \rightarrow x \notin B)$.

Demostració de $C \subseteq A - B$ si, i només si, $C \subseteq A$ i $C \cap B = \emptyset$:

Hem de demostrar dues implicacions (dos subproblemes: part 1 i part 2):

Part 1 ($\Rightarrow$): Hem de veure $C \subseteq A - B \Rightarrow (C \subseteq A \wedge C \cap B = \emptyset)$

Hipòtesi [H]: ($C \subseteq A - B$). Formulada com un condicional, “si $x \in C$, aleshores $x \in A - B$”.

Tesi: $T_1 \wedge T_2$, on

- [T1] si $x \in C$, aleshores $x \in A$,
- [T2] si $x \in C$, aleshores $x \notin B$ (observacions prèvies sobre la condició $C \cap B = \emptyset$).

Són dues les implicacions que es volen demostrar: $H \Rightarrow T1$ i $H \Rightarrow T2$.

O bé:

Si $x \in C$, aleshores $x \in A \wedge x \notin B$.

Són dues: $H \Rightarrow T1$ i $H \Rightarrow T2$.

Però això últim és justament el que ens diu la hipòtesi, d’acord amb la definició de diferència de conjunts $A - B$. ■

Part 2 ($\Leftarrow$): Hem de veure el recíproc, és a dir: $(C \subseteq A \wedge C \cap B = \emptyset) \Rightarrow C \subseteq A - B$.

Hipòtesi [H]: $C \subseteq A \wedge C \cap B = \emptyset$ (és $H1 \wedge H2$) amb

H1: $C \subseteq A$ ($\forall x(x \in C \rightarrow x \in A), x \in C \Rightarrow x \in A$),

H2: $C \cap B = \emptyset$ ($\forall x(x \in C \rightarrow x \notin B), x \in C \Rightarrow x \notin B$).

Tesi [T]: $C \subseteq A - B$ ($\forall x(x \in C \rightarrow x \in A - B)$)

Estructura de l’enunciat: ($H1 \wedge H2 \Rightarrow T$)

Mètode 1 (argumentant sobre elements). Hem de veure $x \in C \Rightarrow x \in A - B$ fent servir $H1$ i $H2$:

$$\left.\begin{array}{l} x \in C \overset{H1}{\Rightarrow} x \in A \\ x \in C \overset{H2}{\Rightarrow} x \notin B \end{array}\right\} \Rightarrow x \in A - B$$

Mètode 2 (sense argumentar sobre elements, utilitzant el complementari i la distributivitat de la intersecció respecte de la unió):

Veure $C \subseteq A - B$ és equivalent a veure $C = C \cap (A - B)$. La hipòtesi $C \subseteq A$ s’expressa equivalentment com $C = C \cap A$.

Vegem, doncs:

$C \cap (A - B) = C \cap (A \cap B^c) = (C \cap A) \cap B^c \stackrel{H1}{=} C \cap B^c = C - B \stackrel{H2}{=} C.$

Observació: Es pot veure que $H2 \Rightarrow C \cap B^c = C$ (aplicant distributivitat de la intersecció respecte de la unió, vegeu la secció posterior). En efecte, $C = C \cap \Omega = C \cap (B \cup B^c) = (C \cap B) \cup (C \cap B^c) \stackrel{H2}{=} \emptyset \cup (C \cap B^c) = C \cap B^c$.

Exercici: resoleu la part 1 com la part 2, amb operacions conjuntistes, és a dir, a "alt nivell", sense fer consideracions ni argumentacions sobre elements.

8.8. Relació entre operacions bàsiques conjuntistes

Propietats de distributivitat

Propietat distributiva de la intersecció respecte de la unió (dita també: distributivitat de la intersecció respecte de la unió)

Teorema 8.5 *Si A, B i C són conjunts, aleshores:*

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

Demostració. Fem servir la propietat distributiva de $\wedge$ respecte de $\vee$.

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

$= \{x | x \in A \wedge x \in (B \cup C)\}$ (per definició d'intersecció)

$= \{x | x \in A \wedge (x \in B \vee x \in C)\}$ (per definició d'unió)

$= \{x | (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\}$ (distributivitat de $\wedge$ respecte de $\vee$)

$= \{x | (x \in A \cap B) \vee (x \in A \cap C)\}$ (per definició d'intersecció)

$= (A \cap B) \cup (A \cap C)$ (per definició d'unió)

Exercici: Escriviu la demostració anterior seguint el model de la propietat següent.

Propietat distributiva de la unió respecte de la intersecció (dita també: distributivitat de la unió respecte de la intersecció)

Teorema 8.6 *Si A, B i C són conjunts, aleshores:*

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

Demostració. Fem servir la propietat distributiva de $\vee$ respecte de $\wedge$.

Presentem una demostració diferent de l'anterior de distributivitat. Cal veure que:

$\forall x (x \in A \cup (B \cap C) \leftrightarrow x \in (A \cup B) \cap (A \cup C))$ és cert.

Sigui doncs x arbitrari però fix. Per a aquest x, cal veure que

$x \in A \cup (B \cap C) \leftrightarrow x \in (A \cup B) \cap (A \cup C)$ és cert, és a dir, que

$x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$

En efecte:

$x \in A \cup (B \cap C) \Leftrightarrow$
$\Leftrightarrow x \in A \vee x \in (B \cap C)$ (per definició d'unió)
$\Leftrightarrow x \in A \vee (x \in B \wedge x \in C)$ (per definició d'intersecció)
$\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ (per distributivitat de $\vee$ respecte de $\wedge$)
$\Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C)$ (per definició d'unió)
$\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$ (per definició d'intersecció)

Observació: Aquest és un cas en el qual s'han pogut encadenar una sèrie d'equivalènci-es:

$\mathscr{A} \Leftrightarrow C_1 \Leftrightarrow C_2 \Leftrightarrow \cdots \Leftrightarrow C_n \Leftrightarrow \mathscr{B}$,

encadenament que ens porta a $\mathscr{A} \Leftrightarrow \mathscr{B}$.

Vegem-ne altres propietats a través dels exercicis.

PROBLEMA 8.8

Siguin A, B conjunts. Proveu que $A \cap (A \cup B) = A$.

Solució. Vegem que $A \cap (A \cup B) = A$

Mètode 1. Tenim la propietat general:

$C \subseteq D$ si, i només si, $C = C \cap D$.

S'aplica a $C = A$, $D = A \cup B$ i s'obté $A = A \cap (A \cup B)$, atès que $A \subseteq A \cup B$.

Mètode 2. Una altra possibilitat:

$A \cap (A \cup B) \subseteq A$ [denotem-la com a propietat 1], per $A \cap W \subseteq A$, per a tot W.

Ara, de $A \subseteq (A \cup B)$ (sempre cert), resulta

$A = A \cap A \subseteq A \cap (A \cup B)$ [propietat 2],

ja que

$C \subseteq D \Rightarrow T \cap C \subseteq T \cap D$, per a tot T.

Per les propietats [1] i [2], resulta $A = A \cap A \subseteq A \cap (A \cup B) \subseteq A$, d'on la igualtat

$A \cap (A \cup B) = A$.

També es pot aplicar que $A \cap C \subseteq A$, per a qualsevol C; amb $C = A \cap B$, resulta que $A \cap (A \cup B) \subseteq A$.

Mètode 3. Per fórmules lògiques equivalents. Descrivim amb una fórmula lògica el conjunt $A \cap (A \cup B)$.

$x \in A \cap (A \cup B)$

$x \in A \wedge x \in (A \cup B)$

$x \in A \wedge (x \in A \vee x \in B)$

Aquesta última fórmula equival a $x \in A$, com a conseqüència de l'equivalència lògica (proposicions): $p \wedge (p \vee q) \equiv p$, que es pot comprovar per taules de veritat i substitució posterior.

Així, $\forall x (x \in A \cap (A \cup B) \leftrightarrow x \in A)$, i resulta demostrada la igualtat dels conjunts.

PROBLEMA 8.9

Siguin A, B conjunts. Proveu que $A \cup (A \cap B) = A$.

Solució. Vegem que $A \cup (A \cap B) = A$

Mètode 1. Utilitzem la propietat general $C \subseteq D \Rightarrow D = C \cup D$, que apliquem amb $C = A \cap B$, $D = A$ i resulta:

$A \cap B \subseteq A \Rightarrow A = (A \cap B) \cup A$.

Mètode 2

$A \subseteq A \cup (A \cap B)$ [1] (sempre, ja que $A \subseteq A \cup X$)

$A \cap B \subseteq A$ [2] (sempre)

Apliquem [2] per a obtenir $A \cup (A \cap B) \subseteq A \cup A = A$ [3]

Per [1] i [3], $A \subseteq A \cup (A \cap B) \subseteq = A$, d'on $A \cup (A \cap B) = A$.

Mètode 3 (per fórmules lògiques equivalents)

$x \in A \cup (A \cap B)$

$x \in A \vee x \in (A \cap B)$

$x \in A \vee (x \in A \wedge x \in B)$

Aquesta última fórmula equival a $x \in A$ perquè $p \vee (p \wedge q) \equiv p$ (pot veure's per taules de veritat del llenguatge de proposicions).

Això demostra la igualtat dels dos conjunts.

Se'n poden formular diverses variants:

Variant argumental 1 (seqüència d'equivalències):

$x \in A \cup (A \cap B)$

$x \in A \vee x \in (A \cap B)$

$x \in A \vee (x \in A \wedge x \in B)$

$(x \in A \vee x \in A) \wedge (x \in A \vee x \in B)$ (per distributivitat de $\vee$ respecte de $\wedge$)

$x \in A \wedge (x \in A \vee x \in B)$

$x \in A \wedge x \in (A \cup B)$

$x \in A \cap (A \cup B)$

$x \in A$ (per l'exercici anterior: $A \cap (A \cup B) = A$).

Variant argumental 2 (seqüència d'equivalències):

$x \in A \cup (A \cap B)$

$x \in A \vee x \in (A \cap B)$

$x \in A \vee (x \in A \wedge x \in B)$

$(x \in A \vee x \in A) \wedge (x \in A \vee x \in B)$ (per distributivitat de $\vee$ respecte de $\wedge$)

$x \in A \wedge (x \in A \vee x \in B)$

Per l'equivalència $p \wedge (p \vee q) \equiv p$, l'última fórmula és equivalent a:

$x \in A$

Mètode 4. S'aplica el resultat del problema anterior ($A \cap (A \cup B) = A$).

De fet, es demostra la igualtat $A \cup (A \cap B) = A \cap (A \cup B)$.

$x \in A \cup (A \cap B)$

$x \in A \vee (x \in A \wedge x \in B)$

Aplicant la propietat distributiva de $\vee$ respecte de $\wedge$:

$(x \in A \vee x \in A) \wedge (x \in A \vee x \in B)$

$x \in A \wedge (x \in A \vee x \in B)$

$x \in A \wedge x \in A \cup B$

$x \in A \cap (A \cup B)$

Mètode 5 (doble inclusió "per elements")

Inclusió: $A \subseteq A \cup (A \cap B)$

Vegem que, per a un x arbitrari, $x \in A \Rightarrow x \in A \cup (A \cap B)$.

$x \in A \Rightarrow x \in A \cup Y$, per a tot conjunt Y; en particular, per a $Y = A \cap B$, resulta: $x \in A \cup (A \cap B)$.

Inclusió: $A \cup (A \cap B) \subseteq A$

Vegem que, per a un x arbitrari, $x \in A \cup (A \cap B) \Rightarrow x \in A$.

$$x \in A \cup (A \cap B) \Rightarrow \left\{ \begin{array}{l} x \in A \\ \text{o} \\ x \in A \cap B \subseteq A \Rightarrow x \in A \end{array} \right\} \Rightarrow x \in A$$

PROBLEMA 8.10

Siguin A, B conjunts. Proveu que $A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$.

Solució. Vegem que $A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$

Mètode 1. Demostrem $\forall x (x \in A \cup B \leftrightarrow x \in (A - B) \cup (A \cap B) \cup (B - A))$.

És a dir, per a un x qualsevol però fix, provem:

$x \in A \cup B \Leftrightarrow x \in (A - B) \cup (A \cap B) \cup (B - A)$

Idea: Intentarem mantenir una cadena d'equivalències, de la qual podrem concloure l'afirmació anterior.

Idea per a la demostració: Sembla que hauríem de començar per

$x \in (A - B) \cup (A \cap B) \cup (B - A)$, que ens donarà més possibilitats de manipulació (més que si comencéssim per $x \in A \cup B$).

$x \in (A - B) \cup (A \cap B) \cup (B - A)$, que equival a [per definició d'unió]

$x \in (A - B) \vee x \in (A \cap B) \vee x \in (B - A)$, que equival a [per definició de diferència i intersecció]

$(x \in A \wedge x \notin B) \vee (x \in A \wedge x \in B) \vee (x \in B \wedge x \notin A)$, que equival a [per distributivitat de $\wedge$ respecte de $\vee$]

$(x \in A \wedge (x \notin B \vee x \in B)) \vee (x \in B \wedge x \notin A)$, que equival a [per tautologia]

$(x \in A \wedge \mathbb{T}) \vee (x \in B \wedge x \notin A)$, que equival a [per equivalència lògica]

$(x \in A) \vee (x \in B \wedge x \notin A)$, que equival a [per distributivitat de $\vee$ respecte de $\wedge$]

$(x \in A \vee x \in B) \wedge (x \in A \vee x \notin A)$, que equival a [per tautologia]

$(x \in A \vee x \in B) \wedge \mathbb{T}$, que equival a [per equivalència lògica]

$x \in A \vee x \in B$, que equival a [per definició d'unió]

$x \in A \cup B$.

S'ha utilitzat: $\neg p \vee p \equiv \mathbb{T}$ (vegeu el capítol de llenguatge de proposicions), amb substitució posterior.

Mètode 2. Efectuant operacions conjuntistes (manipulació conjuntista).

Utilitzem el complementari (vegeu secció posterior). Considerem els complementaris A^c, B^c, C^c respecte de Ω, conjunt que conté A, B i C com a subconjunts.

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

$= (A \cap B^c) \cup (A \cap B) \cup (B \cap A^c)$ (per $C - D = C \cap D^c$)

$= ((A \cap B^c) \cup (A \cap B)) \cup (B \cap A^c)$ (per associativitat de la unió)

$= ((A \cap (B^c \cup B)) \cup (B \cap A^c)$ (per distributivitat de $\cap$ respecte de $\cup$)

$= (A \cap \Omega) \cup (B \cap A^c)$ (per $C \cup C^c = \Omega$)

$= A \cup (B \cap A^c)$ (per $C \cap \Omega = C$)

$= (A \cup B) \cap (A \cup A^c)$ (per distributivitat de $\cup$ respecte de la $\cap$)

$= (A \cup B) \cap \Omega$ (per $C \cup C^c = \Omega$)

$= (A \cup B)$ (per $C \cap \Omega = C$).

Variant argumental 1 (mètode 2b). Associar a la línia 3 segons

$= (A \cap B^c) \cup ((A \cap B) \cup (B \cap A^c))$ (exercici per al lector).

Variant argumental 2 (mètode 2c) (basat en una manipulació conjuntista, associant d'una altra manera en el desenvolupament del mètode 2) ($U = \Omega$ denota el conjunt universal que conté A i B; $\bar{X} = X^c$ denota el complementari $U - X$)

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

$= (A \cap B) \cup (A \cap B^c) \cup (B \cap A^c)$ (expressió en termes de complementari)

$= (A \cap B) \cup [(A \cap B^c) \cup (B \cap A^c)]$ (per associativitat de $\cup$)

$= (A \cap B) \cup [((A \cap B^c) \cup B) \cap ((A \cap B^c) \cup A^c)]$ (per distributivitat de $\cup$ respecte de $\cap$)

$= (A \cap B) \cup [((A \cup B) \cap (B^c \cup B)) \cap ((A \cup A^c) \cap (B^c \cup A^c))]$ (per distributivitat de $\cup$ respecte de $\cap$)

$= (A \cap B) \cup [((A \cup B) \cap U) \cap (U \cap (B^c \cup A^c))]$ (per $X \cup X^c = U$)

$= (A \cap B) \cup [(A \cup B) \cap (B^c \cup A^c)]$ (per $X \cap U = X$)

$= (A \cap B) \cup [(A \cup B) \cap (B \cap A)^c\ ]$ (per De Morgan)

$= [(A \cap B) \cup (A \cup B)] \cap [(A \cap B) \cup (B \cap A)^c]$ (per distributivitat de $\cup$ respecte de $\cap$)

$= (A \cup B) \cap [(A \cap B) \cup (A \cap B)^c]$ (ja que $A \cap B \subseteq A \cup B$)

$= (A \cup B) \cap U$ (per $X \cup X^c = U$)

$= A \cup B$ (per $X \cap U = X$).

Mètode 3 (essencialment, és una altra presentació del mètode 1). Sigui Ω un conjunt universal, un conjunt del qual A i B són subconjunts.

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

$= \{x | x \in A - B \vee x \in A \cap B \vee x \in B - A\}$

$= \{x | (x \in A \wedge x \notin B) \vee (x \in A \wedge x \in B) \vee (x \in B \wedge x \notin A)\}$ (per definició de $\cap$ i de $-$)

$= \{x | [x \in A \wedge (x \notin B \vee x \in B)] \vee (x \in B \wedge x \notin A)\}$ (distributivitat de $\wedge$ respecte de $\vee$)

$= \{x | [x \in A \wedge x \in \Omega] \vee (x \in B \wedge x \notin A)\}$

$= \{x | [x \in (A \cap \Omega)] \vee (x \in B \wedge x \notin A)\}$ (per definició de $\cap$)

$= \{x | x \in A \vee (x \in B \wedge x \notin A)\}$ (per $A \cap \Omega = A$)

$= \{x | (x \in A \vee x \in B) \wedge (x \in A \vee x \notin A)\}$ (per distributivitat de $\vee$ respecte de $\wedge$)

$= \{x | x \in (A \cup B) \wedge x \in \Omega\}$ (per definició de $\cup$ i per $A \cup A^c = \Omega$)

$= \{x | x \in (A \cup B) \cap \Omega\}$

$= (A \cup B) \cap \Omega = A \cup B$ (per $X \cap \Omega = X$).

Mètode 4. Vegem les dues inclusions separadament (subproblemes 1 i 2).

Subproblema 1:

$(A - B) \cup (A \cap B) \cup (B - A) \subseteq A \cup B$, és a dir,

$x \in (A - B) \cup (A \cap B) \cup (B - A) \Rightarrow x \in A \cup B$ per a tot x, és a dir,

$\forall x (x \in (A - B) \cup (A \cap B) \cup (B - A) \rightarrow x \in A \cup B)$

Subproblema 2:

$A \cup B \subseteq (A - B) \cup (A \cap B) \cup (B - A)$, és a dir,

$x \in A \cup B \Rightarrow x \in (A - B) \cup (A \cap B) \cup (B - A)$, per a x arbitrari, és a dir,

$\forall x (x \in A \cup B \rightarrow x \in (A - B) \cup (A \cap B) \cup (B - A))$

Resolem aquests problemes separadament. Hi ha diverses variants de resolució.

Subproblema 1: $(A - B) \cup (A \cap B) \cup (B - A) \subseteq A \cup B$.

Variant argumental 1. Tenim que els conjunts $A - B$, $A \cap B$ i $B - A$ són subconjunts d'un mateix conjunt, de $A \cup B$, ja que

$A - B \subseteq A \subseteq A \cup B$

$A \cap B \subseteq A \cup B$ (o bé per $A \cap B \subseteq A \subseteq A \cup B$, o bé per $A \cap B \subseteq B \subseteq A \cup B$)

$B - A \subseteq B \subseteq A \cup B$

Per tant, la reunió dels tres conjunts anteriors és un subconjunt de $A \cup B$. Això és degut al fet que

$(A_1 \subseteq C \wedge A_2 \subseteq C) \Rightarrow (A_1 \cup A_2) \subseteq C$

$(A_1 \subseteq C \wedge A_2 \subseteq C \wedge A_3 \subseteq C) \Rightarrow (A_1 \cup A_2 \cup A_3) \subseteq C$ $(A_1 \subseteq C_1 \wedge A_2 \subseteq C_2 \wedge A_3 \subseteq C_3) \Rightarrow (A_1 \cup A_2 \cup A_3) \subseteq (C_1 \cup C_2 \cup C_3)$

Per tant:

$$\left.\begin{array}{l} A - B \subseteq A \subseteq A \cup B \\ A \cap B \subseteq A \cup B \\ B - A \subseteq B \subseteq A \cup B \end{array}\right\} \Rightarrow (A - B) \cup (A \cap B) \cup (B - A) \subseteq A \cup B$$

Variant argumental 2 (directament). Podem procedir per disjunció de casos (no mútuament excloents) si $x \in (A \cap B) \cup (A - B) \cup (B - A)$. Aleshores és $x \in A \cap B$ o $x \in A - B$ o $x \in B - A$.

Cas 1. Si $x \in A \cap B$, és $x \in A \cup B$, ja que $A \cap B \subseteq A \cup B$.

Cas 2. Si $x \in A - B$, és $x \in A$ i, per tant, $x \in A \cup B$.

Cas 3. Si $x \in B - A$, és $x \in B$ i, per tant, $x \in A \cup B$.

Variant argumental 3 (pel *contrarecíproc*). Recordeu que el contrarecíproc o proposició contrarecíproca de

$p \to q$ és $\neg q \to \neg p$.

En aquest cas, el contrarecíproc és, doncs:

$x \notin A \cup B \Rightarrow x \notin (A \cap B) \cup (A - B) \cup (B - A)$.

És: $x \notin A \cup B \Rightarrow x \notin A$ i $x \notin B$

Per tant:

$x \notin A \cap B$ (ja que $A \cap B \subseteq A \cup B$)
i

$x \notin A \Rightarrow x \notin A - B$ (ja que $A - B \subseteq A$; d'on $x \notin A \Rightarrow x \notin A - B$) i

$x \notin B \Rightarrow x \notin B - A$ (ja que $B - A \subseteq B$; d'on $x \notin B \Rightarrow x \notin B - A$)

Per tant, $x \notin A \cap B$, $x \notin A - B$, $x \notin B - A$, és a dir, $x \notin A \cap B \wedge x \notin A - B \wedge x \notin B - A$, d'on, per De Morgan, $x \notin (A \cap B) \cup (A - B) \cup (B - A)$.

Per tant, finalment:

$x \notin (A \cap B) \cup (A - B) \cup (B - A)$.

Observació: Es pot arribar a la conclusió anterior detallant més l'argumentació:

$x \notin A - B \wedge x \notin A \cap B \wedge x \notin B - A$

$\neg x \in A - B \wedge \neg x \in A \cap B \wedge \neg x \in B - A$

$\neg(x \in A - B \vee x \in A \cap B \vee x \in B - A)$ (De Morgan)

$\neg(x \in (A - B) \cup (A \cap B) \cup (B - A))$

$x \notin (A - B) \cup (A \cap B) \cup (B - A)$.

Subproblema 2: $A \cup B \subseteq (A - B) \cup (A \cap B) \cup (B - A)$

Cal veure que $\forall x(x \in A \cup B \to x \in (A - B) \cup (A \cap B) \cup (B - A))$ és cert.

Vegem que

$x \in A \cup B \Rightarrow x \in (A - B) \cup (A \cap B) \cup (B - A)$.

Equivalentment:

$x \in A \cup B \Rightarrow (x \in (A - B) \vee x \in (A \cap B) \vee x \in (B - A))$

Observeu l'estructura de l'afirmació anterior:

$p \to (r \vee s \vee t)$, amb $p = x \in A \cup B$, $r = x \in A - B$, $s = x \in A \cap B$, $t = x \in B - A$

Es pot demostrar "directament" o bé demostrant qualsevol de les afirmacions següents, equivalents a l'anterior, demostrable per taules de veritat o utilitzant equivalències lògiques:

$(p \wedge \neg r \wedge \neg t) \to s$ (variant 1)

$(p \wedge \neg r \wedge \neg s) \to t$ (variant 2)

$(p \wedge \neg s \wedge \neg t) \to r$ (variant 3)

$(p \wedge \neg r) \to (s \vee t)$ (variant 4)

$(p \wedge \neg s) \to (r \vee t)$ (variant 5)

$(p \wedge \neg t) \to (r \vee s)$ (variant 6)

Mètode 1 (subproblema 2, segons la variant 1 de la llista anterior). Demostració seguint l'esquema $(p \wedge \neg r \wedge \neg t) \to s$ (variant 1):

Suposem, doncs, escollint $p = x \in A \cup B$, $r = x \in A - B$, $s = x \in A \cap B$, $t = x \in B - A$, que $p \wedge \neg r \wedge \neg t$ és cert (és la hipòtesi):

Hipòtesi:

$x \in A \cup B$, és a dir, $x \in A \vee x \in B$ cert [resultat "a"]

$x \notin A - B$, és a dir $x \notin A \vee x \in B$ cert [resultat "b"]

$x \notin B - A$, és a dir $x \notin B \vee x \in A$ cert [resultat "c"]

Tesi:

Hem de veure $x \in A \cap B$, és a dir, $x \in A$ i $x \in B$ ($x \in A \wedge x \in B$).

Vegem separadament $x \in A$ (subproblema 2a) i $x \in B$ (subproblema 2b).

- Subproblema 2a: Vegem $x \in A$. Si fos $x \notin A$, aleshores, per [a], ha de ser $x \in B$. En conseqüència, per [c], ha de ser $x \in A$, la qual cosa és una contradicció. Per tant, $x \in A$. La demostració anterior és *per reducció a l'absurd*.
- Subproblema 2b: Vegem $x \in B$. Si fos $x \notin B$, aleshores per [a], ha de ser $x \in A$. En conseqüència, per [b] ha de ser $x \in B$, contradicció. Per tant, $x \in B$. La demostració anterior és *per reducció a l'absurd*.

Atenció: Resta com a exercici demostrar el resultat segons les variants 2, 3, 4, 5, 6 anteriors.

Mètode 2 (subproblema 2) ("directament": $x \in A \cup B \Rightarrow x \in (A \cap B) \cup (A - B) \cup (B - A)$, per a tot x).

Sigui $x \in A \cup B$. Aleshores $x \in A$ o $x \in B$ (o pertany a ambdós).

Cas 1. Suposem $x \in A$.

- Cas 1.1. Si $x \in B$, aleshores $x \in A \cap B$, i ja pertany a

  $(A \cap B) \cup (A - B) \cup (B - A)$.
- Cas 1.2. Si $x \notin B$, aleshores $x \in A - B$, i ja és de la unió anterior.

Cas 2. Suposem $x \in B$.

- Cas 2.1. Si $x \in A$, aleshores $x \in A \cap B$,i ja aleshores

  $x \in (A \cap B) \cup (A - B) \cup (B - A)$.
- Cas 2.2. Si $x \notin A$, aleshores és $x \in B - A$, i ja és de la reunió. ■

Exposició alternativa: $x \in A \cup B \Rightarrow x \in A \vee x \in B$. Aleshores tenim:

Cas 1. $x \in A$ i $x \notin B$. Aleshores $x \in A - B$

o

Cas 2. $x \in A$ i $x \in B$. Aleshores $x \in A \cap B$

o

Cas 3. $x \notin A$ i $x \in B$. Aleshores $x \in B - A$

d'on:

$x \in A \cup B \Rightarrow (x \in A \vee x \in B)$

$\Rightarrow ((x \in A \wedge x \notin B) \vee (x \in A \wedge x \in B) \vee (x \notin A \wedge x \in B))$

$\Rightarrow (x \in A - B \vee x \in A \cap B \vee x \in B - A)$

$\Rightarrow x \in (A - B) \cup (A \cap B) \cup (B - A)$.

Mètode 3 (subproblema 2). Variant argumental (contrarecíproc). El lector pot intentar demostrar el contrarecíproc. Recordeu que el contrarecíproc o proposició contrarecíproca de $(p \to q)$ és $(\neg q \to \neg p)$.

Cal provar $\forall x(x \in A \cup B \to x \in (A - B) \cup (A \cap B) \cup (B - A))$, que equival a

$\forall x(x \notin (A - B) \cup (A \cap B) \cup (B - A) \to x \notin A \cup B)$.

S'hauria de provar per a cada x: $x \notin (A - B) \cup (A \cap B) \cup (B - A) \to x \notin A \cup B$.

Resumint, seria:

$\forall x(x \notin (A \cap B) \cup (A - B) \cup (B - A) \to x \notin A \cup B)$. I per a cada x s'hauria de provar:

$(x \notin (A \cap B) \cup (A - B) \cup (B - A)) \to x \notin A \cup B$.

Suposem, doncs:

$x \notin (A \cap B) \wedge x \notin (A - B) \wedge x \notin (B - A)$, és a dir,

$x \notin (A \cap B)$ (és $x \notin (A \cap B \overset{(1)}{\Leftrightarrow} (x \notin A \vee x \notin B)$)

i

$x \notin (A - B)$ (és $x \notin (A - B) \overset{(2)}{\Leftrightarrow} (x \notin A \vee x \in B)$)

i

$x \notin (B - A)$ (és $x \notin (B - A) \overset{(3)}{\Leftrightarrow} (x \notin B \vee x \in A)$)

Considerem (1):

- Si $x \notin A$, aleshores, per (3), és $x \notin B$.

  Així, $x \notin A \Rightarrow (x \notin A \wedge x \notin B) \Rightarrow x \notin A \cup B$, que és el que cal veure.

- Si $x \notin B$, aleshores, per (2), és $x \notin A$.

  Així, $x \notin B \Rightarrow (x \notin B \wedge x \notin A) \Rightarrow x \notin A \cup B$, que és el que cal veure.

Per tant, $x \notin A \cup B$, a partir de la hipòtesi.

Mètode 4 (subproblema 2). Per reducció a l'absurd. Negant la implicació:

$x \in A \cup B \Rightarrow x \in (A \cap B) \cup (A - B) \cup (B - A)$ (per a tot x)

afirmem que existeix un x tal que:

$x \in A \cup B \wedge x \notin A \cap B \wedge x \notin A - B \wedge x \notin B - A$.

Millor encara, s'ha de provar:

$\forall x (x \in A \cup B \rightarrow x \in (A \cap B) \cup (A - B) \cup (B - A))$.

Negació (en aplicació del mètode de reducció a l'absurd):

$\neg \forall x (x \in A \cup B \rightarrow x \in (A \cap B) \cup (A - B) \cup (B - A))$

$\exists x \neg (x \in A \cup B \rightarrow x \in (A \cap B) \cup (A - B) \cup (B - A))$

$\exists x (x \in A \cup B \wedge \neg (x \in (A \cap B) \vee (x \in A - B) \vee x \in (B - A)))$

$\exists x (x \in A \cup B \wedge \neg x \in (A \cap B) \wedge \neg (x \in A - B) \wedge \neg x \in (B - A))$

$\exists x (x \in A \cup B \wedge x \notin (A \cap B) \wedge (x \notin A - B) \wedge x \notin (B - A))$

Vegem que s'arriba a una contradicció.

Suposem $x \in A \cup B$. És $x \in A$ o $x \in B$.

– Suposem $x \in A$. Essent $x \notin A \cap B$, és $x \notin B$. Per tant, $x \in A - B$, contradicció amb $x \notin A - B$.

– Suposem $x \in B$. Essent $x \notin A \cap B$, és $x \notin A$. Per tant, $x \in B - A$, contradicció amb $x \notin B - A$.

S'arriba a una contradicció en tots els casos possibles. Per tant, $\forall x (x \in A \cup B \rightarrow x \in (A \cap B) \cup (A - B) \cup (B - A))$ és cert.

8.9. Operacions conjuntistes: complementari d'un conjunt respecte d'un altre

Definicions

Complementari respecte d'un conjunt. Conjunt universal

El concepte de complementació d'un conjunt donat A és relatiu a un altre que el conté, que denotem per Ω (per exemple) i que és conegut com a conjunt "universal", "univers del discurs"o "conjunt de referència", respecte del qual es considera la complementació. Així, parlem de "complementari del conjunt A respecte de Ω", on $A \subseteq \Omega$.

Per a determinades aplicacions, estarem interessats en un universal per a diversos conjunts $A, B, \ldots$, tots subconjunts del mateix Ω.

Complementació

Definició 8.10 *Si $A \subseteq \Omega$, es defineix **complementari** o **complement** de A respecte de Ω com la diferència de conjunts $\Omega - A$. Existeixen diverses notacions per al complementari: A^c o $\bar{A}$. Normalment, utilitzem la primera, de manera que*

$$A^c = \Omega - A.$$

Així, $A^c = \Omega - A = \{x : x \in \Omega \wedge x \notin A\} = \{x : x \notin A\} = \{x | x \notin A\}$.

Aquesta última expressió s'accepta si queda sobreentès que és relativament a Ω.

També podem escriure $A^c = \{x | \neg(x \in A)\} = \{x | \neg x \in A\}$.

Exemple 8.47 Considerem:

$\Omega = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$,

$A = \{1,4,6\}$,

$B = \{0,4,5,7,9,12,15\}$.

Obtenim els complementaris dels conjunts A, B respecte de Ω:

$A^c = \{0,2,3,5,7,8,9,10,11,12,13,14,15\}$,

$B^c = \{1,2,3,6,8,10,11,13,14\}$,

$(A \cup B)^c = (\{0,1,4,5,6,7,9,12,15\})^c = \{2,3,8,10,11,14\}$,

$(A \cap B)^c = (\{4\})^c = \{0,1,2,3,5,6,7,8,9,10,11,12,13,14,15\}$. ■

Quins són els possibles universals? Depèn del que ens interessi, de l'aplicació o problema que estiguem tractant. Per exemple, si els conjunts són grups d'alumnes, aleshores Ω pot ser el "conjunt dels alumnes matriculats en una assignatura", o "el conjunt dels alumnes d'una facultat" o "el conjunt dels alumnes de la universitat".

O bé, si $A = \{1,5,8\}$, es pot considerar subconjunt de l'universal format pels dígits decimals $\Omega = \{0,1,2,3,4,5,6,7,8,9\}$ i, aleshores, $A^c = \Omega - A = \{0,2,3,4,6,7,9\}$. Però també podríem considerar altres possibles universals, com per exemple $\Omega' = \{0,1,2,\cdots,100\}$, conjunt dels 100 primers nombres naturals, és a dir, $\Omega' = \{n \in \mathbb{N} | 0 \leq n \leq 100\}$ i considerar complementari de A respecte d'aquest. Aleshores,

$\Omega' - A = \{0,2,3,4,6,7,9,10,11,12,13,\cdots,100\}$.

▷ *Com negar ser element del complementari d'un conjunt?*

$x \notin A^c$, que equival a

$\neg x \in A^c$, que equival a

$\neg\neg x \in A$, que equival a

$x \in A$

▷ ***Diferència de conjunts en termes del complementari***

Suposem A, B subconjunts de Ω. El complementari de la fórmula següent és respecte de Ω. Vegem que:

$A - B = A \cap B^c$.

En efecte, $A - B = \{x | x \in A \wedge x \notin B\} = \{x | x \in A \wedge (x \in \Omega \wedge x \notin B)\}$

$= \{x | x \in A \wedge x \in B^c\} = A \cap B^c$.

Aquesta expressió facilita moltes possibilitats de manipulació de fórmules conjuntistes (per a demostracions, per exemple). Vegeu-ne exemples al final de la secció i seccions posteriors.

Propietats de la complementació

Teorema 8.7 *Sigui Ω conjunt universal per a tots els complementaris de l'enunciat. Siguin A, B subconjunts de Ω.*

a) $\emptyset^c = \Omega$, $\Omega^c = \emptyset$

b) $A^{cc} = A$ $\quad (\Omega - (\Omega - A) = A)$ *(doble complementació)*

c) $A \cap A^c = \emptyset$ *(un conjunt i el seu complementari sempre són disjunts)*

d) $A \cup A^c = \Omega$

e) $A \subseteq B \Leftrightarrow B^c \subseteq A^c$

f) $A = B \Leftrightarrow A^c = B^c$

g) $A \cap B = \emptyset \Leftrightarrow A \subseteq B^c$

h) $A \cup B = \Omega \Leftrightarrow A^c \subseteq B$

i) $(A \cup B)^c = A^c \cap B^c$ *(llei de De Morgan, per a conjunts) (DM1)*

j) $(A \cap B)^c = A^c \cup B^c$ *(llei de De Morgan, per a conjunts) (DM2)*

k) $A \cap B = (A^c \cup B^c)^c$

l) $A \cup B = (A^c \cap B^c)^c$

Demostracions (demostracions detallades per a mostrar tècnica demostrativa)

Siguin A, B subconjunts de Ω.

$\emptyset^c = \Omega$, $\Omega^c = \emptyset$

Demostració

$\emptyset^c = \Omega - \emptyset = \{x | x \in \Omega \wedge x \notin \emptyset\} = \{x | x \in \Omega\} = \Omega$

$\Omega^c = \Omega - \Omega = \{x | x \in \Omega \wedge x \notin \Omega\} = \emptyset$ (o com a cas particular de $A - A = \emptyset$)

Propietat de la doble complementació. Notació: $A^{cc} = (A^c)^c$

$A^{cc} = A \qquad (\Omega - (\Omega - A) = A)$

Demostració

$A^{cc} = (A^c)^c = \{x|x \notin A^c\} = \{x|\neg(x \in A^c)\} = \{x|\neg(x \notin A)\} = \{x|\neg(\neg x \in A)\} = \{x|x \in A\} = A$

$A \cap A^c = \emptyset$ (un conjunt i el seu complementari sempre són disjunts)

Demostració

Mètode 1. $A \cap A^c = \{x|x \in A \wedge x \in A^c\} = \{x|x \in A \wedge x \notin A\} = \emptyset$

Mètode 2. Alternativament, per *reducció a l'absurd*. Suposem $A \cap A^c \neq \emptyset$. Sigui, doncs, $x \in A \cap A^c$. Aleshores, $x \in A$ i $x \in A^c$, per definició d'intersecció. Però, per definició de complementari, és $x \notin A$. Per tant, arribem a la contradicció que existeix un x tal que $x \in A \wedge \neg(x \in A)$.

$A \cup A^c = \Omega$

Demostració

Mètode 1. $A \cup A^c = \{x|x \in A \vee x \in A^c\} = \{x|x \in A \vee x \notin A\} = \Omega$

Mètode 2. Alternativament, de $A \subseteq \Omega$ i de $A^c \subseteq \Omega$ resulta $A \cup A^c \subseteq \Omega$

Sigui ara $x \in \Omega$. Aleshores és $x \in A$ o $x \notin A$. És a dir, $x \in A$ o $x \in A^c$, d'on $x \in A \cup A^c$.

$A \subseteq B$ si, i només si, $B^c \subseteq A^c$ $(A \subseteq B \Leftrightarrow B^c \subseteq A^c)$

Demostració

Mètode 1. És una expressió conjuntista de l'equivalència del contrarecíproc.

L'afirmació "$A \subseteq B$ si, i només si, $B^c \subseteq A^c$" es pot reescriure de diverses maneres:

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \forall y(y \notin B \rightarrow y \notin A)$

$\forall x(x \in A \rightarrow x \in B) \leftrightarrow \forall y(\neg y \in B \rightarrow \neg y \in A)$.

Ara bé, per l'equivalència del contrarecíproc:

$(x \in A \rightarrow x \in B)$,
$(\neg x \in B \rightarrow \neg x \in A)$

són equivalents (per a x arbitrari però fix).

Mètode 2. Alternativament, es pot procedir demostrant dues implicacions, corresponents a l'equivalència següent:

$A \subseteq B \Leftrightarrow B^c \subseteq A^c$

1. $A \subseteq B \Rightarrow B^c \subseteq A^c$?

Hipòtesi: $A \subseteq B$

Tesi: $B^c \subseteq A^c$

Sigui $x \in B^c$. Hem de provar $x \in A^c$ aplicant la hipòtesi. En efecte:

$x \in B^c \Rightarrow x \notin B \overset{A\subseteq B}{\Rightarrow} x \notin A \Rightarrow x \in A^c$

2. $B^c \subseteq A^c \Rightarrow A \subseteq B$?

Hipòtesi: $B^c \subseteq A^c$

Tesi: $A \subseteq B$

Sigui $x \in A$. Hem de provar que $x \in B$, aplicant la hipòtesi.

$x \in A \Rightarrow x \notin A^c \overset{B^c\subseteq A^c}{\Rightarrow} x \notin B^c \Rightarrow x \in B$

$A = B$ si, i només si, $A^c = B^c$ $(A = B \Leftrightarrow A^c = B^c)$

Demostració

Mètode 1. És conseqüència que $x \in A \leftrightarrow x \in B$ equival a $\neg x \in A \leftrightarrow \neg x \in B$ (en general, $(\alpha \leftrightarrow \beta) \leftrightarrow (\neg\alpha \leftrightarrow \neg\beta)$ és cert, o bé $(\alpha \leftrightarrow \beta) \Leftrightarrow (\neg\alpha \leftrightarrow \neg\beta)$ o bé són equivalents $(\alpha \leftrightarrow \beta) \equiv (\neg\alpha \leftrightarrow \neg\beta)$). Per tant:

$A = B$ equival a $\forall x(x \in A \leftrightarrow x \in B)$ cert.

$x \in A \leftrightarrow x \in B$ equival a $x \notin A \leftrightarrow x \notin B$, que és el mateix que (equival)

$x \in A^c \leftrightarrow x \in B^c$.

Per tant, $\forall x(x \in A^c \leftrightarrow x \in B^c)$ és cert.

Equival a $A^c = B^c$.

Mètode 2. Demostrem el resultat si demostrem les implicacions següents:

$A = B \Rightarrow B^c \subseteq A^c$ (1)
$A = B \Rightarrow A^c \subseteq B^c$ (2)
$A^c = B^c \Rightarrow B \subseteq A$ (3)
$A^c = B^c \Rightarrow A \subseteq B$ (4)

Provem-ne algunes de les implicacions. Les altres es provarien de manera similar.

(1): $x \in B^c \Rightarrow x \notin B \overset{A=B}{\Rightarrow} x \notin A \Rightarrow x \in A^c$
(3): $x \in B \Rightarrow x \notin B^c \overset{A^c=B^c}{\Rightarrow} x \notin A^c \Rightarrow x \in A$

Mètode 3. Es pot utilitzar la propietat demostrada anteriorment $A \subseteq B \Leftrightarrow B^c \subseteq A^c$ i el fet que $A = B$ equival a la doble inclusió: $A \subseteq B$ i $B \subseteq A$. El lector completarà la demostració.

$A \cap B = \emptyset$ si, i només si, $A \subseteq B^c$ $(A \cap B = \emptyset \Leftrightarrow A \subseteq B^c)$

Demostració. Demostrem separadament dues implicacions.

Subproblema 1. Vegem $A \cap B = \emptyset \Rightarrow A \subseteq B^c$.

Mètode 1 (demostració directa). Sigui $x \in A$. Si fos $x \in B$, seria de la intersecció $A \cap B$, d'on $A \cap B \neq \emptyset$, cosa que contradiu la hipòtesi. Per tant, $x \notin B$. És a dir, $x \in B^c$, i queda demostrat.

Digressions sobre l'estructura de la demostració, en termes d'elements:

$\forall x(x \notin A \cap B) \Rightarrow \forall y(y \in A \to y \in B^c)$ (enunciat)

$A \cap B = \emptyset \Rightarrow (x \in A \Rightarrow x \in B^c)$ (sense quantificar) (x arbitrari)

$(A \cap B = \emptyset \wedge x \in A) \Rightarrow x \in B^c)$ (sense quantificar) (x arbitrari)

$x \in A \Rightarrow (A \cap B = \emptyset \Rightarrow x \in B^c)$.

Podem quantificar. Per exemple:

$\forall x((A \cap B = \emptyset \wedge x \in A) \to x \in B^c))$

$\forall x((\neg \exists x(x \in A \cap B) \wedge x \in A) \to x \in B^c))$

Mètode 2 alternatiu. Es pot demostrar equivalentment el *contrarecíproc*:

$A \not\subseteq B^c \Rightarrow A \cap B \neq \emptyset$.

Suposem $A \not\subseteq B^c$. Aleshores existeix x tal que $x \in A$ i $x \notin B^c$, i això últim equival a $x \in B$. Per tant, $x \in A \cap B$ i, en conseqüència, $A \cap B \neq \emptyset$.

Subproblema 2. Vegem $A \subseteq B^c \Rightarrow A \cap B = \emptyset$, l'altra implicació.

Mètode 1. Demostrem equivalentment el *contrarecíproc*:

$\neg(A \cap B = \emptyset) \Rightarrow \neg(A \subseteq B^c)$, és a dir,

$(A \cap B \neq \emptyset) \Rightarrow (A \not\subseteq B^c)$.

Per la hipòtesi existeix un element x tal que $x \in A \cap B$, és a dir, $x \in A$ i $x \in B$. Per tant, $x \notin B^c$. Així, doncs, existeix x tal que $x \in A \wedge x \notin B^c$; això demostra $A \not\subseteq B^c$.

Observació: Es pot fer una reformulació de la demostració anterior, de manera que en resulti una demostració *per reducció a l'absurd*, com veiem al mètode següent:

Mètode 2 (per reducció a l'absurd). Suposem certa la negació de la implicació $A \subseteq B^c \Rightarrow A \cap B = \emptyset$: és a dir, que es compleix $A \subseteq B^c$ i $A \cap B \neq \emptyset$. Per la condició $A \cap B \neq \emptyset$, existeix $x \in A \cap B$, és a dir, tal que $x \in A$ i $x \in B$. Però, essent $x \in A$ i aplicant $A \subseteq B^c$, resulta $x \in B^c$, d'on $x \notin B$. Hem arribat a la contradicció: $x \in B$ i $x \in B^c$.

$A \cup B = \Omega$ si, i només si, $A^c \subseteq B$ $(A \cup B = \Omega \Leftrightarrow A^c \subseteq B)$.

Demostració. Vegem les dues implicacions separadament.

Subproblema 1. Vegem $A \cup B = \Omega \Rightarrow A^c \subseteq B$.

Mètode 1. Sigui $x \in A^c$, és a dir, $x \notin A$. És òbviament $x \in \Omega$. Per hipòtesi, $x \in (A \cup B)$, d'on la disjuntiva $x \in A$, o bé $x \in B$. Atès que $x \notin A$, necessàriament $x \in B$. En resum, $x \in A^c \Rightarrow x \in B$, i queda demostrat.

Mètode 2 alternatiu: pel contrarecíproc. Vegem $A \nsubseteq B \Rightarrow A \cup B \neq \Omega$.

Mètode 1. Suposem $A^c \nsubseteq B$. Aleshores existeix $x \in A^c$ tal que $x \notin B$. Equivalentment, existeix x tal que $x \notin A$ i $x \notin B$, és a dir, tal que $x \notin A \cup B$. Això implica que $A \cup B \neq \Omega$.

Subproblema 2. Vegem l'altra implicació: $A^c \subseteq B \Rightarrow A \cup B = \Omega$.

Atès que A, B són subconjunts de Ω, ja tenim $A \cup B \subseteq \Omega$. Vegem que $\Omega \subseteq A \cup B$. Sigui $x \in \Omega$. Considerem les possibilitats (casos):

– $x \in A$. Aleshores $x \in A \cup B$, i ja hem acabat.
– $x \notin A$. Aleshores $x \in A^c$. Aplicant la hipòtesi, $x \in B$ d'on $x \in A \cup B$ i ja hem acabat.

Mètode 2 alternatiu: pel contrarecíproc. Recordem que sempre es compleix $A \cup B \subseteq \Omega$.

Si $A \cup B \neq \Omega$, aleshores existeix $x \in \Omega$ tal que $x \notin A \cup B$. Per tant:

$\exists x (x \notin A \wedge x \notin B)$, és a dir,

$\exists x (x \in A^c \wedge x \notin B)$, que equival a dir

$A^c \nsubseteq B$.

Teorema 8.8 **(Lleis-propietats de De Morgan per a conjunts)** *Siguin A, B subconjunts de Ω. Els complementaris són relatius a Ω:*

(DM1): $(A \cup B)^c = A^c \cap B^c$

(DM2): $(A \cap B)^c = A^c \cup B^c$

Són les que corresponen a les lleis de De Morgan per a proposicions.

Alternatives a les fórmules anteriors. Les fórmules anteriors també es poden expressar explicitant l'universal:

$\Omega - (A \cup B) = (\Omega - A) \cap (\Omega - B)$ (DM1)
$\Omega - (A \cap B) = (\Omega - A) \cup (\Omega - B)$ (DM2)

Demostració de les lleis de De Morgan per a conjunts

Demostració de (DM1): $(A \cup B)^c = A^c \cap B^c$

Mètode 1. Consisteix essencialment a aplicar una de les equivalències de De Morgan (lògica).

$(A \cup B)^c =$

$= \{x | x \notin (A \cup B)\}$ (definició de complementari d'un conjunt)

$= \{x | \neg x \in (A \cup B)\}$ (reescriptura)

$= \{x | \neg(x \in A \vee x \in B)\}$ (definició d'unió de conjunts)

$= \{x | (\neg x \in A) \wedge (\neg x \in B)\}$ (De Morgan, lògica)

$= \{x | (x \notin A) \wedge (x \notin B)\}$ (reescriptura)

$= \{x | x \in A^c \wedge x \in B^c\}$ (reescriptura)

$= A^c \cap B^c$ (definició d'intersecció de conjunts)

Observació. Les línies 3, 4, 5 anteriors es poden ometre si fem servir el que s'ha demostrat sobre no pertànyer a la unió de dos conjunts, que involucra l'equivalència lògica de De Morgan per a proposicions/predicats:

$x \notin (A \cup B) \overset{(*)}{\Leftrightarrow} (x \notin A \wedge x \notin B)$.

Recordem que aquesta última es pot obtenir mitjançant la seqüència d'equivalències:

$x \notin (A \cup B)$

$\neg x \in (A \cup B)$

$\neg(x \in A \vee x \in B)$

$\neg x \in A \wedge \neg x \in B)$ (De Morgan, lògica)

$x \notin A \wedge x \notin B)$.

Mètode 2 (i un altre estil expositiu). Es pot escollir un altre estil expositiu, perfectament vàlid. Suposem que volem demostrar la igualtat dels dos conjunts demostrant les dues inclusions:

$(A \cup B)^c \subseteq A^c \cap B^c$ (subproblema 1) i

$A^c \cap B^c \subseteq (A \cup B)^c$ (subproblema 2).

Subproblema 1. Vegem-ne la primera (i anàlogament per a la segona).

S'ha de demostrar que $\forall x(x \in (A \cup B)^c \to x \in A^c \cap B^c)$ és cert.

Fixat un x arbitrari, cal provar la implicació: $x \in (A \cup B)^c \Rightarrow x \in A^c \cap B^c$.

Hipòtesi: $x \in (A \cup B)^c$

Tesi: $x \in A^c \cap B^c$

Sigui $x \in (A \cup B)^c$. Aleshores $x \notin (A \cup B)$. Per tant, pel que abans hem escrit (*), $x \notin A$ i $x \notin B$. En conseqüència, $x \in A^c$ i $x \in B^c$, d'on, finalment, $x \in A^c \cap B^c$.

Subproblema 2. Vegem-ne la segona: $A^c \cap B^c \subseteq (A \cup B)^c$.

Sigui $x \in A^c \cap B^c$; vegem que, consegüentment, $x \in (A \cup B)^c$.

$x \in A^c \cap B^c \Rightarrow (x \in A^c \wedge x \in B^c) \Rightarrow (x \notin A \wedge x \notin B) \overset{*}{\Rightarrow} x \notin A \cup B \Rightarrow x \in (A \cup B)^c$.

Observació: (*) és de fet una equivalència, que es pot afirmar per De Morgan (lògica).

Demostració de (DM2): $(A \cap B)^c = A^c \cup B^c$.

És similar a l'anterior.

$$
\begin{aligned}
(A \cap B)^c &= \\
&= \{x | x \notin (A \cap B)\} && \text{(definició de complementari)} \\
&= \{x | \neg x \in (A \cap B)\} && \text{(reescriptura)} \\
&= \{x | \neg (x \in A \wedge x \in B)\} && \text{(definició d'intersecció)} \\
&= \{x | (\neg x \in A) \vee (\neg x \in B)\} && \text{(De Morgan, lògica)} \\
&= \{x | (x \notin A) \vee (x \notin B)\} && \text{(reescriptura)} \\
&= \{x | x \in A^c \vee x \in B^c\} && \text{(reescriptura)} \\
&= A^c \cup B^c && \text{(definició d'unió).}
\end{aligned}
$$

Observació: Les línies 3, 4, 5 es poden ometre si fem servir el que hem demostrat sobre no pertànyer a la intersecció de dos conjunts, que involucra De Morgan per a proposicions/predicats (lògica):

$x \notin (A \cap B) \Leftrightarrow (x \notin A \vee x \notin B)$.

Es pot procedir de manera similar a la demostració del (DM1) anterior.

PROBLEMA 8.11

a) *Demostreu (DM2), suposat demostrat (DM1).*

b) *Demostreu (DM1), suposat demostrat (DM2).*

Solució

a) *Demostració de (DM2), suposat demostrat (DM1)*

Es poden considerar diverses variants argumentals. Fem servir la igualtat de doble complementació ($D^{cc} = D$).

Variant argumental 1:

$(A \cap B)^c =$

$= (A^{cc} \cap B^{cc})^c$ (doble complementació)

$= A^{ccc} \cup B^{ccc}$ (DM1)

$= A^c \cup B^c$ (doble complementació)

Variant argumental 2:

$(A \cap B)^c =$

$= (A^{cc} \cap B^{cc})^c$ (doble complementació)

$= ((A^c)^c \cap (B^c)^c)^c$

$= ((A^c \cup B^c)^c)^c$ (per DM1)

$= (A^c \cup B^c)^{cc}$

$= A^c \cup B^c$ (doble complementació)

Variant argumental 3:

$A \cap B =$

$= A^{cc} \cap B^{cc}$ (doble complementació)

$= (A^c \cup B^c)^c$ (per DM1)

Ara, fent servir $C = D \Leftrightarrow C^c = D^c$, resulta, per doble complementació,

$(A \cap B)^c = ((A^c \cup B^c)^c)^c = (A^c \cup B^c)^{cc} = A^c \cup B^c$.

b) *Demostració de (DM1), suposat demostrat (DM2)*. Anàlogament al cas anterior. Vegem-ne una variant possible:

$(A \cup B)^c = (A^{cc} \cup B^{cc})^c$ (doble complementació)

$= [(A^c)^c \cup (B^c)^c]^c$

$= [(A^c \cap B^c)^c]^c$ (per DM2)

$= (A^c \cap B^c)^{cc}$

$= A^c \cap B^c$ (doble complementació)

Per a les lleis de De Morgan, són possibles altres mètodes de demostració: doble inclusió conjuntista, seqüència d'equivalències amb elements, per taula de pertinença (secció posterior).

Generalització de les lleis de De Morgan. Vegem com demostrar l'anàleg a les lleis de De Morgan per a tres conjunts. Fem servir la propietat ja demostrada per a dos conjunts i l'associativitat. Per exemple, vegem que:

$(A \cap B \cap C)^c = A^c \cup B^c \cup C^c$

En efecte:

$(A \cap B \cap C)^c =$
$= ((A \cap B) \cap C)^c$ (propietat associativa de la intersecció)
$= (A \cap B)^c \cup C^c$ (DM1)
$= (A^c \cup B^c) \cup C^c$ (DM2)
$= A^c \cup B^c \cup C^c$ (propietat associativa de la unió).

I anàlogament per a

$(A \cup B \cup C)^c = A^c \cap B^c \cap C^c$ (exercici)

Exercici: Escriviu i demostreu resultats anàlegs per a quatre conjunts.

Generalització a n conjunts

En general, seria, per a $n \geq 2$:

$(A_1 \cap \cdots \cap A_n)^c = A_1^c \cup \cdots \cup A_n^c$,
$(A_1 \cup \cdots \cup A_n)^c = A_1^c \cap \cdots \cap A_n^c$.

La demostració es pot fer per inducció (vegeu capítol corresponent).

Vegem unes fórmules interessants:

$\boxed{A \cap B = (A^c \cup B^c)^c}$ $\boxed{A \cup B = (A^c \cap B^c)^c}$

Demostració. És una aplicació de les lleis de De Morgan (conjunts) i de la propietat de doble complementació.

$A \cap B = (A \cap B)^{cc} = ((A \cap B)^c)^c = ((A^c \cup B^c))^c = (A^c \cup B^c)^c$

$A \cup B = (A \cup B)^{cc} = ((A \cup B)^c)^c = ((A^c \cap B^c))^c = (A^c \cap B^c)^c$

Són interessants perquè permeten expressar la unió i la intersecció en funció de l'altra i el complementari.

Vegem, a continuació, per mitjà d'exercicis, exemples d'aplicació de les propietats anteriors, resolts per manipulacions conjuntistes, amb complementari; s'ometen altres possibles mètodes per a demostrar la igualtat de dos conjunts, que el lector hauria d'intentar. Se suposa que els complementaris ho són respecte d'algun conjunt "universal".

PROBLEMA 8.12

Siguin A, B, C conjunts. Demostreu

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

Solució. En efecte:

$A - (B \cup C) =$

$= A \cap (B \cup C)^c$ (per la propietat $X - Y = X \cap Y^c$)

$= A \cap (B^c \cap C^c)$ (per De Morgan, conjunts)

$= (A \cap A) \cap (B^c \cap C^c)$ (per $X \cap X = X$)

$= (A \cap B^c) \cap (A \cap C^c)$ (per les propietats commutativa i associativa de la intersecció)

$= (A - B) \cap (A - C)$.

PROBLEMA 8.13

Siguin A, B, C conjunts. Demostreu, de forma anàloga a l'anterior:

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

Solució

$A - (B \cap C) =$

$= A \cap (B \cap C)^c$

$= A \cap (B^c \cup C^c)$ (per De Morgan, conjunts)

$= (A \cap B^c) \cup (A \cap C^c)$ (per distributivitat de la intersecció respecte de la unió)

$= (A - B) \cup (A - C)$.

PROBLEMA 8.14

Siguin A, B conjunts. Demostreu, de forma anàloga als anteriors:

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

Solució

$(A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B)^c$ (per expressió de la diferència en termes del complementari)

$= (A \cup B) \cap (A^c \cup B^c)$ (per De Morgan, conjunts)

$= [(A \cup B) \cap A^c] \cup [(A \cup B) \cap B^c]$ (per distributivitat de $\cap$ respecte de $\cup$)

$= [(A \cap A^c) \cup (B \cap A^c)] \cup [(A \cap B^c) \cup (B \cap B^c)]$ (per distributivitat de $\cup$ respecte de $\cap$)

$= [\emptyset \cup (B \cap A^c)] \cup [(A \cap B^c) \cup \emptyset]$ (per $X \cap X^c = \emptyset, \forall X$)

$= (B \cap A^c) \cup (A \cap B^c)$ (per $\emptyset \cup X = X, \forall X$)

$= (B - A) \cup (A - B)$ (reexpressió).

PROBLEMA 8.15

Siguin A,B conjunts. Demostreu per manipulació conjuntista, utilitzant el complementari (respecte de Ω), les propietats següents, ja demostrades anteriorment.

a) $A-\emptyset=A$

b) $\emptyset-A=\emptyset$

c) $A-A=\emptyset$

d) $A-B=A-(A\cap B)$

e) $(A-B)\cap B=\emptyset$

f) $(A-B)\cap(B-A)=\emptyset$

Solució

a) $A-\emptyset=A$. En efecte:

$$A-\emptyset=A\cap\emptyset^c=A\cap\Omega=A.$$

b) $\emptyset-A=\emptyset$. En efecte:

$$\emptyset-A=\emptyset\cap A^c=\emptyset.$$

c) $A-A=\emptyset$. En efecte:

$$A-A=A\cap A^c=\emptyset.$$

d) $A-B=A-(A\cap B)$. En efecte:

$$A-(A\cap B)=A\cap(A\cap B)^c=A\cap(A^c\cup B^c) \text{ (per De Morgan, conjunts)}$$
$$=(A\cap A^c)\cup(A\cap B^c) \text{ (per distributivitat de } \cap \text{ respecte de } \cup)$$
$$=\emptyset\cup(A\cap B^c)=A\cap B^c=A-B.$$

e) $(A-B)\cap B=\emptyset$. En efecte:

$$(A-B)\cap B=(A\cap B^c)\cap B=A\cap(B^c\cap B)=A\cap\emptyset=\emptyset.$$

f) $(A-B)\cap(B-A)=\emptyset$. En efecte:

$$(A-B)\cap(B-A)=(A\cap B^c)\cap(B\cap A^c)=(A\cap A^c)\cap(B\cap B^c)=\emptyset\cap\emptyset=\emptyset.$$

PROBLEMA 8.16

Siguin A,B conjunts, subconjunts de Ω. Proveu que $A\cup B=(A\cap B^c)\cup B$.

Observeu que s'expressa $A\cup B$ com a reunió de dos conjunts disjunts.

Solució

Mètode 1. Per equivalències lògiques. Coincideixen perquè ambdós conjunts es descriuen per fórmules lògiques equivalents. Vegem la seqüència d'equivalències:

$x \in (A \cap B^c) \cup B$

$(x \in A \wedge x \notin B) \vee x \in B$

$(x \in A \vee x \in B) \wedge (x \notin B \vee x \in B)$ (per distributivitat de $\vee$ respecte de $\wedge$)

$(x \in A \vee x \in B) \wedge \mathbb{T}$

$(x \in A \vee x \in B)$

$x \in A \cup B$.

Mètode 2. Per operacions conjuntistes:

$(A \cap B^c) \cup B \overset{(1)}{=} (A \cup B) \cap (B^c \cup B) \overset{(2)}{=} (A \cup B) \cap \Omega \overset{(3)}{=} A \cup B$.

(1): aplicant la distributivitat de $\cup$ respecte de $\cap$.

(2): $X^c \cup X = \Omega$.

(3): $X \cap \Omega = X$.

Mètode 3. Veient que les taules de pertinença coincideixen (vegeu secció posterior).

Mètode 4. Per doble inclusió. És a dir, $A \cup B \subseteq (A \cap B^c) \cup B$ i $(A \cap B^c) \cup B \subseteq A \cup B$. El lector en completarà la demostració.

PROBLEMA 8.17

Siguin A, B conjunts, subconjunts de Ω. Proveu que $A \cup B = (A \cap B) \cup (A \cap B^c)$.

Observeu que $A \cup B$ s'expressa com a reunió de dos conjunts disjunts.

Solució

Mètode 1. Per equivalències lògiques. Coincideixen perquè ambdós conjunts es descriuen per fórmules lògiques equivalents:

$x \in (A \cap B) \cup (A \cap B^c)$

$x \in (A \cap B) \vee x \in (A \cap B^c)$

$(x \in A \wedge x \in B) \vee (x \in A \wedge x \in B^c)$

$(x \in A \wedge x \in B) \vee (x \in A \wedge x \notin B)$

$x \in A \wedge (x \in B \vee x \notin B)$

$x \in A \wedge \mathbb{T}$

$x \in A$.

Mètode 2. Per operacions conjuntistes:

$(A \cap B) \cup (A \cap B^c) = A \cap (B \cup B^c) = A \cap \Omega = A$. Hem utilitzat la distributivitat de la intersecció respecte de la reunió.

Mètode 3. Veient que les taules de pertinença coincideixen (vegeu secció posterior).

Mètode 4. Per doble inclusió. És a dir, $A \cup B \subseteq (A \cap B) \cup (A \cap B^c)$ i $(A \cap B) \cup (A \cap B^c) \subseteq A \cup B$. El lector en completarà la demostració.

PROBLEMA 8.18

Siguin A, B, C conjunts, subconjunts de Ω. Es consideraran complementaris respecte de Ω.

a) Demostreu la distributivitat de $\cap$ respecte de $\cup$

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

a partir de la distributivitat de $\cup$ respecte de $\cap$, és a dir,

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \text{ (}X, Y, Z \text{ conjunts) (hipòtesi).}$$

b) Demostreu la distributivitat de $\cup$ respecte de $\cap$

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

a partir de la distributivitat de $\cap$ respecte de $\cup$.

Solució. Demostrem el primer apartat. L'altre es provaria similarment (exercici).

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

$= [A \cap (B \cup C)]^{cc}$ (per doble complementació)

$= [[A \cap (B \cup C)]^c]^c$ (reescriptura)

$= [A^c \cup (B \cup C)^c]^c$ (per De Morgan, conjunts)

$= [A^c \cup (B^c \cap C^c)]^c$ (per De Morgan, conjunts)

$= [(A^c \cup B^c) \cap (A^c \cup C^c)]^c$ (per hipòtesi)

$= (A^c \cup B^c)^c \cup (A^c \cup C^c)^c$ (per De Morgan, conjunts)

$= (A^{cc} \cap B^{cc}) \cup (A^{cc} \cap C^{cc})$ (per De Morgan, conjunts)

$= (A \cap B) \cup (A \cap C)$ (per doble complementari).

8.10. Fórmules conjuntistes i taules de pertinença

8.10.1. Fórmules conjuntistes

A partir de $\emptyset$, Ω (universal) i les lletres (en provisió infinita): $A, \ldots, A_1, \ldots$, i altres, i amb les regles de bona formació (gramàtica) involucrant les operacions conjuntistes (operadors) $\cup$ (unió), $\cap$ (intersecció), $-$ (diferència) (se'n pot considerar una versió equivalent amb l'operador complementari $X^c (= \Omega - X)$), es formen les fórmules conjuntistes.

En seccions anteriors, ja han aparegut fórmules conjuntistes.

Exemples 8.48 Siguin A,B,C conjunts, i Ω el conjunt universal que els conté.

1. $(A-B)\cup(A\cap B)\cup(B-A)$
2. $(\Omega-A)\cap(\Omega-B)$
3. $(A\cup B)^c$
4. $A-(B-C)$
5. $((A-(B\cup C))-D)\cap E$
6. $(A\cup B)-(A\cap B)$. ■

Més formalment, la gramàtica de generació és de tipus similar a la de les fórmules proposicionals i les fórmules de predicat:

Constants: $\emptyset$, Ω

Variables: $A,B,\cdots$

Operadors conjuntistes: $\cup,\cap,^c,-$

Regles de generació de fórmules ben formades:

- $\emptyset$, Ω, $A,B,\ldots$ són fórmules conjuntistes,
- Si F és una fórmula conjuntista, també ho és F^c,
- Si F,G són fórmules conjuntistes, també ho és $F\cup G$,
- Si F,G són fórmules conjuntistes, també ho és $F\cap G$.

Regla addicional:

- Si F,G són fórmules conjuntistes, també ho és $F-G$ i $G-F$.

Qualsevol dels operadors $^c,-$ és redundant si disposem de l'altre, ja que $X^c=\Omega-X$ i $X-Y=X\cap Y^c$. També seria redundant la regla addicional. Però resulta còmode disposar dels dos, i els utilitzarem quan ens convingui.

Observem que el sistema descrit anteriorment és purament lexicosintàctic. No afecta la semàntica, el significat: per a això ja s'han definit prèviament els significats de les operacions conjuntistes.

Subfórmules. També podem parlar de subfórmules, subcadenes de caràcters de la fórmula que, al seu torn, són fórmules. Així, les subfórmules de $(A\cup B)-(A\cap B)$ són: A, B, $(A\cup B)$, $(A\cap B)$, $(A\cup B)-(A\cap B)$. Detallant:

Les lletres: A,B

Les fórmules intermèdies: $A\cup B$, $A\cap B$

La fórmula (total): $(A\cup B)-(A\cap B)$

Conjunts definits per fórmules conjuntistes. En principi, la formació de fórmules conjuntistes és un procés purament sintàctic. Però podem utilitzar-les per definir nous conjunts a partir de conjunts preexistents, subconjunts de Ω. Per exemple, $(A-B)\cup(A\cap B)\cup(B-A)$ definiria un nou conjunt a partir dels conjunts A i B.

Quin és el nou conjunt definit per una fórmula conjuntista? És el que està format pels elements per als quals la fórmula lògica corresponent és certa. Així, per exemple:

$A\cap(B-C)=\{x|x\in A\wedge(x\in B\wedge x\notin C)\}=\{x|x\in A\wedge x\in B\wedge x\notin C\}$

Si F és una fórmula conjuntista, $x\in F$ significa que x és un element del conjunt que defineix F.

Exemple 8.49 Considerem els conjunts $A=\{1,2,4,x\}$, $B=\{2,5,x,y\}$, $C=\{2,y,z,*\}$.

Obteniu $D=(A\cap B)-C$.

En primer lloc, podem procedir atenent les definicions de les operacions conjuntistes:

Calculem $A\cap B=\{2,x\}$ i ara $D=(A\cap B)-C=\{2,x\}-\{2,y,z,*\}=\{x\}$.

O també $(\{1,2,4,x\}\cap\{2,5,x,y\})-\{2,y,z,*\}=\{x\}$.

En segon lloc, alternativament, podríem descriure els elements del conjunt com aquells per als quals una fórmula lògica és certa, concretament

$D=(A\cap B)-C=\{t|(t\in A\wedge t\in B)\wedge t\notin C\}$.

Aquestes formulacions són més útils per a demostracions abstractes, d'igualtat de conjunts, per a tot A,B, etc. En tot cas, vegem-ne alguns exemples:

$1\in D$? Per a $t=1$, la fórmula lògica anterior, definitòria del conjunt, pren el valor veritatiu $(1\wedge 0)\wedge 1\equiv 0\wedge 1\equiv 0$; per tant, $1\notin D$.

$2\in D$? Per a $t=2$, la fórmula lògica anterior pren el valor veritatiu $(1\wedge 1)\wedge 0\equiv 1\wedge 0\equiv 0$; per tant, $2\notin D$.

$x\in D$? Per a $t=x$, la fórmula lògica anterior, definitòria del conjunt, pren el valor veritatiu $(1\wedge 1)\wedge 1\equiv 1\wedge 1\equiv 1$; per tant, $x\in D$.

I així successivament (és poc pràctic; reservem el mètode per a problemes abstractes). ■

PROBLEMA 8.19

Siguin A,B,C,D,E conjunts.

a) *Doneu una fórmula lògica que defineixi el conjunt donat per la fórmula conjuntista:* $(((C\cup(D-E))-A)-(B\cap C))-D$.

b) *Donada la fórmula lògica* $((x\in A\wedge x\in B))\wedge x\notin(C-D))\vee(x\in D\wedge(x\notin A\vee x\notin E)))$, *indiqueu quina fórmula conjuntista defineix.*

Solució

a) $F = (((C \cup (D - E)) - A) - (B \cap C)) - D$

Per tal de facilitar l'obtenció i l'escriptura de la fórmula, escrivim:

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

$V = (C \cup (D - E)) - A$,

$T = C \cup (D - E)$. Aleshores, escriurem una seqüència de fórmules equivalents, totes equivalents a $x \in F$. Recordem que podem substituir $x \notin$ per $\neg x \in$:

$x \in W \wedge x \notin D$

$(x \in V \wedge x \notin B \cap C) \wedge x \notin D$

$(x \in V \wedge (x \notin B \vee x \notin C)) \wedge x \notin D$

$((x \in T \wedge x \notin A) \wedge (x \notin B \vee x \notin C)) \wedge x \notin D$

$(((x \in C \vee x \in D - E) \wedge x \notin A) \wedge (x \notin B \vee x \notin C)) \wedge x \notin D$

$(((x \in C \vee (x \in D \wedge x \notin E)) \wedge x \notin A) \wedge (x \notin B \vee x \notin C)) \wedge x \notin D$.

No hem fet cap intent final de simplificació. És una traducció literal.

b) $((x \in A \wedge x \in B)) \wedge x \notin (C - D)) \vee (x \in D \wedge (x \notin A \vee x \notin E)))$

Partim de la fórmula i n'obtenim literalment la fórmula conjuntista corresponent, sense cap intent de simplificació o modificació de la fórmula lògica.

$((x \in A \wedge x \in B)) \wedge x \notin (C - D)) \vee (x \in D \wedge (x \notin A \vee x \notin E)))$

$(x \in (A \cap B) \wedge x \notin (C - D)) \vee (x \in D \wedge x \notin (A \cap E))$

$x \in (A \cap B) - (C - D) \vee x \in D - (A \cap E)$

$((A \cap B) - (C - D)) \cup (D - (A \cap E))$.

Equivalentment, la fórmula lògica hauria pogut ser

$((x \in A \wedge x \in B)) \wedge (x \notin C \vee x \in D)) \vee (x \in D \wedge (x \notin A \vee x \notin E)))$,

ja que

$x \notin C - D$ és $\neg x \in C - D$, que equival a

$\neg(x \in C \wedge x \notin D)$, que equival, per De Morgan, a

$\neg x \in C \vee \neg x \notin D)$, que equival a

$x \notin C \vee x \in D$, per doble negació.

PROBLEMA 8.20

Donats els conjunts:

$A = \{1,3,5,\{x\},y,\{z,t\}\},$

$B = \{3,*,x,y\},$

$C = \{3,y,w\},$

obteniu $D = (A \cup (B - C)) - (C \cap B)$.

Solució. Procedim per parts (de fet, calculem el valor de les subfórmules, que hem d'identificar):

$B - C = \{*,x\}$

$C \cap B = \{3,y\}$

$A \cup (B - C) = \{1,3,5,\{x\},y,\{z,t\},*,x\}$

$D = (A \cup (B - C)) - (C \cap B) = \{1,3,5,\{x\},y,\{z,t\},*,x\} - \{3,y\} = \{1,5,\{x\},\{z,t\},*,x\}.$

Igualtat. Què vol dir que dues fórmules conjuntistes són iguals? Per exemple, quan escrivim $(A-B)\cup(A\cap B)\cup(B-A) = A\cup B$, les fórmules són diferents (cadenes de caràcters diferents), però la igualtat significa que els conjunts que defineixen, a partir del conjunts A,B, són iguals, és a dir, tenen els mateixos elements. Els elements respectius satisfan fórmules lògiques equivalents.

Per exemple, $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$ perquè són equivalents: $x \in A \wedge (x \in B \vee x \in C)$ i $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$.

Exemple 8.50 Siguin A,B,C conjunts.

Vegem que els conjunts definits per les fórmules $(A\cup B)-C$, $(A-C)\cup(B-C)$ són iguals.

És a dir, $(A\cup B)-C = (A-C)\cup(B-C)$.

Mètode 1. Efectuant operacions conjuntistes:

$(A\cup B) - C = (A\cup B)\cap C^c$

$= (A\cap C^c)\cup(B\cap C^c)$, per la distributivitat de $\cap$ respecte de $\cup$,

$= (A-C)\cup(B-C)$.

Mètode 2. Per una seqüència d'equivalències lògiques:

Per a un x arbitrari, tenim la seqüència de fórmules equivalents que demostren la igualtat:

$x \in (A\cup B) - C$

$x \in (A\cup B) \wedge x \notin C$ (o bé: $x \in (A\cup B) \wedge \neg x \in C$)

$(x \in A \vee x \in B) \wedge x \notin C$

$(x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C)$ (per distributivitat de $\wedge$ respecte de $\vee$)

$(x \in A - C) \vee (x \in B - C)$

$x \in (A - C) \cup (B - C)$.

Una variant expositiva (on, de fet, demostrem $(A \cup B) - C \subseteq (A - C) \cup (B - C)$):

$x \in (A \cup B) - C \Rightarrow$

$\Rightarrow x \in (A \cup B) \wedge x \notin C$

$\Rightarrow (x \in A \vee x \in B) \wedge x \notin C$

$\Rightarrow (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C)$ (per distributivitat de $\wedge$ respecte de $\vee$)

$\Rightarrow (x \in A - C) \vee (x \in B - C)$

$\Rightarrow (x \in A - C) \cup (B - C)$.

Les implicacions anteriors són reversibles, de manera que demostrem equivalències ($\Leftrightarrow$); en conseqüència, l'altra inclusió resulta demostrada i, per tant, la igualtat dels conjunts:

$x \in (A \cup B) - C \Rightarrow$

$\Leftrightarrow x \in (A \cup B) \wedge x \notin C$

$\Leftrightarrow (x \in A \vee x \in B) \wedge x \notin C$

$\Leftrightarrow (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C)$ (per distributivitat de $\wedge$ respecte de $\vee$)

$\Leftrightarrow (x \in A - C) \vee (x \in B - C)$

$\Leftrightarrow x \in (A - C) \cup (B - C)$.

Una variant argumental conjuntista:

$(A \cup B) - C = \{x | (x \in A \vee x \in B) \wedge x \notin C\} =$

$= \{x | (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C)\}$

$= \{x | (x \in A - C) \vee (x \in B - C)\}$

$= \{x | x \in (A - C) \cup (B - C)\}$

$= (A - C) \cup (B - C)$.

Així, $\forall A \forall B \forall C ((A \cup B) - C = (A - C) \cup (B - C))$, amb A, B, C conjunts. ■

Exemple 8.51 Siguin A, B, C conjunts.

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

Es demostra de forma similar a l'exemple anterior. Vegem-ne alguns mètodes.

Mètode 1. Efectuant operacions conjuntistes:

$(A \cap B) - C = (A \cap B) \cap C^c$

$(A \cap B) \cap (C^c \cap C^c)$ (per $X = X \cap X$)

$= (A \cap C^c) \cap (B \cap C^c)$, per l'associativitat de $\cap$

$= (A - C) \cap (B - C)$.

Mètode 2. Per una seqüència d'equivalències lògiques:

Per a un x arbitrari, tenim la seqüència de fórmules equivalents que demostren la igualtat:

$x \in (A \cap B) - C$

$x \in (A \cap B) \wedge x \notin C$

$(x \in A \wedge x \in B) \wedge x \notin C$

$(x \in A \wedge x \in B) \wedge (x \notin C \wedge x \notin C)$

$(x \in A \wedge x \notin C) \wedge (x \in B \wedge x \notin C)$ (per associativitat de $\wedge$)

$(x \in A - C) \vee (x \in B - C)$

$x \in (A - C) \cup (B - C)$.

Així, $\forall A \forall B \forall C((A \cap B) - C = (A - C) \cap (B - C))$. ■

PROBLEMA 8.21

Siguin A, B, C conjunts. Demostreu per diversos mètodes:

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

Solució. Escrivim una seqüència d'equivalències lògiques:

$x \in A - (B \cup C)$, equivalent a

$x \in A \wedge x \notin (B \cup C)$, equivalent a

$x \in A \wedge (x \notin B \wedge x \notin C)$, equivalent a

$(x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C)$, equivalent a

$(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$, equivalent a

$x \in A - B \wedge x \in A - C$, equivalent a

$x \in (A - B) \cap (A - C)$.

En resum, per a un x arbitrari, resulta:

$x \in A - (B \cup C) \Leftrightarrow x \in (A - B) \cap (A - C)$, és a dir, és cert

$\forall x(x \in A - (B \cup C) \leftrightarrow x \in (A - B) \cap (A - C))$.

I així queda demostrada la igualtat dels conjunts.

Equival a demostrar la doble inclusió:

$A - (B \cup C) \subseteq (A - B) \cap (A - C)$ (per $x \in A - (B \cup C) \Rightarrow x \in (A - B) \cap (A - C)$)

$(A - B) \cap (A - C) \subseteq A - (B \cup C)$ (per $(A - B) \cap (A - C) \Rightarrow A - (B \cup C)$).

Alternatives expositives. Es poden fer reformulacions, essencialment reescriptura, de les mateixes idees:

En termes de $\Leftrightarrow$:

$x \in A - (B \cup C)$

$\Leftrightarrow x \in A \wedge x \notin (B \cup C)$

$\Leftrightarrow x \in A \wedge (x \notin B \wedge x \notin C)$

$\Leftrightarrow (x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C)$

$\Leftrightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$

$\Leftrightarrow x \in A - B \wedge x \in A - C$

$\Leftrightarrow x \in (A - B) \cap (A - C)$.

O bé amb la seqüència d'implicacions, **totes reversibles**:

$x \in A - (B \cup C)$

$\Rightarrow x \in A \wedge x \notin (B \cup C)$

$\Rightarrow x \in A \wedge (x \notin B \wedge x \notin C)$

$\Rightarrow (x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C)$

$\Rightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$

$\Rightarrow x \in A - B \wedge x \in A - C$

$\Rightarrow x \in (A - B) \cap (A - C)$.

O bé:

$A - (B \cup C) =$

$= \{x | x \in A \wedge x \notin (B \cup C)\} =$

$= \{x | x \in A \wedge (x \notin B \wedge x \notin C)\}$

$= \{x | (x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C)\}$

$= \{x | (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)\}$

$= \{x | x \in A - B \wedge x \in A - C\}$

$= A - B) \cap (A - C)$.

Observació. Anteriorment, s'ha resolt per operacions conjuntistes. També es resoldrà per taules de pertinença.

PROBLEMA 8.22

Siguin A, B, C conjunts. Demostreu per diversos mètodes:

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

Solució. És similar a l'exercici anterior. Per aquest motiu, només en presentem un mètode; la resta són similars a l'exercici anterior.

Vegem que, per a un x qualsevol:

$x \in A - (B \cap C) \Leftrightarrow x \in (A - B) \cup (A - C)$.

És a dir, és cert:

$\forall x(x \in A - (B \cap C) \leftrightarrow x \in (A - B) \cup (A - C))$.

Equival a demostrar les dues inclusions:

$A - (B \cap C) \subseteq (A - B) \cup (A - C)$

$(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

Establim l'afirmació per mitjà d'una seqüència d'equivalències:

$x \in A - (B \cap C)$, que equival a

$x \in A \wedge x \notin (B \cap C)$, que equival a

$x \in A \wedge (x \notin B \vee x \notin C)$, que, per distributivitat de $\wedge$ respecte de $\vee$, equival a

$(x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C)$, que equival a

$(x \in A - B) \vee (x \in A - C)$, que equival a

$x \in (A - B) \cap (A - C)$.

Observació. Anteriorment, s'ha resolt per operacions conjuntistes. També es resoldrà per taules de pertinença.

8.10.2. Les taules de pertinença

Per a cada operació conjuntista ($\cup$, $\cap$, $-$), en podem escriure la taula de pertinença associada. Per exemple, suposant dos operands A, B (conjunts), per a cada x són possibles quatre casos si considerem la pertinença als conjunts A, B.

Per a x qualsevol:

(x)	A	B
Cas 1	$x \in A$? (0-1)	$x \in B$? (0-1)
Cas 2	$x \in A$? (0-1)	$x \in B$? (0-1)
Cas 3	$x \in A$? (0-1)	$x \in B$? (0-1)
Cas 4	$x \in A$? (0-1)	$x \in B$? (0-1)

(x)	A	B
Cas 1	$x \notin A$	$x \notin B$
Cas 2	$x \notin A$	$x \in B$
Cas 3	$x \in A$	$x \notin B$
Cas 4	$x \in A$	$x \in B$

(x)	A	B
Cas 1	0	0
Cas 2	0	1
Cas 3	1	0
Cas 4	1	1

A la taula d'una fórmula F amb dos operands, finalment escriuríem a la columna de la fórmula 0 o 1 per a cada cas dels anteriors, indicant amb 0 que l'element $x \notin F$ (és a dir, no pertany al conjunt definit per la fórmula F) i indicant amb 1 que l'element $x \in F$ (és a dir, pertany al conjunt definit per la fórmula F).

(x)	A	B	F
Cas 1	0	0	0–1?
Cas 2	0	1	0–1?
Cas 3	1	0	0–1?
Cas 4	1	1	0–1?

Les taules de pertinença bàsiques. Són les corresponents a les operacions conjuntistes bàsiques.

A	B	$A\cup B$	$A\cap B$	$A-B$	$B-A$
0	0	0	0	0	0
0	1	1	0	0	1
1	0	1	0	1	0
1	1	1	1	0	0

$A\subseteq\Omega$	A	Ω	$\Omega-A$	A^c
$x\in A$	0	1	1	1
$x\notin A$	1	1	0	0

La taula de pertinença d'una fórmula conjuntista

A partir de la pertinença d'un x arbitrari a A o B (se'n consideren els quatre casos possibles), es van escrivint les taules de pertinença de les subfórmules fins a arribar a la fórmula final. A cada pas, s'utilitza una de les taules bàsiques. Caldrà analitzar les fórmules i veure quines en són les subfórmules, amb les quals anirem calculant la taula "incrementalment". Vegem-ne un exemple:

Exemple 8.52 Sigui A,B conjunts.

Obtenim la taula de pertinença de $(A\cup B)-(A\cap B)$.

Lletres: A,B

Subfórmules: $A\cup B$, $A\cap B$, $(A\cup B)-(A\cap B)$

Taula de pertinença:

A	B	$A\cup B$	$A\cap B$	$(A\cup B)-(A\cap B)$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

■

Exemple 8.53 Siguin A,B conjunts.

Obtenim la taula de pertinença de $(A-B)\cup(B-A)$.

Lletres: A,B

Subfórmules: $A-B$, $B-A$, $(A-B)\cup(B-A)$

A	B	$A-B$	$B-A$	$(A-B)\cup(B-A)$
0	0	0	0	0
0	1	0	1	1
1	0	1	0	1
1	1	0	0	0

■

Exemple 8.54 Siguin A,B,C conjunts.

Vegem quina seria la taula de pertinença de $A-(B-C)$.

Lletres: A,B,C (conjunts de base)

Subfórmules: $B-C$, $A-(B-C)$

A	B	C	$B-C$	$A-(B-C)$
0	0	0	0	0
0	0	1	0	0
0	1	0	1	0
1	0	0	0	1
0	1	1	0	0
1	0	1	0	1
1	1	0	1	0
1	1	1	0	1

■

PROBLEMA 8.23

Siguin A,B conjunts, subconjunts de Ω, respecte del qual es consideren complementaris. Obteniu la taula de pertinença de la fórmula conjuntista: $(A^c\cap B)\cup(A\cap B^c)$.

Solució

Lletres: A,B

Subfórmules: A^c, B^c, $A^c\cap B$, $A\cap B^c$, $(A^c\cap B)\cup(A\cap B^c)$

A	B	A^c	B^c	$A^c\cap B$	$A\cap B^c$	$(A^c\cap B)\cup(A\cap B^c)$
0	0	1	1	0	0	0
0	1	1	0	1	0	1
1	0	0	1	0	1	1
1	1	0	0	0	0	0

Igualtat per taules de pertinença. Les taules de pertinença poden ser útils per a demostrar la igualtat de conjunts definits per fórmules conjuntistes.

Es poden obtenir les taules de pertinença i comparar-les per a dos conjunts C, D. Si les taules coincideixen, els conjunts són iguals ja que, a la vista de la taula, resulta $x \in C \Leftrightarrow x \in D$. Aquí es pot aplicar perquè són fórmules conjuntistes amb unió, intersecció i diferència.

El mètode funciona suposant que, per a un x arbitrari, són possibles diversos casos considerant la pertinença a A i B. Suposem que volem demostrar $A \cup B = (A \cap B) \cup (A - B) \cup (B - A)$. A partir de les taules, resulta que, si coincideixen (englobant tots els casos possibles), aleshores:

$x \in A \cup B \Leftrightarrow x \in (A \cap B) \cup (A - B) \cup (B - A)$ i, per tant, els conjunts coincideixen. Vegem-ho a l'exemple següent:

Exemple 8.55 Demostreu per taules de pertinença que

$A \cup B = (A \cap B) \cup (A - B) \cup (B - A)$, on A, B són conjunts arbitraris.

Cal analitzar les fórmules, veient quines en són les subfórmules, amb les quals anirem calculant la taula "incrementalment". Les subfórmules de

$(A \cap B) \cup (A - B) \cup (B - A)$ són: A, B (operands), $(A \cap B), A - B, B - A$, $(A \cap B) \cup (A - B)$, $((A \cap B) \cup (A - B)) \cup (B - A)$, que hem escrit, per associativitat, com $(A \cap B) \cup (A - B) \cup (B - A)$, que ja és la fórmula final.

Podem demostrar la igualtat dels conjunts demostrant que les taules de pertinença coincideixen:

A	B	$A \cup B$	$A \cap B$	$A - B$	$B - A$	$(A \cap B) \cup (A - B)$	$(A \cap B) \cup (A - B) \cup (B - A)$
1	1	**1**	1	0	0	1	**1**
1	0	**1**	0	1	0	1	**1**
0	1	**1**	0	0	1	0	**1**
0	0	**0**	0	0	0	0	**0**

Les columnes corresponents coincideixen; per tant, els conjunts són iguals. ■

Desigualtat de conjunts donats per fórmules conjuntistes mitjançant taules de pertinença. Dos conjunts definits per fórmules conjuntistes són diferents si tenen taules de pertinença diferents (és a dir, no coincidents en alguna fila).

Les taules de pertinença no tenen cap utilitat per a altres situacions, com demostrar, per exemple, la igualtat $\{2n+1 | n \in \mathbb{Z}\} = \{2n-1 | n \in \mathbb{Z}\}$.

PROBLEMA 8.24

Demostreu per taules de pertinença la propietat associativa de la intersecció de conjunts.

Solució. Siguin A, B, C conjunts. La propietat associativa és $(A \cap B) \cap C = A \cap (B \cap C)$. Vegem que les taules de pertinença coincideixen.

A	B	C	$A\cap B$	$(A\cap B)\cap C$	$B\cap C$	$A\cap(B\cap C)$
1	1	1	1	**1**	1	**1**
1	1	0	1	**0**	0	**0**
1	0	1	0	**0**	0	**0**
1	0	0	0	**0**	0	**0**
0	1	1	0	**0**	1	**0**
0	1	0	0	**0**	0	**0**
0	0	1	0	**0**	0	**0**
0	0	0	0	**0**	0	**0**

PROBLEMA 8.25

Proveu per taules de pertinença la propietat distributiva de la unió respecte de la intersecció. Siguin A,B,C conjunts. La propietat esmentada és

$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$.

Solució

A	B	C	$B\cap C$	$A\cup(B\cap C)$	$A\cup B$	$A\cup C$	$(A\cup B)\cap(A\cup C)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

Les taules coincideixen; per tant, les fórmules són iguals. I anàlogament seria per a la distributivitat de $\cap$ respecte de $\cup$: $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

PROBLEMA 8.26

Demostreu per taules de pertinença les lleis de De Morgan per a dos conjunts.

Siguin A,B conjunts, subconjunts del conjunt Ω, respecte del qual es consideren els complementaris. Les dues fórmules de De Morgan són:

$(A\cup B)^c=A^c\cap B^c$

$(A\cap B)^c=A^c\cup B^c$

Solució. Veient que les taules de pertinença coincideixen. Vegem la primera de les fórmules:

A	B	$A\cup B$	$(A\cup B)^c$	A^c	B^c	$A^c\cap B^c$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

La demostració per taules per a l'altra fórmula de De Morgan es faria de manera similar.

PROBLEMA 8.27

Donats els conjunts A,B,C, estudieu, utilitzant les taules de pertinença si són iguals els conjunts $A-(B-C)$ i $(A-B)-C$. En cas contrari, identifiqueu alguna situació o cas que ho impedeixi (si així fos, utilitzeu aquesta informació per a trobar algun contraexemple).

Solució

Lletres: A,B,C (conjunts de base)

Subfórmules: $B-C, A-(B-C)$ (de $A-(B-C)$)

Subfórmules: $A-B$, $(A-B)-C$ (de $(A-B)-C$)

Calculem una taula conjunta per a ambdues fórmules.

A	B	C	$B-C$	$\boldsymbol{A-(B-C)}$	$A-B$	$\boldsymbol{(A-B)-C}$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	1	0	0	0
1	0	0	0	1	1	1
0 1	1 0	1 1	0 0	0 ▶ 1	0 1	0 ▶ 0
1	1	0	1	0	0	0
1	1	1	0	▶ 1	0	▶ 0

Observeu que les files 6 i 8 mostren les situacions que impedeixen la igualtat dels conjunts.

Fila 8. La fila 8 correspon a l'existència d'algun element a la intersecció dels tres conjunts, és a dir, $A\cap B\cap C\neq\emptyset$. Si $a\in A\cap B\cap C$, aleshores:

$a\in B, a\in C$, d'on $a\notin B-C$.

Essent $a\in A$, $a\notin B-C$, és $a\in A-(B-C)$.

Essent $a\in A, a\in B$, és $a\notin A-B$, d'on $a\notin (A-B)-C$.

Així, hi ha un element que és d'un conjunt i no de l'altre; per tant, són diferents.

En podem trobar contraexemples, exemples de noigualtat dels conjunts, escollint-los de manera que $A\cap B\cap C\neq\emptyset$. Per exemple, $A=\{a,1,2,3\}$, $B=\{a,1,4,6,9\}$,

$C = \{a,4,6,7\}$; aleshores, $A - (B - C) = A - \{1,9\} = \{a,2,3\}$ i $(A - B) - C = \{2,3\} - C = \{2,3\}$.

PROBLEMA 8.28

Siguin A, B conjunts, subconjunts de Ω. Proveu per taules de pertinença que $A - B = A \cap B^c$.

Solució. Vegem que les taules de les fórmules coincideixen.

Lletres: A, B

Subfórmules conjuntes: A, B, $A - B$, $A \cap B^c$

A	B	$\boldsymbol{A - B}$	B^c	$\boldsymbol{A \cap B^c}$
0	0	0	1	0
0	1	0	0	0
1	0	1	1	1
1	1	0	0	0

PROBLEMA 8.29

Siguin A, B, C conjunts. Proveu per taules de pertinença:

a) $(A \cup B) - C = (A - C) \cup (B - C)$
b) $(A \cap B) - C = (A - C) \cap (B - C)$

Solució

a) $(A \cup B) - C = (A - C) \cup (B - C)$

Lletres de la fórmula: A, B, C

Subfórmules de $(A \cup B) - C$: A, B, C, $A \cup B$, $(A \cup B) - C$

Subfórmules de $(A - C) \cup (B - C)$: A, B, C, $A - C$, $B - C$, $(A - C) \cup (B - C)$

Taula de pertinença conjunta:

A	B	C	$A \cup B$	$(A \cup B) - C$	$A - C$	$B - C$	$(A - C) \cup (B - C)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	1	0	1	1	0	1	1
1	0	0	1	1	1	0	1
0	1	1	1	0	0	0	0
1	0	1	1	0	0	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	0

Queda provat perquè les taules respectives coincideixen.

b) $(A \cap B) - C = (A - C) \cap (B - C)$

Es procedeix anàlogament al primer apartat.

PROBLEMA 8.30

Siguin A, B, C conjunts. Demostreu per taules de pertinença:

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

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

Solució. Les fórmules defineixen els mateixos conjunts (són “iguals”) si les taules de pertinença respectives coincideixen.

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

Lletres: A, B, C

Subfórmules de la fórmula de la dreta: $A - B$, $A - C$, $(A - B) \cap (A - C)$

Subfórmules de la fórmula de l'esquerra: $B \cup C$, $A - (B \cup C)$

Es pot fer una única taula conjunta o dues taules separades. Presentem una taula conjunta:

A	B	C	$A-B$	$A-C)$	$(A-B)\cap(A-C)$	$B\cup C$	$A-(B\cup C)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	0	1	0
1	0	0	1	1	1	0	1
0	1	1	0	0	0	1	0
1	0	1	1	0	0	1	0
1	1	0	0	1	0	1	0
1	1	1	0	0	0	1	0

Conclusió: S'observa que les taules coincideixen; per tant, les fórmules són iguals.

b) $A - (B \cap C) = (A - B) \cup (A - C)$. Es resol similarment a l'apartat anterior.

PROBLEMA 8.31

Siguin A, B conjunts. Demostreu per taules de pertinença algunes de les propietats següents, ja demostrades anteriorment.

a) $A - \emptyset = A$

b) $\emptyset - A = \emptyset$

c) $A - A = \emptyset$

d) $A - B = A - (A \cap B)$

e) $(A - B) \cap B = \emptyset$

f) $(A - B) \cap (B - A) = \emptyset$

Solució. Vegem, per exemple:

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

Obtenim la taula de pertinença:

A	B	$A-B$	$B-A$	$(A-B)\cap(B-A)$
0	0	0	0	0
0	1	0	1	0
1	0	1	0	0
1	1	0	0	0

El valor de pertinença de qualsevol x a $(A-B)\cap(B-A)$ és 0, és a dir, cap element pertany a $(A-B)\cap(B-A)$. Per tant, és el conjunt buit: $(A-B)\cap(B-A)=\emptyset$

I també: $A-\emptyset=A$

A	B	$A-\emptyset$
0	0	0
1	0	1

8.11. Producte cartesià

Una manera de combinar conjunts per obtenir-ne de nous és el producte cartesià.

Definició 8.11 (producte cartesià) *Donats dos conjunts A,B no buits, el producte cartesià en l'ordre $A\times B$ és el conjunt dels parells ordenats, és a dir:*

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

En cas que algun dels factors sigui buit, aleshores es defineix el producte cartesià com el conjunt buit.

Observació. Els parells són ordenats; per tant, l'ordre importa i $(a,b),(b,a)$ són diferents si $a\neq b$. Aquesta no és una situació nova: els punts (3,5), (5,3) són diferents.

La *igualtat* de parells ordenats es formalitza com

$(x,y)=(z,t)\leftrightarrow(x=z\wedge y=t)$

Aplicant-hi De Morgan, s'obté:

$((x,y)\neq(z,t)\leftrightarrow(x\neq z\vee y\neq t))$

Observació. Existeixen definicions més rigoroses d'un parell ordenat (consulteu la bibliografia).

Exemple 8.56 Si $A = \{a,b,c\}$, $B = \{0,1\}$, és:

$$\begin{aligned}
&A \times B = \{(a,0),(a,1),(b,0),(b,1),(c,0),(c,1)\}\\
&B \times A = \{(0,a),(0,b),(0,c),(1,a),(1,b),(1,c)\}\\
&B \times B = \{(0,0),(0,1),(1,0),(1,1)\}\\
&A \times \emptyset = \emptyset\\
&\emptyset \times A = \emptyset\\
&\emptyset \times \emptyset = \emptyset \blacksquare
\end{aligned}$$

Observació. Els parells són ordenats; per tant, l'ordre importa i $(a,b),(b,a)$ són diferents si $a \neq b$. Aquesta no és una situació nova: els punts (3,5), (5,3) són diferents.

La igualtat de dues parelles ordenades és "terme a terme" o "component a component":

$(a,b) = (c,d)$ si, i només si, $a = c$ i $b = d$. Per tant, $(a,1) \neq (1,a)$ si $a \neq 1$.

Es pot generalitzar a ternes ordenades, elements de

$A \times B \times C = \{(a,b,c) | a \in A, b \in B, c \in C\}$.

PROBLEMA 8.32

Si $A = \{a,b,c\}$*,* $B = \{0,1\}$*,* $C = \{\clubsuit,\heartsuit,\spadesuit\}$*, obteniu*

a) $A \times B \times C$

b) $A \times B \times A$

Solució

a) $A \times B \times C = \{$
$(a,0,\clubsuit),(a,0,\heartsuit),(a,0,\spadesuit),$
$(a,1,\clubsuit),(a,1,\heartsuit),(a,1,\spadesuit),$
$(b,0,\clubsuit),(b,0,\heartsuit),(b,0,\spadesuit),$
$(b,1,\clubsuit),(b,1,\heartsuit),(b,1,\spadesuit),$
$(c,0,\clubsuit),(c,0,\heartsuit),(c,0,\spadesuit),$
$(c,1,\clubsuit),(c,1,\heartsuit),(c,1,\spadesuit)$
$\}$

b) $A \times B \times A = \{$
$(a,0,a),(a,0,b),(a,0,c),$
$(a,1,a),(a,1,b),(a,1,c),$
$(b,0,a),(b,0,b),(b,0,c),$
$(b,1,a),(b,1,b),(b,1,c),$
$(c,0,a),(c,0,b),(c,0,c),$
$(c,1,a),(c,1,b),(c,1,c)$
$\}$

El concepte es pot generalitzar al conjunt de les n–ples ordenades (amb simplificació notacional):

$$A_1 \times \cdots \times A_m = \{(a_1, a_2, \cdots, a_m) | a_i \in A_i, \forall i = 1, \cdots, m\}.$$

Els conjunts poden ser el mateix, és a dir, $A = B$ o, més en general, $A_1 = \cdots = A_m = A$.

Teorema 8.9 (cardinal del producte cartesià) *Si els conjunts A, B són finits i no buits, aleshores $|A \times B| = |A||B|$ (i també $|A \times B| = |A||B| = |B \times A|$. En general, $|A_1 \times \cdots \times A_m| = |A_1| \cdots |A_m|$.*

Exemples 8.57 (addicionals de producte cartesià)

Exemple 1. *Producte cartesià i geometria:* $\mathbb{R}^2, \mathbb{R}^3, \mathbb{R}^n$ *com a producte cartesià*. Eventualment, els factors d'un producte cartesià poden repetir-se, com hem vist, com seria en el cas de $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$ i, en general, $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \mathbb{R}^n$ (n còpies). ■

Exemple 2. Podem considerar productes cartesians d'intervals. Per exemple, en el pla bidimensional, amb un sistema de coordenades cartesianes rectangulars, podem expressar rectangles de costats respectivament paral·lels als eixos de coordenades com a productes cartesians, subconjunts de $\mathbb{R}^2$:

$$[a_1, a_2] \times [b_1, b_2] = \{(x, y) \in \mathbb{R}^2 | \; a_1 \leq x \leq a_2, b_1 \leq y \leq b_2\}. \blacksquare$$

Exemple 3. Considerem el cub Q de costats de longitud 1, amb el vèrtex de coordenades mínimes situat a l'origen i amb els costats respectivament paral·lels als eixos de coordenades. Podem expressar el conjunt dels punts del cub com $Q = \{(x, y, z) | 0 \leq x \leq 1, 0 \leq y \leq 1, 0 \leq z \leq 1\}$ i, en termes de producte cartesià, com
$Q = [0, 1] \times [0, 1] \times [0, 1]$. ■

Exemple 4. Podem expressar el quadrat que té per vèrtexs oposats l'origen de coordenades del pla de coordenades $z = 0$ i el punt $(a, a, 0)$ mitjançant un producte cartesià: $[0, a] \times [0, a] \times \{0\}$, ja que és el conjunt de punts de la forma $(x, y, 0)$, amb $0 \leq x \leq a$, $0 \leq y \leq a$. O bé es pot expressar com a conjunt com $Q = \{(x, y, 0) | 0 \leq x \leq a, 0 \leq y \leq a\}$. ■

Exemple 5. El conjunt de les cadenes binàries de longitud $n \geq 1$ és el producte cartesià $\{0, 1\} \times \overset{n}{\overbrace{\cdots}} \times \{0, 1\}$. ■

Exemple 6. Un alumne fa un test de 20 preguntes, de 5 respostes cadascuna. Cada pregunta admet una única resposta, i se suposa que les contesta totes. De quantes maneres es pot fer? Es pot formalitzar la situació combinatòria en termes del producte cartesià. Considerem el conjunt de les possibles respostes $R = \{a, b, c, d, e\}$. Suposem que la resposta global al test consisteix a omplir una cadena lineal, de 20 caselles, en què la casella i–èsima contindrà la resposta a la i–èsima pregunta. El conjunt d'aquestes cadenes és el conjunt de les respostes possibles, i això és exactament el producte cartesià $T = R \times \overset{20}{\overbrace{\cdots}} \times R$; la resposta és $|T| = |R| \overset{20}{\overbrace{\cdots}} |R| = |R|^{20} = 5^{20}$. Si admetem que

pot no respondre's a una pregunta, podem modelitzar la situació ampliant les possibilitats a una nova resposta fictícia, "0", indicativa de "noresposta". Així, considerem $R' = \{a,b,c,d,e,0\}$, nou conjunt de respostes. A continuació, l'argumentació és la mateixa i resulta finalment 6^{20}. ■
linea Vegem diversos d'exemples en relació amb el cardinal d'un producte cartesià.

Exemples 8.58

Exemple 1. Calculeu, en funció de $|A|,|B|,|C|,|D|$, el cardinal de $D\times\mathscr{P}(\mathscr{P}(A)\times\mathscr{P}(B))\times C$ (on A,B,C,D són conjunts finits).

$|D\times\mathscr{P}(\mathscr{P}(A)\times\mathscr{P}(B))\times C| =$

$|D|\ |\mathscr{P}(\mathscr{P}(A)|\ |\mathscr{P}(B))|\ |C| =$

$|D|\ 2^{|\mathscr{P}(A)|}\ 2^{|B|}\ |C| =$

$|D|\ 2^{(2^{|A|})}\ 2^{|B|}\ |C|$

Hem fet servir que $|\mathscr{P}(X))| = 2^{|X|}$, amb X conjunt finit, i que

$|X\times Y\times Z| = |X||Y||Z|$, per a conjunts finits X, Y, Z. ■

Exemple 2. Quants subconjunts té $\{a,b,c\}\times\{0,1\}$?

$|\mathscr{P}(\{a,b,c\}\times\{0,1\})| = 2^{|\{a,b,c\}\times\{0,1\}|} = 2^{|\{a,b,c\}|\ |\{0,1\}|} = 2^{3\times 2} = 2^6$

Hem fet servir que $|\mathscr{P}(X))| = 2^{|X|}$, amb X conjunt finit. ■

Propietats addicionals. Per a A,B,C conjunts:

$(A\cup B)\times C = (A\times C)\cup(B\times C)$

$(A\cap B)\times C = (A\times C)\cap(B\times C)$

$(A-B)\times C = (A\times C)-(B\times C)$.

8.12. Problemes diversos de conjunts

PROBLEMA 8.33

Per a A,B,C conjunts:

$(A-B)\times C = (A\times C)-(B\times C)$

Solució. Provarem dues inclusions.

Subproblema 1. Vegem, en primer lloc, $(A-B)\times C\subseteq(A\times C)-(B\times C)$:
Sigui $(x,y)\in(A-B)\times C$.

Aleshores $x\in A-B$ i $y\in C$.

Per tant, $x\in A$, $x\notin B$ (afirmació [A]), $y\in C$.

D'una banda, doncs, $(x,y) \in A \times C$.

De l'altra banda, $(x,y) \notin B \times C$, ja que, si fos $(x,y) \in B \times C$, seria en particular $x \in B$, en contradicció amb l'afirmació [A] anterior (observi el lector que acabem de fer una demostració per reducció a l'absurd).

De les dues anteriors, en resulta $(x,y) \in (A \times C) - (B \times C)$,

que és el que havíem de provar:

$(x,y) \in (A \times C) - (B \times C)$.

Subproblema 2. Vegem que $(A \times C) - (B \times C) \subseteq (A - B) \times C$:

Sigui $(x,y) \in (A \times C) - (B \times C)$. Aleshores:

$(x,y) \in A \times C$ (afirmació [A]) i

$(x,y) \notin B \times C$ (afirmació [B])

Per [A], $x \in A$, $y \in C$.

Per [B], $x \notin B$ o $y \notin C$. Però, per [A], és $y \in C$ i, en conseqüència, ha de ser $x \notin B$.

Així, tenim: $x \in A$, $x \notin B$, $y \in C$, és a dir, $x \in A - B$, $y \in C$,

d'on $(x,y) \in (A - B) \times C$.

PROBLEMA 8.34

Per a A,B,C conjunts:

$(A \cap B) \times C = (A \times C) \cap (B \times C)$.

Solució. Resulta de la seqüència d'equivalències:

$(x,y) \in (A \cap B) \times C$,

que equival a $\quad x \in A \cap B \wedge y \in C$

que equival a $\quad (x \in A \wedge x \in B) \wedge y \in C$

que equival a $\quad x \in A \wedge x \in B \wedge (y \in C \wedge y \in C)$

que equival a $\quad (x \in A \wedge y \in C) \wedge (x \in B \wedge y \in C)$

que equival a $\quad (x,y) \in A \times C) \wedge (x,y) \in B \times C)$

que equival a $\quad (x,y) \in (A \times C) \cap (B \times C)$.

Així:

$(x,y) \in (A \cap B) \times C \Leftrightarrow (x,y) \in (A \times C) \cap (B \times C)$,

que estableix la igualtat dels dos conjunts.

PROBLEMA 8.35

Siguin A, B, C, D conjunts. Proveu:

$((A \cup B \subseteq C \cup D) \wedge (A \cap B = \emptyset) \wedge (C \subseteq A)) \Rightarrow (B \subseteq D)$

Solució. Escrivim separadament les diverses propietats de la hipòtesi amb l'objectiu de poder-nos-hi referir:

(1): $A \cup B \subseteq C \cup D$
(2): $A \cap B = \emptyset$
(3): $C \subseteq A$

Per a demostrar $B \subseteq D$, hem de provar:

$$x \in B \Rightarrow x \in D$$

(De fet: $\forall x (x \in B \Rightarrow x \in D)$).

En efecte:

Sigui $x \in B$.

Llavors, per (2), $x \notin A$.

Però, aleshores, per (3), $x \notin C$.

Ara bé, $x \in B \overset{sempre}{\Rightarrow} x \in A \cup B \overset{per(1)}{\Rightarrow} x \in C \cup D$.

Essent $x \notin C$, és $x \in D$.

PROBLEMA 8.36

Siguin A, B conjunts. Proveu:

$A - (A - B) = A \cap B$

Solució

Mètode 1. Per operacions conjuntistes:

$A - (A - B) =$

$= A \cap (A - B)^c$

$= A \cap (A \cap B^c)^c$

$= A \cap (A^c \cup B^{cc})$, per De Morgan per a conjunts,

$= A \cap (A^c \cup B)$ (doble complementari)

$= (A \cap A^c) \cup (A \cap B)$, per distributivitat de $\cap$ respecte de $\cup$,

$= \emptyset \cup (A \cap B)$

$= A \cap B$

Mètode 2. Per una seqüència d'equivalències, per a un x qualsevol:

$x \in A - (A - B)$

$x \in A \wedge x \notin A - B$

$x \in A \wedge \neg(x \in A - B)$

$x \in A \wedge \neg(x \in A \wedge \neg x \in B)$

$x \in A \wedge (\neg x \in A \vee \neg\neg x \in B)$ (De Morgan)

$x \in A \wedge (\neg x \in A \vee x \in B)$

$(x \in A \wedge \neg x \in A) \vee (x \in A \wedge x \in B)$

$\mathbb{F} \vee (x \in A \wedge x \in B)$

$(x \in A \wedge x \in B)$

$x \in A \cap B$.

Variant:

$A - (A - B) =$

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

$= \{x | x \in A \wedge \neg(x \in A - B)\}$

$= \{x | x \in A \wedge \neg(x \in A \wedge \neg x \in B)\}$

$= \{x | x \in A \wedge (\neg x \in A \vee \neg\neg x \in B)\}$

$= \{x | x \in A \wedge (\neg x \in A \vee x \in B)\}$

$= \{x | (x \in A \wedge \neg x \in A) \vee (x \in A \wedge x \in B)\}$

$= \{x | x \in \emptyset \vee (x \in A \wedge x \in B)\}$

$= \{x | (x \in A \wedge x \in B)\}$

$= A \cap B$.

Mètode 3. Per taules de pertinença:

A	B	$A-B$	$A-(A-B)$	$A \cap B$
0	0	0	0	0
0	1	0	0	0
1	0	1	0	0
1	1	0	1	1

La coincidència de les taules de pertinença permet afirmar la igualtat dels conjunts.

PROBLEMA 8.37

Siguin A, B conjunts. Proveu:

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

Solució

Mètode 1. Per operacions conjuntistes.

$(A-B)\cup B =$

$= (A\cap B^c)\cup B$

$= (A\cup B)\cap(B^c\cup B)$ (per distributivitat de $\cup$ respecte de $\cap$)

$= (A\cup B)\cap\Omega$

$= A\cup B.$

Mètode 2. Per una seqüència d'equivalències, per a x arbitrari:

$x\in(A-B)\cup B$

$x\in(A-B)\vee x\in B$

$(x\in A\wedge x\notin B)\vee x\in B$

$(x\in A\vee x\in B)\wedge(x\notin B\vee x\in B$ (per distributivitat de $\vee$ respecte de $\wedge$)

$(x\in A\vee x\in B)\wedge\mathbb{T}$

$x\in A\vee x\in B$

$x\in A\cup B.$

Mètode 3. Per taules de pertinença:

A	B	$A-B$	$(A-B)\cup B$	$A\cup B$
0	0	0	0	0
0	1	0	1	1
1	0	1	1	1
1	1	0	1	1

La coincidència de les taules de pertinença permet afirmar la igualtat dels conjunts.

PROBLEMA 8.38

Siguin A,B,C subconjunts de Ω. Proveu:

$[(A\cup B^c)-C]^c = (A^c\cup C)\cap(B\cup C).$

Solució. Demostrem-ho efectuant operacions conjuntistes.

$[(A\cup B^c)-C]^c =$

$= [(A\cup B^c)\cap C^c]^c$

$= (A\cup B^c)^c\cup(C^c)^c$ (per De Morgan per a conjunts)

$= (A \cup B^c)^c \cup C$ (per doble complementari)

$= (A^c \cap (B^c)^c) \cup C$ (per De Morgan per a conjunts)

$= (A^c \cap B) \cup C$ (per doble complementari)

$= (A^c \cup C) \cap (B \cup C)$ (per distributivitat de $\cup$ respecte de $\cap$).

Altres mètodes possibles. Per taules de pertinença, demostrant la doble inclusió, mitjançant una seqüència d'equivalències.

PROBLEMA 8.39

Considereu els conjunts:

$A = \{x \in \mathbb{R} | x^2 - 7x + 10 < 0\}$

$B = \{x \in \mathbb{R} | 2 < x < 5\}$

Proveu que $A = B$.

Solució. En primer lloc, resolem l'equació de segon grau $x^2 - 7x + 10 = 0$. Rutinàriament, resulta $x = \dfrac{7 \pm \sqrt{49-40}}{2} = \dfrac{7 \pm 3}{2}$. Per tant, les solucions són $2, 5$. La gràfica de $y = x^2 - 7x + 10$ és una paràbola que talla l'eix x en els punts $P_1 = (2,0)$ i $P_2 = (5,0)$. Atès el signe positiu del coeficient de x^2, és una paràbola oberta cap al semiplà de les y positives. Per tant, resulta:

$A = \{x \in \mathbb{R} | x^2 - 7x + 10 < 0\} = (2,5) = B$.

Hem fet servir una argumentació intuïtiva de base graficogeomètrica. Vegem-ne un argument formal. Convé tenir present que, del que hem vist, en resulta la factorització $(x-2)(x-5) = x^2 - 7x + 10$ i, per tant,

$x^2 - 7x + 10 < 0 \Leftrightarrow (x-2)(x-5) < 0$.

Veurem la igualtat $A = B$ demostrant les inclusions $B \subseteq A$ i $A \subseteq B$.

Subproblema 1 ($B \subseteq A$). Hem de provar que $x \in B \Rightarrow x \in A$:

Sigui $x \in B$. Llavors, $2 < x < 5$. De $2 < x$ resulta $x - 2 > 0$; de $x < 5$ resulta $x - 5 < 0$. Per tant, $(x-2)(x-5) < 0$. Equivalentment, $x^2 - 7x + 10 < 0$, d'on $x \in A$.

Recíprocament,

Subproblema 2 ($A \subseteq B$). Hem de provar que $x \in A \Rightarrow x \in B$:

Sigui $x \in A$. Aleshores $x^2 - 7x + 10 < 0$. Equivalentment, $(x-2)(x-5) < 0$. Per tant, $x - 2$ i $x - 5$ són de signes diferents. En principi, són possibles dos casos:

1. $x - 2 < 0$ i $x - 5 > 0$
2. $x - 2 > 0$ i $x - 5 < 0$

En el cas 1, $x < 2$ i $x > 5$, condicions incompatibles. Per tant, aquest cas no es pot donar. S'ha de satisfer el cas 2.

En el cas 2, resulta equivalentment a les condicions que $x > 2$ i $x < 5$, és a dir, $2 < x < 5$. Per tant, $x \in B$.

Variants: Reexpresseu $C = \{x \in \mathbb{R} | x^2 - 7x + 10 \geq 0\}$. És C el complementari de A en $\mathbb{R}$. Per tant, $C = \{x \in \mathbb{R} | x \leq 2 \vee x \geq 5$ (automatitzadament com a negació de la condició $2 < x \wedge x < 5$ per De Morgan). Per tant, $C = \{x \in \mathbb{R} | x \leq 2\} \cup \{x \in \mathbb{R} | x \geq 5\} = (-\infty, 2] \cup [5, +\infty)$.

Sigui $D = \{x \in \mathbb{R} | x^2 - 7x + 10 > 0\}$. És $D = \{x \in \mathbb{R} | (x-2)(x-5) > 0\}$. La condició $(x-2)(x-5) > 0$ equival que els dos factors són del mateix signe, de manera que, en principi, serien possibles dos casos, una disjunció:

1. $x - 2 > 0$ i $x - 5 > 0$ (o)
2. $x - 2 < 0$ i $x - 5 < 0$, és a dir, respectivament:

1. $x > 2$ i $x > 5$ o
2. $x < 2$ i $x < 5$,

És a dir, $(x > 2 \wedge x > 5) \vee (x < 2 \wedge x < 5)$.

Ara bé:

$(x > 2 \wedge x > 5) \Rightarrow x > 5$

$(x < 2 \wedge x < 5) \Rightarrow x < 2$, d'on

$((x > 2 \wedge x > 5) \vee (x < 2 \wedge x < 5)) \Rightarrow ((x < 2) \vee (x > 5))$.

Per tant, $D = (-\infty, 2) \cup (5, +\infty)$

També tenim:

$D = \{x \in \mathbb{R} | x^2 - 7x + 10 > 0\} = (-\infty, 2) \cup (5, +\infty)$

$D = \{x \in \mathbb{R} | x < 2 \vee x > 5\}$

PROBLEMA 8.40

Sigui $A = \{(x,y) \in \mathbb{R}^2 | xy = 2 \wedge x^2 + y^2 - 5 = 0\}$. *Descriviu el conjunt per extensió, explicitant-ne els seus elements.*

Solució. Es tracta de resoldre el sistema d'equacions anterior. Per la condició $xy = 2$, ja tenim que $x \neq 0$ (ja que, en cas contrari, seria $2 = xy = 0 \cdot y = 0$, absurd). Per tant, $y = \frac{2}{x}$. Substituïm a l'altra equació: $x^2 + (\dfrac{2}{x})^2 - 5 = 0$, d'on $x^4 - 5x^2 + 4 = 0$. Per a resoldre aquesta última equació, fem $w = x^2$, d'on cal resoldre $w^2 - 5w + 4 = 0$.

Les solucions són $w = \dfrac{5 \pm \sqrt{25-16}}{2}$. Per tant, $w = 4$ o $w = 1$. D'on $x = 2$ o $x = -2$ o $x = 1$ o $x = -1$. Tornant a la primera equació, les y corresponents respectivament a les x anteriors són $1, -1, 2, -2$. Les solucions són els punts $(2,1), (-2,-1), (1,2), (-1,-2)$. Aquests punts satisfan efectivament el sistema d'equacions.

Per tant,

$A = \{(x,y) \in \mathbb{R}^2 | xy = 2 \wedge x^2 + y^2 - 5 = 0\}$

$= \{(2,1), (-2,-1), (1,2), (-1,-2)\}$.

Des del punt de vista geomètric, són els punts de la intersecció de la circumferència $x^2 + y^2 - 5 = 0$, de centre l'origen i de radi $\sqrt{5}$, amb la hipèrbola $xy = 2$.

PROBLEMA 8.41

Descriviu els elements del conjunt

$A = \{(x,y) \in \mathbb{R}^2 | x(3-2x-y) = 0 \wedge y(3-2y-x) = 0\}$.

Solució. Els elements del conjunt són els que satisfan:

"$x = 0$ o $3-2x-y = 0$" i "$y = 0$ o $3-2y-x = 0$".

Pot ser difícil de manejar lògicament el conjunt de condicions. Sortosament la resolució es pot sistematitzar utilitzant equivalències lògiques:

$(x = 0 \vee 3-2x-y = 0) \wedge (y = 0 \vee 3-2y-x = 0)$

Ara bé:

$(x = 0 \vee 3-2x-y = 0) \wedge (y = 0 \vee 3-2y-x = 0)$ equival, per distributivitat de $\wedge$ respecte de $\vee$, a

$[x = 0 \wedge (y = 0 \vee 3-2y-x = 0)] \vee [(3-2x-y = 0) \wedge (y = 0 \vee 3-2y-x = 0)]$, que equival, per distributivitat de $\wedge$ respecte de $\vee$, a

$[(x = 0 \wedge y = 0) \vee (x = 0 \wedge 3-2y-x = 0)] \vee [(3-2x-y = 0 \wedge y = 0) \vee (3-2x-y = 0 \wedge 3-2y-x = 0)]$. És a dir:

$(x = 0 \wedge y = 0) \vee (x = 0 \wedge 3-2y-x = 0) \vee (3-2x-y = 0 \wedge y = 0) \vee (3-2x-y = 0 \wedge 3-2y-x = 0)$.

Més en general, aplicant les propietats de distributivitat, resulta:

$(a \vee b) \wedge (c \vee d) \equiv (a \wedge c) \vee (a \wedge d) \vee (b \wedge c) \vee (b \wedge d)$.

En efecte:

$(a \vee b) \wedge (c \vee d)$

$\equiv [(a \vee b) \wedge c] \vee [(a \vee b) \wedge d]$

$\equiv [(a \wedge c) \vee (b \wedge c)] \vee [(a \wedge d) \vee (b \wedge d)]$

$\equiv (a \wedge c) \vee (b \wedge c) \vee (a \wedge d) \vee (b \wedge d)$ (associativitat).

Cada operand de la disjunció anterior aporta solucions del sistema, elements (punts) al conjunt:

$(x = 0 \wedge y = 0)$: $P_1 = (0,0)$,

$(x = 0 \wedge 3 - 2y - x = 0)$: $P_2 = (0,3/2)$,

$(3 - 2x - y = 0 \wedge y = 0)$: $P_3 = (3/2,0)$,

De $(3 - 2x - y = 0 \wedge 3 - 2y - x = 0)$ resulta $x = y$. Ara tornem a les equacions originals:

substituint $y = x$ a la primera s'obté $3x(1-x) = 0$, d'on $x = 0$ o $x = 1$; si $x = 0$, és $y = x = 0$ i resultaria el punt P_1. En el cas $x = 1$, resulta $y = x = 1$, d'on, finalment, $P_4 = (1,1)$.

Es pot comprovar que satisfan el sistema, simplement per substitució.

Així, $A = \{(0,0),(3/2,0),(0,3/2),(1,1)\}$.

PROBLEMA 8.42

Siguin A,B conjunts. Proveu que $B \subseteq A \Rightarrow B = A - (A - B)$.

Solució

Mètode 1. Per operacions conjuntistes.

Convé tenir en compte que la hipòtesi es pot expressar equivalentment com

$A \cap B = B$ i també $A \cup B = A$.

$A - (A - B) =$

$= A \cap (A - B)^c$

$= A \cap (A \cap B^c)^c$

$= A \cap (A^c \cup B^{cc})$, per De Morgan (conjunts)

$= A \cap (A^c \cup B)$ (per doble complementació)

$= (A \cap A^c) \cup (A \cap B)$, (per distributivitat de $\cap$ respecte de $\cup$)

$= \emptyset \cup (A \cap B)$

$= A \cap B$

$= B$, per la hipòtesi ($A \cap B = B$).

Observem com aquí s'aplica la hipòtesi al final de l'argumentació.

Mètode 2. Per una seqüència d'equivalències que estableix la doble inclusió, i que segueix en paral·lel la seqüència del mètode 1. Per a x arbitrari:

$x \in A - (A - B)$, equivalent a

$x \in A \wedge x \notin A - B$, equivalent a

$x \in A \wedge (x \notin A \vee x \in B)$, equivalent a

$(x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B)$, equivalent a

$\mathbf{0} \vee (x \in A \wedge x \in B)$, equivalent a

$x \in A \wedge x \in B$, equivalent a

$x \in A \cap B$

Tenim $x \in A \cap B \Rightarrow x \in B$ sempre (equivalentment, $A \cap B \subseteq B$). Ara bé, per la hipòtesi, tenim l'equivalència $x \in A \cap B \Leftrightarrow x \in B$ i, en conseqüència, l'argumentació anterior pot prosseguir:

...

$x \in A \cap B$, equivalent a

$x \in B$.

Això prova la tesi que $\forall x(x \in A - (A - B) \leftrightarrow x \in B)$ és cert.

Globalment, $\forall y(y \in B \rightarrow y \in A) \rightarrow \forall x(x \in A - (A - B) \leftrightarrow x \in B)$.

PROBLEMA 8.43

Descriviu els elements del conjunt:

$A = \{(x,y) \in \mathbb{R}^2 | (x-2)^2 + y^2 = 8 \wedge y = x\}$.

Solució. És la intersecció de la recta $y = x$ (bisectriu del primer i el tercer quadrants) i la circumferència de centre $(2,0)$ i radi $\sqrt{8}$. També es podria escriure

$A = \{(x,y) \in \mathbb{R}^2 | (x-2)^2 + y^2 = 8\} \cap \{(x,y) \in \mathbb{R}^2 | y = x\}$.

Substituïm $y = x$ a la primera equació:

$(x-2)^2 + x^2 = 8$

$x^2 - 2x - 2 = 0$

$x = 1 \pm \sqrt{3}$

És a dir, les solucions són $x_1 = 1 + \sqrt{3}$ o $x_2 = 1 - \sqrt{3}$. Tornant a la segona equació, resulta:

$A = \{(1+\sqrt{3}, 1+\sqrt{3}), (1-\sqrt{3}, 1-\sqrt{3})\}$

PROBLEMA 8.44

Escriviu els conjunts de punts del pla bidimensional descrits per:

a) Els punts del primer quadrant sense els eixos de coordenades (del quadrant).

b) Els punts del primer quadrant amb els eixos de coordenades (del quadrant).

c) *Els punts del tercer quadrant amb els eixos (del quadrant).*

d) *Els punts del tercer i el quart quadrants amb els eixos de coordenades (dels quadrants).*

e) *Els punts del segon i el quart quadrants amb els eixos de coordenades (dels quadrants).*

f) *La recta que passa pel punt* $(0,c)$ *i és perpendicular a l'eix d'ordenades.*

g) *Els punts del segon quadrant amb els eixos de coordenades (del quadrant).*

h) *Els punts de semiplà de les y no negatives.*

i) *Els punts dels quadrants segon i tercer sense els eixos de coordenades (dels quadrants).*

j) *El pla excepte els eixos de coordenades.*

k) *El pla sense l'eix Ox.*

l) *El pla sense la bisectriu del primer-tercer quadrant.*

m) *El semicercle al primer i al segon quadrants corresponent a la circumferència* $x^2 + y^2 = 5$.

Solució

a) Els punts del primer quadrant sense els eixos de coordenades

$\{(x,y) \in \mathbb{R}^2 | x > 0, y > 0\} = \{(x,y) \in \mathbb{R}^2 | x > 0 \wedge y > 0\}$.

b) Els punts del primer quadrant amb els eixos de coordenades

$\{(x,y) \in \mathbb{R}^2 | x \geq 0 \wedge y \geq 0\}$.

c) Els punts del tercer quadrant amb els eixos

$\{(x,y) \in \mathbb{R}^2 | x \leq 0 \wedge y \leq 0\}$.

d) Els punts del tercer i el quart quadrants amb els eixos de coordenades

$\{(x,y) \in \mathbb{R}^2 | y \leq 0\}$.

e) Els punts del segon i el quart quadrants amb els eixos de coordenades

$\{(x,y) \in \mathbb{R}^2 | (x \leq 0 \wedge y \geq 0) \vee (x \geq 0 \wedge y \leq 0)\}$.

f) La recta que passa pel punt $(0,c)$ i és perpendicular a l'eix d'ordenades

$\{(x,c) \in \mathbb{R}^2 | x \in \mathbb{R}\}$.

g) Els punts del segon quadrant amb els eixos de coordenades

$\{(x,y) \in \mathbb{R}^2 | x \leq 0 \wedge y \geq 0\}$.

h) Els punts de semiplà de les y no negatives

$\{(x,y) \in \mathbb{R}^2 | y \geq 0\}$.

i) Els punts dels quadrants segon i tercer sense els eixos de coordenades

$\{(x,y) \in \mathbb{R}^2 | x < 0 \wedge y \neq 0\}$.

j) El pla excepte els eixos de coordenades

$\{(x,y) \in \mathbb{R}^2 | x \neq 0 \wedge y \neq 0\}$

k) El pla sense l'eix Ox

$\{(x,y) \in \mathbb{R}^2 | y \neq 0\}$.

l) El pla sense la bisectriu del primer-tercer quadrant

$\{(x,y) \in \mathbb{R}^2 | y \neq x\}$.

m) El semicercle al primer i al segon quadrants corresponent a la circumferència $x^2 + y^2 = 5$

$\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 5 \wedge y \geq 0\}$.

PROBLEMA 8.45

Descriviu els elements del conjunt:

$A = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 5 \wedge x = 0\}$.

Solució. També és $A = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 5\} \cap \{(x,y) \in \mathbb{R}^2 | x = 0\}$.

És la intersecció de la circumferència $x^2 + y^2 = 5$, de centre $(0,0)$ i radi $\sqrt{5}$, amb l'eix Oy.

Posant $x = 0$ a la primera equació, obtenim $y^2 = 5$, d'on $y = \sqrt{5}$ o $y = -\sqrt{5}$. Per tant:

$A = \{(0, \sqrt{5}), (0, -\sqrt{5})\}$.

PROBLEMA 8.46

Descriviu els elements del conjunt:

$A = \{(x,y) \in \mathbb{R}^2 | (x-2)^2 + y^2 = 9 \wedge (x = 0 \vee y = 0)\}$.

Solució. El conjunt de punts que satisfan la condició $(x-2)^2 + y^2 = 9 \wedge (x = 0 \vee y = 0)$ és el dels que satisfan la condició equivalent $((x-2)^2 + y^2 = 9 \wedge x = 0) \vee ((x-2)^2 + y^2 = 9 \wedge y = 0)$, intersecció de la circumferència $(x-2)^2 + y^2 = 9$, de centre $(2,0)$ i radi 3, amb els eixos de coordenades, interseccions que calculem separadament:

$A = \{(x,y) \in \mathbb{R}^2 | (x-2)^2 + y^2 = 9 \wedge x = 0\} \cup \{(x,y) \in \mathbb{R}^2 | (x-2)^2 + y^2 = 9 \wedge y = 0)\}$

Posant $x = 0$ a l'equació $(x-2)^2 + y^2 = 9$, resulta $y = \pm\sqrt{5}$. Per tant, les solucions són $(0, \sqrt{5})$, $(0, -\sqrt{5})$.

Posant $y = 0$ a l'equació $(x-2)^2 + y^2 = 9$, resulta $x = 5$ o $x = -1$. Per tant, les solucions són $(5,0)$, $(0,-1)$. Així:

$A = \{(0, \sqrt{5}), (0, -\sqrt{5}), (5,0), (0,-1)\}$.

PROBLEMA 8.47

Siguin A, B conjunts, subconjunts de Ω. Proveu: $A - B = B - A \Leftrightarrow A = B$.

Solució. Cal provar dues implicacions.

Primera implicació. La implicació $A = B \Rightarrow A - B = B - A$ és una obvietat: $A - B = A - A = B - A$, aplicant la hipòtesi dues vegades.

Segona implicació. Vegem la implicació $A - B = B - A \Rightarrow A = B$, que demostrem per manipulació conjuntista:

$A = A \cap \Omega =$

$= A \cap (B \cup B^c)$

$= (A \cap B) \cup (A \cap B^c)$, per distributivitat de $\cap$ respecte de $\cup$,

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

$= (A \cap B) \cup (B - A)$, per hipòtesi,

$= (A \cap B) \cup (B \cap A^c)$

$= (A \cap B) \cup (A^c \cap B)$

$= (A \cup A^c) \cap B$, per distributivitat de $\cap$ respecte de $\cup$,

$= \Omega \cap B$

$= B$.

Altres mètodes de demostració, per a la segona implicació: $(A - B = B - A \Rightarrow A = B)$

Per reducció a l'absurd. Partim de la negació de la implicació, és a dir, de$A - B = B - A$ i $A \neq B$. Vegem que s'arriba a una contradicció.

De $A \neq B$, existeix x tal que $x \in A$ i $x \notin B$, o bé existeix y tal que $y \in A$ i $y \notin B$ (poden ser totes dues). Considerem el primer cas; per al segon, procediríem anàlogament o, fins i tot, no caldria fer res per raons de simetria.

En efecte, si $x \in A$ i $x \notin B$, aleshores és $x \in A - B$. Aplicant la hipòtesi, és $x \in B - A$, d'on $x \in B$ i $x \notin A$, contradicció. Per tant, $A - B = B - A \Rightarrow A = B$.

Podem adaptar la idea anterior per a donar un argument *pel contrarecíproc*: $A \neq B \Rightarrow A - B \neq B - A$. En efecte, suposem que existeix x tal que $x \in A$ i $x \notin B$ (anàlogament per a l'altra possibilitat). Aleshores $x \in A - B$. Per tant, $x \notin B$ i, en conseqüència, $x \notin B - A$, per definició de diferència de conjunts. Per tant, $A - B \neq B - A$.

PROBLEMA 8.48

Siguin A, B conjunts, subconjunts de Ω. Proveu:

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

Solució. Mètode: per manipulació conjuntista. Idea: no resulta obvi com abordar el problema a partir de A, és a dir, $A = ...?...$. Serà millor partir de l'expressió del membre de la dreta, on trobem possibilitats de manipulació:

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

$= (A \cap B) \cup (A \cap B^c)$

$= A \cap (B \cup B^c)$, per distributivitat de $\cap$ respecte de $\cup$,

$= A \cap \Omega$

$= A$

Observi el lector que hem aplicat la distributivitat "en sentit contrari a l'habitual".

Altres mètodes. Per taules de pertinença, per seqüència d'equivalències, per doble inclusió.

PROBLEMA 8.49

Siguin A, B conjunts, subconjunts de Ω. Proveu: $(A \cap B) \cap (A - B) = \emptyset$.

Solució

Mètode 1. Per reducció a l'absurd. Suposem $(A \cap B) \cap (A - B) \neq \emptyset$. Aleshores existeix algun element $x \in (A \cap B) \cap (A - B)$, d'on $x \in A \cap B$ i $x \in A - B$. De $x \in A \cap B$ resulta, en particular, $x \in B$. De $x \in A - B$ se'n deriva $x \notin B$. Per tant, hem arribat a la contradicció $x \in B$ i $x \notin B$. En conseqüència, $(A \cap B) \cap (A - B) = \emptyset$.

Mètode 2. Alternativament, ho provem *per operacions conjuntistes*. Idea: no resulta obvi com abordar el problema a partir de $\emptyset$, és a dir, $\emptyset = ...?...$. Serà millor partir de l'expressió del membre de la dreta, on trobem possibilitats de manipulació:

$(A \cap B) \cap (A - B) =$

$= (A \cap B) \cap (A \cap B^c) =$

$= (A \cap A) \cap (B \cap B^c)$

$= A \cap \emptyset$

$= \emptyset.$

Altres mètodes. També es podria demostrar per taules de pertinença, doble inclusió i seqüència d'equivalències.

PROBLEMA 8.50

Siguin A, B conjunts. Demostreu que

$\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B).$

Solució. Vegem les dues inclusions corresponents a la igualtat de conjunts.

$\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$

$\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$

$\triangleright$ $\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$?

Sigui $C \in \mathscr{P}(A \cap B)$. Aleshores $C \subseteq A \cap B$. Atès que $A \cap B \subseteq A$ i $A \cap B \subseteq B$, resulta $C \subseteq A$ i $C \subseteq B$. Per tant, $C \in \mathscr{P}(A)$ i $C \in \mathscr{P}(B)$, d'on $C \in \mathscr{P}(A) \cap \mathscr{P}(B)$.

$\triangleright$ $\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$?

Sigui $D \in \mathscr{P}(A) \cap \mathscr{P}(B)$. Aleshores $D \in \mathscr{P}(A)$ i $D \in \mathscr{P}(B)$. Equivalentment, $D \subseteq A$ i $D \subseteq B$. Per tant, $D \subseteq A \cap B$. Finalment, $D \in \mathscr{P}(A \cap B)$.

PROBLEMA 8.51

Sigui A un conjunt. Proveu $A - (A - A) = A$.

Solució

Mètode 1. Essent $A - A = \emptyset$, podem escriure $A - (A - A) = A - \emptyset = A$.

Mètode 2. Considerant $A \subseteq \Omega$, per manipulació conjuntista:

$A - (A - A) = A \cap (A - A)^c = A \cap (A \cap A^c)^c = A \cap (A^c \cup A^{cc}) = A \cap (A^c \cup A) = A \cap \Omega = A$

Mètode 3. Considerem la seqüència d'equivalències:

$x \in A - (A - A)$, equivalent a

$x \in A \wedge x \notin (A - A)$, equivalent a

$x \in A \wedge (x \notin A \vee x \in A)$, equivalent a

$(x \in A \wedge x \notin A) \vee (x \in A \wedge x \in A)$, equivalent a

$\mathbb{F} \vee (x \in A \wedge x \in A)$, equivalent a

$x \in A \wedge x \in A$, equivalent a

$x \in A$.

També es podria provar per taules de pertinença.

PROBLEMA 8.52

Sigui A un conjunt. Proveu $(A - A) - A = \emptyset$.

Solució

Mètode 1. Essent $A - A = \emptyset$, podem escriure $(A - A) - A = \emptyset - A = \emptyset$.

Mètode 2. Per operacions conjuntistes: $(A-A)-A=(A\cap A^c)\cap A^c=A\cap A^c=\emptyset$.

Mètode 3. Per reducció a l'absurd. Suposem $(A-A)-A\neq\emptyset$ i sigui, per tant, $x\in(A-A)-A$. Aleshores $x\in A-A$ i $x\notin A$. Ara bé, de $x\in A-A$ resulta $x\in A$ (i també $x\notin A$). Per tant, hem arribat a la contradicció: $x\in A$ i $x\notin A$.

També per taules de pertinença i per seqüència d'equivalències.

PROBLEMA 8.53

Expresseu com a interval o reunió d'intervals $A=\{x\in\mathbb{R}||3x-1|<2\}$.

Solució. Si $3x-1\geq 0$, és $|3x-1|=3x-1$ i, per tant, la condició definitòria és $0\leq 3x-1<2$, d'on $1\leq 3x<3$ Així, $\frac{1}{3}\leq x<1$.

Si $3x-1<0$, és $|3x-1|=-(3x-1)$ i, per tant, la condició definitòria és $-(3x-1)<2)$, d'on $-2<3x-1<0$. D'on $-1<3x<1$. Per tant, $-\frac{1}{3}<x<\frac{1}{3}$.

Així:

$$\begin{aligned}
A&=\{x\in\mathbb{R}||3x-1|<2\}\\
&=\{x\in\mathbb{R}|3x-1\geq 0\wedge|3x-1|<2\}\cup\{x\in\mathbb{R}|3x-1<0\wedge|3x-1|<2\}\\
&=\{x\in\mathbb{R}|\tfrac{1}{3}\leq x<1\}\cup\{x\in\mathbb{R}|-\tfrac{1}{3}<x<\tfrac{1}{3}\}\\
&=[\tfrac{1}{3},1)\cup(-\tfrac{1}{3},\tfrac{1}{3})\\
&=(-\tfrac{1}{3},1).
\end{aligned}$$

Per tant, alternativament, $A=\{x\in\mathbb{R}|-\frac{1}{3}<x<1\}$.

PROBLEMA 8.54

Doneu una descripció alternativa del conjunt $A=\{(x,y)\in\mathbb{R}^2|xy=0\}$.

Solució. Observem que $xy=0\Rightarrow(x=0\vee y=0)$. Per tant,

$$\begin{aligned}
A&=\{(x,y)\in\mathbb{R}^2|x=0\vee y=0\}\\
&=\{(0,y)|y\in\mathbb{R}\}\cup\{(x,0)|x\in\mathbb{R}\}.
\end{aligned}$$

Està format pels dos eixos de coordenades.

PROBLEMA 8.55

Descriviu per extensió el conjunt $A=\{(x,y)\in\mathbb{R}^2|(x+y)(xy+1)=0\}$.

Solució. Analitzem la condició definitòria. És $(x+y)(xy+1)=0\Rightarrow(x+y=0\vee xy+1=0)$.

De la primera condició, $y = -x$. Substituint a la segona, $-x^2 + 1 = 0$, d'on $x^2 = 1$, és a dir, $x = 1$ o $x = -1$. Tornant a la condició $y = -x$, en resulten, respectivament, els valors $y = -1$ o $y = 1$. Per tant, $A = \{(1,-1),(-1,1)\}$.

PROBLEMA 8.56

Siguin W, S conjunts. Proveu:

$\forall x(x \in W \to x \notin S) \Leftrightarrow W \cap S = \emptyset$.

Solució. Podem demostrar dues implicacions o bé fer una prova directa de l'equivalència.

▷ Hem de demostrar dues implicacions:

Primera implicació. $\forall x(x \in W \to x \notin S) \Rightarrow W \cap S = \emptyset$

Mètode de demostració pel contrarecíproc. Cada afirmació implica la de sota (en alguns casos, són equivalents):

Suposem $W \cap S \neq \emptyset$. Aleshores:

$\exists a(a \in W \cap S)$

$\exists a(a \in W \wedge a \in S)$

$\exists a(a \in W \wedge \neg\neg a \in S)$ (per doble negació)

$\exists a(a \in W \wedge \neg a \notin S)$

$\exists a \neg(a \in W \to a \notin S)$ (per negació del condicional)

$\neg\forall a(a \in W \to a \notin S)$ (per negació del quantificador universal $\forall$).

Observació: Amb una variant expositiva, podem produir una demostració per reducció a l'absurd.

Segona implicació. $W \cap S = \emptyset \Rightarrow \forall x(x \in W \to x \notin S)$

Mètode de demostració: per reducció a l'absurd. Suposem falsa la implicació i certa la seva negació. Recordem que la negació de $A \Rightarrow B$ és (equivalent a) "A i no B" ($\neg(A \to B) \equiv A \wedge \neg B$). Cada afirmació implica la de sota (en alguns casos, són equivalents):

Suposem cert $W \cap S = \emptyset$ i $\neg\forall x(x \in W \to x \notin S)$. Escrivim una seqüència de fórmules equivalents a la segona:

$\neg\forall x(x \in W \to x \notin S)$

$\exists x \neg(x \in W \to x \notin S)$

$\exists x(x \in W \wedge \neg x \notin S)$

$\exists x(x \in W \wedge \neg\neg x \in S)$

$\exists x(x \in W x \in S)$

$\exists x(x \in W \cap S)$

$W \cap S \neq \emptyset$, contradicció.

Per tant, la implicació és certa.

Observació: Canvis mínims en l'exposició anterior produeixen una demostració pel contrarecíproc: $\neg\forall x(x \in W \to x \notin S) \Rightarrow W \cap S \neq \emptyset$.

▷ *Prova directa de l'equivalència*. Seqüència d'equivalències:

$\forall x(x \in W \to x \notin S)$

$\neg\neg\forall x(x \in W \to x \notin S)$ (per doble negació)

$\neg\exists x\neg(x \in W \to x \notin S)$ (per negació de $\forall$)

$\neg\exists x(x \in W \wedge \neg x \notin S)$ (per negació del condicional)

$\neg\exists x(x \in W \wedge x \in S)$ (per doble negació)

$\neg\exists x(x \in W \cap S)$ (per definició de la intersecció de dos conjunts)

$\neg(W \cap S \neq \emptyset)$

$W \cap S = \emptyset$.

Observeu que, pel contrarecíproc aplicat a $x \in W \to x \notin S$, resulta una nova afirmació equivalent a les anteriors: $\forall x(x \in S \to x \notin W)$. En efecte, per a un x arbitrari (però fix) $x \in W \to x \notin S$ equival, pel contrarecíproc, a $\neg x \notin S \to x \notin W$, és a dir, $x \in S \to x \notin W$; per generalització s'obté l'afirmació.

Per tant, són equivalents:

$\forall x(x \in W \to x \notin S)$

$\forall x(x \in S \to x \notin W)$

$W \cap S = \emptyset$

De fet, també $W \cap S = \emptyset$ és equivalent a

$\forall x(x \in W \to x \notin S) \wedge \forall x(x \in S \to x \notin W)$.

PROBLEMA 8.57

Siguin A, B, C subconjunts de Ω. Proveu que $(A \cap B \cap C) \cap [(A - B) - C] = \emptyset$.

Solució

Mètode 1. Per manipulació conjuntista:

$(A \cap B \cap C) \cap [(A - B) - C] = (A \cap B \cap C) \cap [(A - B) \cap C^c] =$

$= (C \cap C^C) \cap (A \cap B \cap (A - B)) = \emptyset \cap (A \cap B \cap (A - B)) = \emptyset$.

Mètode 2. També *per reducció a l'absurd*:

Suposem $(A\cap B\cap C)\cap[(A-B)-C]\neq\emptyset$. Sigui $x\in(A\cap B\cap C)\cap[(A-B)-C]$. En particular, $x\in C$ i $x\in(A-B)-C$; d'aquesta última resulta que $x\notin C$. De manera que hem arribat a: $x\in C$ i $x\notin C$, contradicció. Per tant:

$(A\cap B\cap C)\cap[(A-B)-C]=\emptyset$.

PROBLEMA 8.58

Siguin A,B,C conjunts. Proveu que

si $a\in A\cap B\cap C$, aleshores $a\in A-(B-C)$ i $a\notin(A-B)-C$.

Solució. Vegem separadament

$a\in A\cap B\cap C\Rightarrow a\in A-(B-C)$ i $a\in A\cap B\cap C\Rightarrow a\notin(A-B)-C$.

a) $a\in A\cap B\cap C\Rightarrow a\in A-(B-C)$?

   Sigui $a\in A\cap B\cap C$. Aleshores $a\in A\wedge a\in B\wedge a\in C$. De $a\in B\wedge a\in C$ en deduïm que $a\notin B-C$. Juntament amb $a\in A$, obtenim $a\in A-(B-C)$.

b) $a\in A\cap B\cap C\Rightarrow a\notin(A-B)-C$?

   Per contrarecíproc: si $a\in(A-B)-C$, en particular $a\notin C$. Però, aleshores, $a\notin a\in A\cap B\cap C$.

   Directament, si $a\in A\cap B\cap C$, aleshores $a\in A\wedge a\in B$, d'on $a\notin A-B$. En conseqüència, $a\notin(A-B)-C$.

   Exposició alternativa:

   $a\in A\cap B\cap C\Rightarrow a\in A\wedge a\in B\Rightarrow a\notin A-B\Rightarrow a\notin(A-B)-C$.

Observacions: Una conclusió posterior seria que $a\in(A-(B-C))-((A-B)-C)$. I també resulta que $A-(B-C)\neq(A-B)-C$.

8.13. Qüestions conceptuals

Recordem algunes notacions

$|A|$ denota el cardinal de A. Tots els conjunts dels quals es considera el cardinal són finits (o el buit).

Universal(s): U,Ω, indistintament.

Complementari del conjunt A respecte de U: $A^c, U-A, \Omega-A, \overline{A}, U\setminus A, \Omega\setminus A$ (on $A\subseteq U$).

El conjunt de les parts de A es denota per $\mathscr{P}(A)$. Recordeu: $\mathscr{P}(A)=\{B|B\subseteq A\}$.

$\mathscr{P}_k(A)$ és el conjunt dels subconjunts de A que són de cardinal k. És a dir, $\mathscr{P}_k(A) = \{B : B \subseteq A \wedge |B| = k\} = \{B \in \mathscr{P}(A) | |B| = k\}$.

Recordeu que $|\mathscr{P}(A)| = 2^{|A|}$ i $|\mathscr{P}_k(A)| = \binom{|A|}{k}$.

64 Cert o fals?

a) $\{\emptyset\} = \emptyset$
b) $\emptyset \in \{\emptyset\}$
c) $\emptyset \subseteq \{\emptyset\}$
d) $|\{\emptyset\}| = 0$
e) $|\{\emptyset\}| = 1$
f) $\emptyset \subseteq \mathscr{P}(\{\emptyset\})$
g) $\emptyset \in \mathscr{P}(\{\emptyset\})$
h) $\{\emptyset\} \in \mathscr{P}(\{\emptyset\})$
i) $\{\{\emptyset\}\} \in \mathscr{P}(\{\emptyset\})$
j) $\{\{\emptyset\}\} \subseteq \mathscr{P}(\{\emptyset\})$
k) $\mathscr{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

Ajut: En alguns casos, pot ser útil obtenir el conjunt de les parts separant per cardinals: subconjunts de 0 elements, subconjunts d'1 element, etc, corresponent a:

$$\mathscr{P}(A) = \mathscr{P}_0(A) \cup \mathscr{P}_1(A) \cup \mathscr{P}_2(A) \cup \cdots \cup \mathscr{P}_k(A) \cup \cdots \cup \mathscr{P}_{|A|}(A) = \bigcup_{k=0}^{|A|} \mathscr{P}_k(A).$$

64* *Resposta:*

a) Fals.
b) Cert.
c) Cert.
d) Fals.
e) Cert.
f) Cert, propietat general.
g) Cert, propietat general, ja que $\emptyset \subseteq \{\emptyset\}$.
h) Cert, sempre $A \in \mathscr{P}(A)$.
i) Fals.
j) Cert.
k) Cert.

65 Escriviu els elements del conjunt:

$$A = \{1, 2, 4, \{3\}, \{\{3\}\}, \emptyset, \{\emptyset\}, \{\{\{\emptyset\}\}\}\}$$

65* *Resposta:*Hi ha 8 elements:

$$1, 2, 4, \{3\}, \{\{3\}\}, \emptyset, \{\emptyset\}, \{\{\{\emptyset\}\}\}$$

66 Indiqueu quines afirmacions són certes:

a) $1 \in \{1,2,3\}$
b) $\{1\} \in \{1,2,3\}$
c) $\{1\} \subseteq \{1,2,3\}$
d) $\emptyset \in \{1,2,3\}$
e) $\emptyset \subseteq \{1,2,3\}$
f) $\{1,2,3\} \neq \emptyset$
g) $\{1,2,3\} \neq \{\emptyset\}$

66* *Resposta:*

a) Cert.
b) Fals.
c) Cert.
d) Fals.
e) Cert, sempre.
f) Cert.
g) Cert.

67 Si $A = \{1,2,\{3,4\},5\}$, indiqueu quines afirmacions són certes:

a) $3 \notin A$
b) $\emptyset \notin A$
c) $\emptyset \subseteq A$
d) $\{3,4\} \in A$
e) $\{\{3,4\}\} \subseteq A$
f) $\{\{\{3,4\}\}\} \subseteq A$

67* *Resposta:*

a) Cert.
b) Cert.
c) Cert, sempre.
d) Cert.
e) Cert.
f) Fals.

68 Indiqueu la resposta correcta:

$\{\emptyset,\{\emptyset\}\} \cup \{\{\emptyset\}\} =$

a) $\emptyset$ b) $\{\emptyset\}$ c) $\{\{\emptyset\}\}$ d) $\{\emptyset,\{\emptyset\}\}$

68* *Resposta:*

a) Fals. b) Fals. c) Fals. d) Cert.

69 Indiqueu la resposta correcta:

$\{\emptyset,\{\emptyset\}\} \cap \{\{\emptyset\}\} =$

a) $\emptyset$ b) $\{\emptyset\}$ c) $\{\{\emptyset\}\}$ d) $\{\{\{\emptyset\}\}\}$

69* *Resposta:*

a) Fals. b) Cert. c) Fals. d) Fals.

70 Obteniu:

a) $\{\emptyset\} - \emptyset$
b) $\emptyset - \{1,2,3,\emptyset\}$
c) $\{\emptyset\} - \{\{\emptyset\}\}$
d) $\{\emptyset\} - \{\emptyset,\{\emptyset\}\}$
e) $\{\emptyset,\{\emptyset\}\} - \{\emptyset\}$

70* *Resposta:*

a) $\{\emptyset\} - \emptyset = \{\emptyset\}$
b) $\emptyset - \{1,2,3,\emptyset\} = \emptyset$
c) $\{\emptyset\} - \{\{\emptyset\}\} = \{\emptyset\}$
d) $\{\emptyset\} - \{\emptyset,\{\emptyset\}\} = \emptyset$
e) $\{\emptyset,\{\emptyset\}\} - \{\emptyset\} = \{\{\emptyset\}\}$

71 Obteniu:

a) $(\{\emptyset\} \cup \{\emptyset\}) - \emptyset$
b) $(\{\emptyset\} \cup \{\emptyset\}) - \{\emptyset\}$
c) $\emptyset \cup \emptyset$
d) $\{\emptyset\} \cup \emptyset$
e) $\{\emptyset,\{\emptyset\}\} \cup \{\emptyset\}$

71* *Resposta:*

a) $(\{\emptyset\} \cup \{\emptyset\}) - \emptyset = \{\emptyset\} - \emptyset = \{\emptyset\}$
b) $(\{\emptyset\} \cup \{\emptyset\}) - \{\emptyset\} = \{\emptyset\} - \{\emptyset\} = \emptyset$
c) $\emptyset \cup \emptyset = \emptyset$
d) $\{\emptyset\} \cup \emptyset = \{\emptyset\}$
f) $\{\emptyset, \{\emptyset\}\} \cup \{\emptyset\} = \{\emptyset, \emptyset, \{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$

72 Cert o fals? (A, B conjunts qualssevol, Ω, conjunt universal; els complementaris estan referits a l'universal).

a) $A = B \Leftrightarrow A^c = B^c$
b) $A = B \Rightarrow \mathscr{P}(A) = \mathscr{P}(B)$
c) $(A \subseteq A \cup B) \wedge (B \subseteq A \cup B)$
d) $A \neq B \Leftrightarrow A^c \neq B^c$
e) $A \cap B \subseteq A \cup B$
f) $(A \cap B \subseteq A) \wedge (A \cap B \subseteq B)$
g) $A \subseteq B \Leftrightarrow A^c \subseteq B^c$
h) $A \subseteq B \Leftrightarrow B^c \subseteq A^c$
i) $A \nsubseteq B \Leftrightarrow A^c \nsubseteq B^c$
j) $A \nsubseteq B \Leftrightarrow B^c \nsubseteq A^c$
k) $(A \cup B)^c = (B \cup A)^c$
l) $A^c \cap B^c = \emptyset \Leftrightarrow A \cup B = \Omega$
m) $\Omega - (A \cap B) = \Omega - (B \cap A)$
n) $\Omega - (A \cup B) = (\Omega - A) \cap (\Omega - B)$

72* *Resposta:*

a) Cert.
b) Cert.
c) Cert.
d) Cert.
e) Cert.
f) Cert.
g) Fals.
h) Cert.
i) Fals.
j) Cert.
k) Cert.
l) Cert.
m) Cert.
n) Cert.

73 (Anàlisi de demostracions). A la demostració següent es prova:

$\mathscr{P}(A) = \mathscr{P}(B) \Rightarrow A = B$, per a tota parella de conjunts A, B.

Enteneu-la, justifiqueu tots els passos i identifiqueu on s'aplica la hipòtesi.

A partir de la hipòtesi, hem de demostrar $x \in A \Leftrightarrow x \in B$.

Vegem $x \in A \Rightarrow x \in B$.

$$\begin{aligned} x \in A \Rightarrow\ & \{x\} \subseteq A \\ \Rightarrow\ & \{x\} \in \mathscr{P}(A) \\ \Rightarrow\ & \{x\} \in \mathscr{P}(B) \\ \Rightarrow\ & \{x\} \subseteq B \\ \Rightarrow\ & x \in B \end{aligned}$$

Resta per al lector provar $x \in B \Rightarrow x \in A$ per una argumentació similar.

73* *Resposta:* La hipòtesi és $\mathscr{P}(A) = \mathscr{P}(B)$ i s'aplica en el pas

$\{x\} \in \mathscr{P}(A) \Rightarrow \{x\} \in \mathscr{P}(B)$.

74 Indiqueu quines afirmacions són certes (A, B conjunts qualssevol; Ω, conjunt universal; els complementaris estan referits a l'universal):

a) $A^c = B^c \Rightarrow A = B$
b) $\Omega - \emptyset = \Omega$
c) $\Omega - \Omega = \emptyset$
d) $A - A = \emptyset$
e) $A - \emptyset = A$
f) $\emptyset - A = \emptyset$
g) $(A-B) \cap (B-A) = \emptyset$
h) $A - B \subseteq A$
i) $(A-B) \cap B = \emptyset$
j) $(A-B) \cup A = A$
k) $(A-B) \cap A = A - B$
l) $(A-B) \cup B = A \cup B$
m) $A \cap A = A$
n) $A \cup A = A$

74* *Resposta:*

a) Cert. b) Cert. c) Cert. d) Cert. e) Cert. f) Cert. g) Cert. h) Cert. i) Cert. j) Cert. k) Cert. l) Cert. m) Cert. n) Cert.

75 Calculeu $|\{\{\{\{\{x,y,z\}\}\}\}\}|$. Quants i quins elements té el conjunt?

75* *Resposta:* El cardinal és 1. L'únic element és $\{\{\{\{x,y,z\}\}\}\}$.

76 Indiqueu quines afirmacions són certes. Els conjunts A, B són disjunts si:

a) $A \cap B = \emptyset$
b) $A \cap B = \{\emptyset\}$
c) $\emptyset \in A \cap B$
d) $|A \cap B| = 0$
e) $A \not\subseteq B$ i $B \not\subseteq A$
f) $A \cup B = A \cap B$
g) $A = B \neq \emptyset$
h) $A \neq B$
i) $A - B = \emptyset$
j) $A \cup B - A \cap B = A \cup B$
k) $(A-B) \cap (B-A) = \emptyset$
l) $A = (A-B) \cup (A \cap B)$
m) $|A \cup B| = |A| + |B|$

76* *Resposta:*

a) Cert (definició de ser disjunts).
b) Fals; en aquest cas, no són disjunts.
c) Fals; en aquest cas, no són disjunts.
d) Cert.
e) No. Poden ser disjunts o no.
f) No necessàriament.
g) No.
h) No.
i) No.
j) Cert.
k) No; aquesta propietat és certa sempre.
l) No; aquesta propietat és certa sempre.
m) Cert.

77 Indiqueu si són o no disjunts:

a) $A = \{1,5,7,9,a,c,\heartsuit,\aleph\}$, $B = \{\spadesuit,4,\aleph,6,9,\alpha\}$
b) $C = \{\emptyset,\neg,\nabla\}$, $D = \{\infty,2,\forall\}$

77* *Resposta:* a) No, i és $A \cap B = \{9,\aleph\}$ b) Si, és $C \cap D = \emptyset$.

78 Cert o fals?

a) $a \in \{x,y,z\} \Rightarrow ((a=x) \vee (a=y) \vee (a=z))$.
b) $a \in \{x,y,z\} \Rightarrow \neg((a=x) \vee (a=y) \vee (a=z))$.
c) $\{x,y,z\} = \{x\} \cup \{y\} \cup \{z\}$.
d) $a \in \{x,y,z\} \Leftrightarrow ((a=x) \vee (a=y) \vee (a=z))$.
e) $\{a\} \subseteq \{x,y,z\} \Rightarrow ((a=x) \vee (a=y) \vee (a=z))$.
f) $\{a\} \in \mathscr{P}(\{x,y,z\}) \Rightarrow ((a=x) \vee (a=y) \vee (a=z))$.
g) $\{x,y,z\} = \{x\} \cup \{y\} \cup \{z\} \cup \emptyset$.
h) $\{x,y,z\} = \{x\} \cup \{y\} \cup \{z\} \cup \{\emptyset\}$.

78* *Resposta:*

a) Cert. c) Cert. e) Cert. g) Cert.
b) Fals. d) Cert. f) Cert.

h) Fals. És $\{x\} \cup \{y\} \cup \{z\} \cup \{\emptyset\} = \{x,y,z,\emptyset\}$

79 Escriviu què vol dir que els conjunts A_1, A_2, A_3, A_4, A_5 són dos a dos disjunts.

79* *Resposta:* Cada dos són disjunts:

$A_1 \cap A_2 = \emptyset$, $A_1 \cap A_3 = \emptyset$, $A_1 \cap A_4 = \emptyset$, $A_1 \cap A_5 = \emptyset$,
$A_2 \cap A_3 = \emptyset$, $A_2 \cap A_4 = \emptyset$, $A_2 \cap A_5 = \emptyset$,
$A_3 \cap A_4 = \emptyset$, $A_3 \cap A_5 = \emptyset$,
$A_3 \cap A_5 = \emptyset$.

80 Si $A = \{1,2,3,4,x,y\}$, $B = \{\beta, 6, \alpha, y, 4, x\}$, obteniu:

a) $A \cap B$ b) $A \cup B$ c) $A - B$ d) $A - A \cap B$ e) $B - A$

80* *Resposta:*

a) $A \cap B = \{4,x,y\}$.
b) $A \cup B = \{1,2,3,4,x,y,6,\alpha,\beta\}$.
c) $A - B = \{\} = \emptyset$.
d) $A - A \cap B = \{1,2,3\}$.
e) $B - A = \{\alpha, \beta, 6\}$.

81 Indiqueu quins noms tenen les fórmules conjuntistes següents, on A, B, C són conjunts; U, universal.

a) $(A \cup B) \cup C = A \cup (B \cup C)$
b) $A \cap B = B \cap A$
c) $U - (A \cup B) = (U - A) \cap (U - B)$
d) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
e) $(A \cap B) \cap C = A \cap (B \cap C)$
f) $A \cup B = B \cup A$
g) $(A \cap B)^c = A^c \cup B^c$
h) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

81* *Resposta:*

a) Propietat associativa de la reunió.
b) Commutativitat de la intersecció.
c) De Morgan.
d) Distributiva de la unió respecte de la intersecció.
e) Propietat associativa de la intersecció.
f) Commutativitat de la unió.
g) De Morgan.
h) Distributiva de la intersecció respecte de la reunió.

82 Sigui A un conjunt de cardinal n. Quin és el cardinal de $\mathscr{P}(\mathscr{P}(\mathscr{P}(A)))$?

82* *Resposta:* $|\mathscr{P}(\mathscr{P}(\mathscr{P}(A)))| = 2^{(|\mathscr{P}(\mathscr{P}(A))|)} = 2^{(2^{|\mathscr{P}(A)|})} = 2^{(2^{(2^n)})}$

Hem utilitzat que $|\mathscr{P}(A)| = 2^{|A|}$.

83 Si $A = \{\emptyset, a, \{a,b\}\}$, escriviu $\mathscr{P}(A)$.

83* *Resposta:*

$\{$
$\emptyset$, (subconjunts de 0 elements)
$\{\emptyset\}, \{a\}, \{\{a,b\}\}$, (subconjunts d'1 element)
$\{\emptyset, a\}, \{\emptyset, \{a,b\}\}, \{a, \{a,b\}\}$, (subconjunts de 2 elements)
$\{\emptyset, a, \{a,b\}\}$ (subconjunts de 3 elements)
$\}$

84 Quin és el cardinal de $\{x, \{x, \{x,y, \{x,y,z, \{x,y, \{x,y\}\}\}\}\}\}$?

84* *Resposta:* El cardinal és 2. El conjunt té 2 elements:

x,
$\{x, \{x,y, \{x,y,z, \{x,y, \{x,y\}\}\}\}\}$.

85 És cert o fals que $B - A = B \cap A^c$ (A, B conjunts)?

85* *Resposta:* Cert.

86 Calculeu en funció de $|A|, |B|, |C|, |D|$ el cardinal de $D \times \mathscr{P}(\mathscr{P}(A) \times \mathscr{P}(B)) \times C$ (on A, B, C, D són conjunts finits).

86* *Resposta:*

$|D \times \mathscr{P}(\mathscr{P}(A) \times \mathscr{P}(B)) \times C| =$
$|D|\ |\mathscr{P}(\mathscr{P}(A)|\ |\mathscr{P}(B))|\ |C| =$
$|D|\ 2^{|\mathscr{P}(A)|}\ 2^{|B|}\ |C| =$
$|D|\ 2^{(2^{|A|})}\ 2^{|B|}\ |C|$

87 Escriviu les lleis de De Morgan per a conjunts.

87* *Resposta:* Les expressem segons diverses notacions:

a) i) $(A \cap B)^c = A^c \cup B^c$
ii) $\Omega - (A \cap B) = (\Omega - A) \cup (\Omega - B)$
iii) $\Omega \backslash (A \cap B) = (\Omega \backslash A) \cup (\Omega \backslash B)$

b) i) $(A \cup B)^c = A^c \cap B^c$
ii) $\Omega - (A \cup B) = (\Omega - A) \cap (\Omega - B)$
iii) $\Omega \backslash (A \cup B) = (\Omega \backslash A) \cap (\Omega \backslash B)$

88 Identifiqueu, d'entre les següents, la propietat distributiva de la reunió respecte de la intersecció de conjunts:

a) $p \vee (r \wedge s) \equiv (p \vee r) \wedge (p \vee s)$
b) $(A \cup B) \cup (A \cup C) = A \cup (B \cup C)$
c) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
d) $(B \cap C) \cup A = (B \cup A) \cap (C \cup A)$
e) $(B \cap C) \cup A = (A \cup C) \cap (B \cup A)$
f) $(C \cap B) \cup A = (A \cup B) \cap (C \cup A)$
g) $(A \cap B) \cap (A \cap C) = A \cap B \cap C$
h) $|A \cup B| + |A \cap B| = |A| + |B|$ (conjunts finits)
i) $|A| + |B| + |C| = |A \cup B \cup C| - |A \cap B \cap C| + |A \cap B| + |A \cap C| + |B \cap C|$ (conjunts finits)
j) Cap de les anteriors.

88* *Resposta:*

a) No, són proposicions.
b) No.
c) No. És la distributivitat de la intersecció respecte de la unió.
d) Sí.
e) Sí, combinat amb propietats commutatives.
f) Sí, combinat amb propietats commutatives.
g) No.
h) No.
i) No.
j) No.

89 Identifiqueu, d'entre les següents, la propietat distributiva de la intersecció respecte de la reunió de conjunts.

a) $(C \cup B) \cap A = (A \cap B) \cup (C \cap A)$
b) $|A \cup B| + |A \cap B| = |A| + |B|$ (conjunts finits)

c) $|A|+|B|+|C| = |A\cup B\cup C| - |A\cap B\cap C| + |A\cap B| + |A\cap C| + |B\cap C|$ (conjunts finits)
d) $|A\cap(B\cup C)| = |(A\cap B)\cup(A\cap C)| = |A\cap B| + |A\cap C| - |A\cap B\cap C|$ (conjunts finits)
e) Cap de les anteriors.

89* *Resposta:* És la propietat (a), que és $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$, combinada amb propietats de commutativitat.

90 Si A, B són conjunts finits, el nombre d'elements $|A\times B|$ del producte cartesià $A\times B$ és:

a) $(|A|-|B|)(|B|-|A|)$
b) $|A|+|B|$
c) $|A||B|$
d) $2^{|A||B|}$
e) $2^{|A|+|B|}$
f) Cap dels anteriors.

90* *Resposta:*

a) No.
b) No.
c) Sí.
d) No.
e) No.
f) No.

91 Expresseu la intersecció de dos conjunts en termes de la reunió i del complementari.

91* *Resposta:* Per De Morgan: $A\cap B = (A^c\cup B^c)^c$. En efecte, $A\cap B = ((A\cap B)^c)^c = (A^c\cup B^c)^c$.

També es pot expressar: $A\cap B = \Omega - ((\Omega - A)\cup(\Omega - B))$.

92 Expresseu la unió de dos conjunts en termes de la intersecció i del complementari.

92* *Resposta:* $A\cup B = (A^c\cap B^c)^c$. En efecte, $A\cup B = (A\cup B)^{cc} = (A^c\cap B^c)^c$, per doble complementació i per una de les propietats de De Morgan. També es pot expressar: $A\cup B = \Omega - ((\Omega - A)\cap(\Omega - B))$.

93 De les propietats de la llista següent, indiqueu quines es compleixen per a la intersecció.

a) associativa
b) commutativa
c) $A\cap A = A$
d) $A\cap\emptyset = \emptyset$
e) $A\cap B = (A^c\cup B^c)^c$
f) $A\cap A^c = \emptyset$
g) $A\cap\Omega = A$
h) $A\cap B = A \Leftrightarrow A\subseteq B$
i) $A\subseteq B \Leftrightarrow B^c = A^c\cap B^c$

93* *Resposta:*

a) Sí.
b) Sí.
c) Sí.
d) Sí.
e) Sí.
f) Sí.
g) Sí.
h) Sí.

i) Sí. Si $A \subseteq B$, és $B = A \cup B$, d'on $B^c = (A \cup B)^c = A^c \cap B^c$, per De Morgan. I recíprocament.

94 Considereu la demostració d'una propietat relativa a fórmules conjuntistes (la propietat no importa; només importa saber què ens permet fer les manipulacions que s'hi fan). Es justifica cada pas indicant quina propietat s'hi aplica. A l'exercici, s'omet aquesta explicació, que ha de subministrar el lector:

Deducció (Ω conjunt universal):

$$
\begin{array}{rll}
A = & A \cap \Omega, & \text{per ...} \\
= & A \cap ((B \cup C) \cup ((B \cup C)^c)), & \text{per ...} \\
 & & \;\;\text{...} \\
= & [A \cap (B \cup C)] \cup [A \cap ((B \cup C)^c)], & \text{per ...} \\
= & [A \cap (B \cup C)] \cup [A \cap (B^c \cap C^c)], & \text{per ...} \\
= & [A \cap (B \cup C)] \cup [A \cap B^c \cap C^c], & \text{per ...} \\
= & [A \cap (B \cup C)] \cup [C^c \cap B^c \cap A], & \text{per ...} \\
= & [A \cap (C \cup B)] \cup [C^c \cap B^c \cap A], & \text{per ...}
\end{array}
$$

94* *Resposta:*

$$
\begin{array}{rll}
A = & A \cap \Omega, & \text{per } X \subseteq Y \Rightarrow X = X \cap Y \\
= & A \cap ((B \cup C) \cup ((B \cup C)^c)), & \text{per } X \subseteq \Omega \Rightarrow X \cup X^c = \Omega \\
= & [A \cap (B \cup C)] \cup [A \cap (B \cup C)^c)], & \text{per distributivitat de la intersecció} \\
 & & \text{respecte de la unió} \\
= & [A \cap (B \cup C)] \cup [A \cap (B^c \cap C^c)], & \text{per una de les lleis de De Morgan} \\
= & [A \cap B \cup C] \cup [A \cap B^c \cap C^c], & \text{per associativitat de la intersecció} \\
= & [A \cap (B \cup C)] \cup [C^c \cap B^c \cap A], & \text{per commutativitat de la intersecció} \\
= & [A \cap (C \cup B)] \cup [C^c \cap B^c \cap A], & \text{per commutativitat de la unió}
\end{array}
$$

95 Escriviu la fórmula de distributivitat de la reunió d'un conjunt respecte de la intersecció de quatre conjunts.

95* *Resposta:* $A \cup (B \cap C \cap D \cap E) = (A \cup B) \cap (A \cup C) \cap (A \cup D) \cap (A \cup E)$

96 Si $A \cap B = \{1,2,3,6,z\}$, $A \cap C = \{x,y,2,z\}$, obteniu $A \cap (B \cup C)$. Quines propietats utilitzeu?

96* *Resposta:* Per la propietat distributiva de la intersecció respecte de la reunió, podem escriure:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) = \{1,2,3,6,z\} \cup \{x,y,2,z\} = \{1,2,3,6,x,y,z\}.$$

97 Per què podem escriure sense ambigüitat $A \cup B \cup C \cup D \cup E \cup F$?

97* *Resposta:* Per l'associativitat de la reunió.

98 Quants elements té el conjunt $\{x,y,z,\{x,\{x,\{x,y\}\},z\},t,\{x,z\}\}$?

98* *Resposta:* El conjunt té sis elements:

x, y, z, t,
$\{x,\{x,\{x,y\}\},z\}$,
$\{x,z\}$

99 És certa la igualtat següent? Si ho és, té algun nom? $\Omega - (A \cup B \cup C) = (\Omega - A) \cap (\Omega - B) \cap (\Omega - C)$

99* *Resposta:* Sí, és la propietat de De Morgan per al complementari de la reunió de tres conjunts.

100 Indiqueu quines propietats utilitzem quan escrivim

$A \cup (B \cap C) = (C \cup A) \cap (B \cup A)$.

100* *Resposta:* La distributivitat de la reunió respecte de la intersecció, la commutativitat de la reunió i la commutativitat de la intersecció. Concretament:

$$\begin{aligned} A \cup (B \cap C) = {} & (A \cup B) \cap (A \cup C), && \text{per distributivitat de la unió respecte de la intersecció} \\ = {} & (B \cup A) \cap (C \cup A), && \text{per la commutativitat de la unió} \\ = {} & (C \cup A) \cap (B \cup A), && \text{per la commutativitat de la intersecció} \end{aligned}$$

101 Quines són les igualtats següents?

a) $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$
b) $(A \cup C) \cap (B \cup C) = (A \cap B) \cup C$
c) $(U - A) \cup (U - B) \cup (U - C) \cup (U - D) = (A \cap B \cap C \cap D)^c$
d) $A \cap (B \cup C \cup D) = (A \cap B) \cup (A \cap C) \cup (A \cap D)$

101* *Resposta:*

a) Distributivitat de la intersecció respecte de la unió.
b) Distributivitat de la unió respecte de la intersecció.
c) Una de les lleis de De Morgan.
d) Distributivitat de la intersecció respecte de la reunió (de 3 conjunts).

102 Sigui $A = \{1, 2, 3\}$.

Aleshores $\emptyset - A =$

a) A^c
b) $\emptyset$
c) A
d) $-A$
e) $A - \emptyset$
f) $\{-1, -2, -3\}$
g) Cap dels anteriors.

102* *Resposta:*

a) Fals.
b) Cert.
c) Fals.
d) Fals (la fórmula no té sentit).
e) Fals.
f) Fals.
g) Fals.

103 Si A,B són conjunts, és $-A\cap\cup\emptyset B))(-))$ una fórmula conjuntista ben formada?

103* *Resposta:* No.

104 Escriviu les subfórmules de la fórmula conjuntista $(A-B)\cup(A\cap B)\cup(B-A)$ (escriptura, per associativitat, de $((A-B)\cup(A\cap B))\cup(B-A)$. Per a què és útil aquesta enumeració de les subfórmules?

104* *Resposta:* $A,B,A-BA\cap B,B-A,(A-B)\cup(A\cap B),((A-B)\cup(A\cap B))\cup(B-A)$. Pot ser útil per a calcular la taula de pertinença.

105 Sigui $A\subseteq\Omega$. Si $\Omega=\{1,2,3,4,5,6,7\}$, $\Omega-A=\{3,5,7\}$, obteniu A.

105* *Resposta:* $A=\Omega-(\Omega-A)=\{1,2,3,4,5,6,7\}-\{3,5,7\}=\{1,2,4,6\}$.

Dit d'una altra manera, $A=(A^c)^c=(\{3,5,7\})^c=\{1,2,4,6\}$.

106 Sigui A un conjunt. Indiqueu si són equivalents:

a) $a\in A$ b) $\{a\}\subseteq A$ c) $\{a\}\in\mathscr{P}(A)$

106* *Resposta:* Sí.

107 Considereu diverses manipulacions conjuntistes que es realitzen a partir d'una fórmula. Justifiqueu cada pas:

$$\begin{aligned}
A-(B-C) &= A\cap(B-C)^c, && \text{per ...}\\
&= A\cap(B\cap C^c)^c, && \text{per ...}\\
&= A\cap(B^c\cup(C^c)^c), && \text{per ...}\\
&= A\cap(B^c\cup C), && \text{per ...}\\
&= (A\cap B^c)\cup(A\cap C), && \text{per ...}\\
&= (A-B)\cup(A\cap C), && \text{per ...}
\end{aligned}$$

107* *Resposta:*

$$\begin{aligned}
A-(B-C) &= A\cap(B-C)^c, && \text{per expressió de la diferència de conjunts}\\
& && \text{en termes del complementari}\\
&= A\cap(B\cap C^c)^c, && \text{per } X-Y=X\cap Y^c\\
&= A\cap(B^c\cup(C^c)^c), && \text{per De Morgan}\\
&= A\cap(B^c\cup C), && \text{per doble complementació}\\
&= (A\cap B^c)\cup(A\cap C), && \text{per distributivitat de la intersecció}\\
& && \text{respecte de la unió}\\
&= (A-B)\cup(A\cap C), && \text{per } X\cap Y^c=X-Y
\end{aligned}$$

108 Considereu diverses manipulacions conjuntistes que es realitzen a partir d'una fórmula. Justifiqueu cada pas:

$$\begin{aligned}(A-B)-C = {} & (A\cap B^c)-C, && \text{per ...}\\ = {} & (A\cap B^c)\cap C^c, && \text{per ...}\\ = {} & A\cap(B^c\cap C^c), && \text{per ...}\\ = {} & A\cap((B\cup C)^c), && \text{per ...}\\ = {} & A-(B\cup C), && \text{per ...}\end{aligned}$$

108* *Resposta:*

$$\begin{aligned}(A-B)-C = {} & (A\cap B^c)-C, && \text{per } X-Y=X\cap Y^c\\ = {} & (A\cap B^c)\cap C^c, && \text{per } X-Y=X\cap Y^c\\ = {} & A\cap(B^c\cap C^c), && \text{per associativitat de la intersecció}\\ = {} & A\cap((B\cup C)^c), && \text{per De Morgan}\\ = {} & A-(B\cup C), && \text{per } X\cap Y^c=X-Y\end{aligned}$$

109 Si A,B,C,D,E són conjunts, escriviu fórmules lògiques (de predicats) per descriure el conjunt:

$T = A-(B\cap(C\cup(D-E)))$

(és a dir, els elements del conjunt anterior).

109* *Resposta:* Sigui x un element qualsevol de T.
Escrivim la seqüència de fórmules lògiques equivalents, aplicant diverses equivalències lògiques (resta per al lector completar l'exercici dient quines). Qualsevol de les fórmules equival a la següent. Qualsevol d'elles resol l'exercici.

$x\in A\wedge\neg x\in B\cap(C\cup(D-E))$

$x\in A\wedge\neg(x\in B\wedge x\in(C\cup(D-E)))$

$x\in A\wedge\neg(x\in B\wedge(x\in C\vee x\in D-E))$

$x\in A\wedge\neg(x\in B\wedge(x\in C\vee(x\in D\wedge\neg x\in E)))$

$x\in A\wedge(x\notin B\vee\neg(x\in C\vee(x\in D\wedge\neg x\in E)))$

$x\in A\wedge(x\notin B\vee(x\notin C\wedge\neg(x\in D\wedge\neg x\in E)))$

$x\in A\wedge(x\notin B\vee(x\notin C\wedge(x\notin D\vee x\in E)))$

$x\in A\wedge(x\notin B\vee(x\notin C\wedge x\notin D)\vee(x\notin C\wedge x\in E)))$

És a dir, $T=\{x : x\in A\wedge(x\notin B\vee(x\notin C\wedge x\notin D)\vee(x\notin C\wedge x\in E)))\}$.

110 Si A i B són conjunts, deduïu que $x\notin A^c-B^c$ equival a $x\in A\vee x\notin B$.

110* *Resposta:* Es pot resoldre efectuant operacions conjuntistes, sense raonar directament sobre elements i pertinences a conjunts.

Observem que $x \notin A^c - B^c$ equival a $x \in (A^c - B^c)^c$.

$(A^c - B^c)^c = (A^c \cap (B^c)^c)^c = (A^c \cap B)^c = (A^c)^c \cup B^c = A \cup B^c$

Per tant, $x \notin A^c - B^c \Leftrightarrow x \in (A^c - B^c)^c \Leftrightarrow x \in A \cup B^c \Leftrightarrow x \in A \vee x \notin B$.

Mètode 2. Raonem sobre elements:

$\neg(x \in A^c - B^c)$

$\neg(x \in A^c \wedge \neg x \in B^c)$

$\neg(\neg x \in A \wedge \neg\neg x \in B)$

$\neg(\neg x \in A \wedge x \in B)$

$\neg\neg x \in A \vee \neg x \in B$

$x \in A \vee \neg x \in B$

$x \in A \vee x \notin B$

(correspon a $A \cup B^c$)

El lector acabarà de justificar cada pas de la seqüència anterior.

111 Siguin A, B, C, D conjunts. Deduïu que $x \notin A \cap (B - (C \cup D))$ equival a

$x \notin A \vee x \notin B \vee x \in C \vee x \in D$.

111* *Resposta:* Es pot raonar efectuant operacions conjuntistes:

$[A \cap (B - (C \cup D))]^c =$

$= [A \cap (B \cap (C \cup D)^c)]^c =$

$= [A \cap (B \cap (C^c \cap D^c)]^c =$

$= (A \cap B \cap C^c \cap D^c)^c =$

$= (A^c \cup B^c \cup C \cup D)$

El lector acabarà de justificar cada pas de la seqüència anterior.

Raonant amb elements:

$\neg[x \in A \wedge x \in B - (C \cup D)]$

$\neg[x \in A \wedge (x \in B \wedge \neg x \in C \cup D)]$

$\neg[x \in A \wedge x \in B \wedge \neg x \in C \cup D]$

$\neg[x \in A \wedge x \in B \wedge \neg(x \in C \vee x \in D)]$

$\neg[x \in A \wedge x \in B \wedge \neg x \in C \wedge \neg x \in D]$

$\neg x \in A \vee \neg x \in B \vee \neg\neg x \in C \vee \neg\neg x \in D$

$x \notin A \vee x \notin B \vee x \in C \vee x \in D$

El lector acabarà de justificar cada pas de la seqüència anterior.

112 Siguin A i B conjunts. Indiqueu si és cert:

$(x \notin C \wedge x \in B) \Rightarrow x \notin B \cap C$

112* *Resposta:* Sí, és cert. Donat que $B \cap C \subseteq C$, si fos $x \in B \cap C$, seria $x \in C$, contradicció.

113 Si B i C són conjunts, relacioneu:

a) $x \notin C \rightarrow (x \in B \rightarrow x \notin B \cap C)$
b) $x \in B \rightarrow (x \notin C \rightarrow x \notin B \cap C)$
c) $(x \notin C \wedge x \in B) \rightarrow x \notin B \cap C)$
d) $(x \notin C \rightarrow x \in B) \rightarrow x \notin B \cap C)$

113* *Resposta:* Els tres primers són equivalents. El quart no equival a cap dels anteriors. Per què?

114 Siguin C i D conjunts. Relacioneu:

a) $x \notin C \cup D$
b) $x \notin C \vee x \notin D$
c) $x \notin C \wedge x \notin D$
d) $x \in C \wedge x \in D$
e) $x \in C \vee x \in D$
f) $x \notin C \cap D$

114* *Resposta:*

(a) i (c) són equivalents.
(b) i (f) són equivalents.
(d) implica (e).
(a) implica (f).
(d) equival a no (f).
(a) equival a no (e.)

El lector acabarà de justificar les afirmacions anteriors.

115 Quin és el conjunt format amb tots els elements de la llista: $1,1,2,2,2,3,3,4,1,5,6,7,7$?

a) $\{1,1,2,2,2,3,3,4,1,5,6,7,7\}$
b) $\{\{1,1\},\{2,2,2\},\{3,3\},4,1,5,6,\{7,7\}\}$
c) $\{1,2,3,4,5,6,7\}$

115* *Resposta:*

a) No. b) No. c) Sí.

116 Si A és un conjunt, indiqueu si és possible:

$a \in A$, $\{a\} \in A$, $\{a\} \subseteq A$, $\{\{a\}\} \subseteq A$.

116* *Resposta:* Sí, per exemple en el cas $A = \{a,\{a\},\{\{a\}\}\}$.

117 Siguin A,B conjunts. Expresseu mitjançant fórmules de predicat:

a) $A = B$
b) $A \neq B$
c) $A \subseteq B$ i $A \neq B$

117* *Resposta:*

a) $\forall x(x \in A \leftrightarrow x \in B)$

$\forall x((x \in A \to x \in B) \wedge (x \in B \to x \in A))$

b) Neguem la fórmula anterior (la segona):

$\neg\forall x((x \in A \to x \in B) \wedge (x \in B \to x \in A))$, que equival a

$\exists x\neg((x \in A \to x \in B) \wedge (x \in B \to x \in A))$, que equival a

$\exists x(\neg(x \in A \to x \in B) \vee \neg(x \in B \to x \in A))$ (per De Morgan), que equival a

$\exists x((x \in A \wedge \neg x \in B) \vee (x \in B \wedge \neg x \in A))$ (per negació del condicional), que equival a

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

c) Utilitzem l'última fórmula de (b):

$A \subseteq B \wedge A \neq B$

$\forall z(z \in A \to z \in B) \wedge \exists x((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A))$

118 Considerem el conjunt $A = \{1,2,3,\{4,5,\{6\}\},\emptyset,\{7\}\}$. Indiqueu si les afirmacions següents són certes o falses.

a) $3 \in A$
b) $4 \in A$
c) $7 \in A$
d) $\{7\} \subseteq A$
e) $\{\{7\}\} \subseteq A$
f) $\{7\} \in A$
g) $\{4,5\} \subseteq A$
h) $4 \notin A, 5 \notin A, \{4,5,\{6\}\} \in A$
i) $\{1,3\} \subseteq A$
j) $\emptyset \in A$
k) $\emptyset \subseteq A$
l) $\{6\} \in A$
m) $\{3\} \notin A$
n) $\{3\} \subseteq A$
o) $2 \notin A$
p) $4 \notin A$, $5 \notin A$, $\{4,5\} \nsubseteq A$
q) $4 \notin A$, $5 \notin A$, $\{4,5\} \subseteq A$

118* *Resposta:*

a) Cert.	d) Fals.	g) Fals.	j) Cert.	m) Cert.	p) Cert.
b) Fals.	e) Cert.	h) Cert.	k) Cert.	n) Cert.	
c) Fals.	f) Cert.	i) Cert.	l) Fals.	o) Fals.	q) Fals.

119 Siguin A,B subconjunts d'un conjunt no buit Ω. Indiquem per W^c el complementari de W en Ω.

Indiqueu quines afirmacions són certes (en general, per a tot A,B) i quines no.

a) $A - B = A \cap B^c$
b) $A - B = A - (A \cap B)$
c) $A - B = B \cap A^c$
d) $A - B = (A \cup B) - B$
e) $A - B = (A \cup B) - A$
f) $A - B = (A \cup B) - (A \cap B)$
g) $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$
h) $(A \cup B) - (A - B) = B$
i) $A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$

119* *Resposta:*

a) Cert.	c) Fals.	d) Fals.	f) Cert.	h) Cert.
b) Cert.	c) Cert.	e) Fals.	g) Cert.	

120 Siguin A,B,C subconjunts d'un conjunt no buit Ω. Digueu si són certs, per a tot A,B,C:

a) $A^c \cap B^c = A^c - B = B^c - A$
b) $A^c - B^c = B - A$
c) $A^c - B^c = A^c - (A^c \cap B^c) = A^c - (A \cap B)^c$
d) $A^c \cap B = B - (A \cap B)$
e) $B^c \cap (C - A) = (C - A) - B$
f) $(A \cup B)^c \cap C = C - (A \cup B)$
g) $(A \cap B)^c \cap C = (A^c \cup B^c) \cap C = (A^c \cap C) \cup (B^c \cap C)$

120* *Resposta:*

a) Cert. c) Cert. e) Cert. g) Cert.
b) Cert. d) Cert. f) Cert.

121 Digueu si $a \in \{1,2,3\}$ és equivalent a alguna de les afirmacions següents:

a) $a = 1 \vee a = 2 \vee a = 3$
b) $a = 1 \wedge a = 2 \wedge a = 3$
c) $a \neq 1 \vee a \neq 2 \vee a \neq 3$
d) $a \neq 1 \wedge a \neq 2 \wedge a \neq 3$

121* *Resposta:*

a) Sí. b) No. c) No.

(a) No. Equival a $a \notin \{1,2,3\}$

122 Com expressar que a és un nombre enter diferent de zero sense utilitzar $\neq$?

122* *Resposta:* $a \in \mathbb{Z} - \{0\}$

123 Siguin C un conjunt no buit i $a, b \in C$. Com expressar que a i b són diferents sense utilitzar $\neq$?

123* *Resposta:* Per exemple, $a \in C - \{b\}$ o $b \in C - \{a\}$.

124 El conjunt:

$$R = \{(\emptyset,\{\emptyset\}),(\{\emptyset\},\emptyset),(\{\emptyset\},\{\emptyset\}),(\emptyset,\emptyset)\}$$

es pot expressar com a producte cartesià?

124* *Resposta:* Sí. $R = \{\emptyset,\{\emptyset\}\} \times \{\emptyset,\{\emptyset\}\}$.

125 Si $A = \{a,\{a\}\}$, és $a \in A$ i $\{a\} \subseteq A$?

125* *Resposta:* Sí.

126 Digueu quines de les afirmacions són certes:

a) $\{a,b\} = \{b,a\}$
b) $\{a,b,c,d\} = \{b,d,c,a\}$
c) $\{a,b,a\} = \{a,b\}$
d) $\{2,\{2\}\} = \{2\}$
e) $\{a,b,c,d\} = \{a,b\} \cup \{a,c,d,d\}$
f) $\{2,2\} = \{2\}$
g) $\{2\} \cap \{\{2\}\} = \emptyset$
h) $\{2,\{\{2\}\}\} \cap \{\{2\}\} = \emptyset$
i) $\{2,\{\{2\}\},\{2\}\} \cap \{\{2\}\} = \{2\}$

126* *Resposta:*

a) Cert. c) Cert. e) Cert. g) Cert. i) Fals.
b) Cert. d) Fals. f) Cert. h) Cert.

127 Siguin A, B conjunts. Indiqueu quines relacions d'equivalència o implicació existeixen entre les afirmacions següents:

a) $x \notin A \cup B$
b) $x \notin A \vee x \notin B$
c) $x \notin A \wedge x \notin B$
d) $x \notin A \cap B$
e) $x \in A \vee x \in B$

127* *Resposta:*

$(a) \Leftrightarrow (c)$

$(b) \Leftrightarrow (d)$

$(a) \Rightarrow (d)$

i les derivades:

$(c) \Rightarrow (d)$

$(a) \Rightarrow (b)$

$(c) \Rightarrow (b)$

Finalment, $(e) \Leftrightarrow (\neg a)$

128 Siguin A, B conjunts, subconjunts de Ω, respecte del qual es considera el complementari. Indiqueu quines fórmules són equivalents a $x \notin A \cap B^c$:

a) $x \notin A \vee x \notin B$
b) $x \notin A \vee x \in B$
c) $x \notin A \wedge x \notin B$
d) $x \notin A \wedge x \in B$

128* *Resposta:* (b) és equivalent a la fórmula donada:

Vegem una seqüència d'equivalències (cada fórmula és equivalent a la següent, estudieu per què):

$x \notin A \cap B^c$ (equival a)

$x \notin (A \cap B^c)$

$\neg x \in (A \cap B^c)$

$\neg(x \in A \wedge x \in B^c)$

$\neg(x \in A) \vee \neg(x \in B^c)$

$(x \notin A) \vee (x \notin B^c)$

$(x \notin A) \vee \neg(x \notin B)$

$(x \notin A) \vee \neg\neg(x \in B)$

$(x \notin A) \vee (x \in B)$

El lector estudiarà les altres fórmules.

Es pot veure alternativament a partir de fórmules conjuntistes:

$(A\cap B)^c$ és el conjunt dels elements x que satisfà $x\notin A\cap B^c$.

$A^c\cup B$ és el conjunt dels elements x que satisfà $x\notin A\vee x\in B$.

$(A\cap B)^c = A^c\cup B^{cc} = A^c\cup B$, per De Morgan i doble complementació.

129 Siguin A,B subconjunts de Ω, respecte del qual es considera el complementari. Escriviu fórmules de predicat que descriguin la pertinença als diversos conjunts que s'indiquen, en termes de la pertinença (o no pertinença) als conjunts A,B:

a) $x\in(A\cap B)^c$
b) $x\in A^c\cup B$
c) $x\notin A^c\cup B$
d) $x\notin A^c\cap B$
e) $x\notin A^c\cap B^c$
f) $x\in A^c\cup B^c$
g) $x\notin(A\cap B)^c$
h) $x\in(A-B)^c$
i) $x\notin A-B$
j) $x\notin(A^c\cup B)-(A\cap B^c)$

129* *Resposta:* Es presenten seqüències d'enunciats equivalents (el lector les justificarà):

a) $\neg(x\in(A\cap B))$ (és a dir, $x\notin A\cap B$)

$\neg(x\in A\wedge x\in B)$

$\neg(x\in A)\vee\neg(x\in B)$

$x\notin A\vee x\notin B$

b) $x\in A^c\vee x\in B$

$x\notin A\vee x\in B$

c) $\neg x\in(A^c\cup B)$

$\neg(x\in A^c\vee x\in B)$

$\neg(\neg(x\in A)\vee x\in B)$

$\neg\neg(x\in A)\wedge\neg(x\in B)$

$x\in A\wedge x\notin B$

d) $x\notin(A^c\cap B)$

$\neg(x\in(A^c\cap B))$

$\neg(x\in A^c\wedge x\in B)$

$\neg(\neg x\in A\wedge x\in B)$

$\neg\neg x\in A\vee\neg x\in B)$

$x\in A\vee x\notin B)$

e) $x \notin A^c \cap B^c$

$\neg x \in A^c \cap B^c$

$\neg(x \in A^c \wedge x \in B^c)$

$\neg(\neg x \in A \wedge \neg x \in B)$

$(\neg\neg x \in A) \vee (\neg\neg x \in B)$

$x \in A \vee x \in B$

També, per De Morgan:

$x \notin A^c \cap B^c$

$x \notin (A \cup B)^c$

$x \in A \cup B$

$x \in A \vee x \in B$

f) $x \in A^c \cup B^c$

$x \in A^c \vee x \in B^c$

$x \notin A \vee x \notin B$

g) $x \notin (A \cap B)^c$

$\neg x \in (A \cap B)^c$

$\neg x \notin (A \cap B)$

$\neg\neg x \in (A \cap B)$

$x \in (A \cap B)$

$x \in A \wedge x \in B$

h) $x \in (A - B)^c$

$\neg x \in (A - B)$

$\neg(x \in A \wedge x \notin B)$

$\neg(x \in A \wedge \neg x \in B)$

$\neg(x \in A) \vee \neg(\neg x \in B)$

$x \notin A \vee x \in B$

i) $x \notin A - B$

$\neg(x \in A - B)$

$\neg(x \in A \wedge x \notin B)$

$\neg(x \in A \wedge \neg(x \in B))$

$\neg(x \in A) \vee \neg\neg(x \in B)$

$(x \notin A) \vee (x \in B)$

$x \notin A \vee x \in B$

j) $x \notin (A^c \cup B) - (A \cap B^c)$, equivalent a

$\neg(x \in (A^c \cup B) - (A \cap B^c))$

$\neg(x \in (A^c \cup B) \wedge x \notin (A \cap B^c))$

$\neg((x \in A^c \vee x \in B) \wedge \neg x \in (A \cap B^c))$

$\neg((x \in A^c \vee x \in B) \wedge \neg(x \in A \wedge x \in B^c))$

$\neg((x \notin A \vee x \in B) \wedge \neg(x \in A \wedge x \notin B))$

$\neg((\neg(x \in A) \vee x \in B) \wedge \neg(x \in A \wedge \neg(x \in B)))$

$\neg(\neg(x \in A) \vee x \in B) \vee \neg(\neg(x \in A \wedge \neg(x \in B)))$

$(\neg\neg(x \in A) \wedge \neg(x \in B)) \vee (x \in A \wedge \neg(x \in B))$

$((x \in A) \wedge \neg(x \in B)) \vee (x \in A \wedge \neg(x \in B))$

$(x \in A) \wedge \neg(x \in B)$

$x \in A \wedge x \notin B$

Pot resultar més còmode efectuant operacions conjuntistes:

$[(A^c \cup B) - (A \cap B^c)]^c$

$= [(A^c \cup B) \cap (A \cap B^c)^c]^c$

$= (A^c \cup B)^c \cup (A \cap B^c)^{cc}$ (De Morgan)

$= (A^c \cup B)^c \cup (A \cap B^c)$ (doble complementació)

$= (A^{cc} \cap B^c) \cup (A \cap B^c)$ (De Morgan)

$= (A \cap B^c) \cup (A \cap B^c)$ (doble complementació)

$= (A \cap B^c)$

Així, una fórmula equivalent és: $x \in A \wedge x \notin B$.

130 Obteniu $\mathscr{P}(\{a,b,\{c,d\}\})$.

130* *Resposta:*

$$\mathscr{P}(\{a,b,\{c,d\}\}) = \{\emptyset, \{a\}, \{b\}, \{\{c,d\}\}, \{a,b\}, \{a,\{c,d\}\}, \{b,\{c,d\}\}, \{a,b,\{c,d\}\}\}$$

131 Siguin A,B,C conjunts. Estudieu si són equivalents les fórmules:

$x \notin (A \cup B^c) - C$

$(x \notin A \wedge x \in B) \vee x \in C$

131* *Resposta:* Són equivalents. N'escrivim fórmules equivalents:

$x \notin (A \cup B^c) - C$

$\neg(x \in (A \cup B^c) - C)$

$\neg(x \in (A \cup B^c) \wedge \neg x \in C)$

$\neg((x \in A \vee x \in B^c) \wedge \neg x \in C)$

$\neg((x \in A \vee \neg x \in B) \wedge \neg x \in C)$

$\neg(x \in A \vee \neg x \in B) \vee \neg\neg x \in C$, per l'equivalència de De Morgan

$(\neg x \in A \wedge \neg\neg x \in B) \vee \neg\neg x \in C$, per l'equivalència de De Morgan

$(\neg x \in A \wedge x \in B) \vee x \in C$, per l'equivalència de doble negació

$(x \notin A \wedge x \in B) \vee x \in C$

132 Obtingueu $\{1,2,3\} \times \{a,b\}$

132* *Resposta:* $\{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$

133 Quants subconjunts té $\{a,b,c\} \times \{0,1\}$?

133* *Resposta:* $|\mathscr{P}(\{a,b,c\} \times \{0,1\})| = 2^{|\{a,b,c\} \times \{0,1\}|} = 2^{|\{a,b,c\}|\ |\{0,1\}|} = 2^{3\times 2} = 2^6$

134 Obteniu $\mathscr{P}(\{1,\{\emptyset\}\})$

134* *Resposta:* $\{\emptyset,\{1\},\{\{\emptyset\}\},\{1,\{\emptyset\}\}\}$

135 Siguin $A = \{1,2,3,a\}$, $B = \{x,y,1,a\}$. Obtingueu

a) $A \cap B$
b) $A - (B - B)$
c) $A - (A \cap B)$
d) $A - B$
e) $B - A$
f) $((A - B) - B) - A$
g) $(A \cup B) - (A \cap B)$
h) $A - (A \cup B)$
i) $(A \cup B) - A$
j) $A - A$

135* *Resposta:*

a) $A \cap B = \{1,a\}$
b) $A - (B - B) = A - \emptyset = A$
c) $A - (A \cap B) = A - \{1,a\} = \{2,3\}$
d) $A - B = \{2,3\}$
e) $B - A = \{x,y\}$
f) $((A - B) - B) - A = (\{2,3\} - B) - A = \{2,3\} - A = \emptyset$
g) $(A \cup B) - (A \cap B) = \{1,2,3,x,y,a\} - \{1,a\} = \{2,3,x,y\}$
h) $A - (A \cup B) = A - \{1,2,3,x,y,a\} = \{1,2,3,a\} - \{1,2,3,x,y,a\} = \emptyset$
i) $(A \cup B) - A = \{1,2,3,x,y,a\} - \{1,2,3,a\} = \{x,y\}$
j) $A - A = \emptyset$

136 Indiqueu si l'afirmació $a \notin \{1,2\}$ equival a alguna de les següents:

a) $a \neq 1 \wedge a \neq 2$
b) $a \neq 1 \vee a \neq 2$

136* *Resposta:* Equival a $a \neq 1 \wedge a \neq 2$.

137 Indiqueu si és cert:

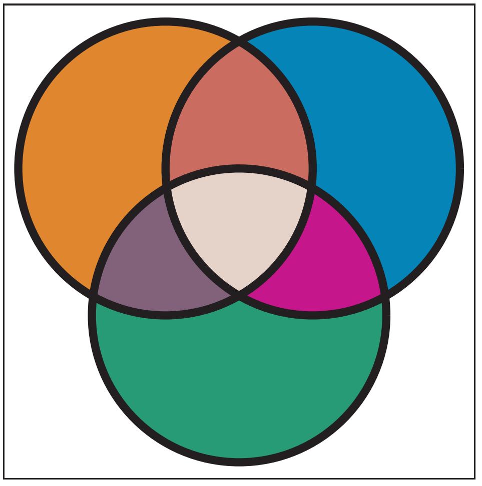
$$(x,y) \neq (z,t) \Rightarrow (x \neq z \wedge y \neq t).$$

137* *Resposta:* Comentari. La igualtat de parells ordenats es formalitza:

$$(x,y) = (z,t) \leftrightarrow (x = z \wedge y = t).$$

La negació és:

$$((x,y) \neq (z,t) \not\leftrightarrow (x \neq z \vee y \neq t)).$$



→ 9

Fórmula del binomi de Newton

En aquest capítol, presentem la fórmula del binomi de Newton, amb diversos exemples d'ús per a resoldre alguns problems de sumació i alguns problemes de divisibilitat, tot i que aquests últims és possible que també es puguin resoldre per altres mètodes. En alguns casos, ja se n'han vist propietats i definicions al capítol de preliminars.
Molts dels problemes que es resolen aquí també es poden resoldre **per inducció** (per a nombres naturals) o altres mètodes. Convidem el lector a intentar resoldre per inducció, si és possible, la demostració dels enunciats que es presenten aquí.

9.1. Factorials i nombres binomials

Recordem-ne algunes definicions i propietats bàsiques:

Factorial de *n*, nombre natural

$$n! = \begin{cases} 1 \cdot 2 \cdots n, & \text{si } n \geq 1 \\ 1, & \text{si } n = 0 \end{cases}$$

El nombre combinatori $\binom{n}{k}$ es defineix de manera general, per a $n \geq 0$, com:

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } n \geq 0; 0 \leq k \leq n \\ 0 & \text{si } n \geq 0; (k < 0 \text{ o } k > n) \end{cases}$$

No oblidem que $\binom{n}{k}$ sempre és un nombre natural. És el nombre de subconjunts de k elements que es poden formar a partir d'un conjunt de n elements: per tant, és un nombre natural.

Vegem-ne uns quants exemples:

Exemple 9.1

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{1 \cdot n!} = 1$$

$$\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n \cdot (n-1)!}{1 \cdot (n-1)!} = \frac{n}{1} = n$$

$$\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)(n-2)!}{2!(n-2)!} = \frac{n(n-1)}{2!} = \frac{n(n-1)}{2}$$

$$\binom{n}{3} = \frac{n!}{3!(n-3)!} = \frac{n(n-1)(n-2)(n-3)!}{3!(n-3)!} = \frac{n(n-1)(n-2)}{3!} = \frac{n(n-1)(n-2)}{6}$$

$\ldots$

$$\binom{n}{(n-1)} = \frac{n!}{(n-1)!(n-(n-1))!} = \frac{n!}{(n-1)!1!} = n$$

$$\binom{n}{n} = \frac{n!}{(n)!(n-n)!} = \frac{n!}{n!0!} = 1. \blacksquare$$

Exemple 9.2 En concret,

$$\binom{7}{4} = \frac{7!}{4!(7-4)!} = \frac{7!}{4!3!} = \frac{7 \cdot 6 \cdot 5 \cdot 4!}{4!3!} = \frac{7 \cdot 6 \cdot 5}{3!} = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} = 7 \cdot 5 = 35. \blacksquare$$

Com a exemples addicionals, calculem tots els coeficients binomials per a $n = 5$:

Exemple 9.3

$$\binom{5}{0} = \frac{5!}{0!(5-0)!} = 1$$

$$\binom{5}{1} = \frac{5!}{1!(5-1)!} = \frac{5 \cdot 4!}{4!} = 5$$

$$\binom{5}{2} = \frac{5!}{2!(5-2)!} = \frac{5!}{2!3!} = \frac{5 \cdot 4 \cdot 3!}{2!3!} = \frac{5 \cdot 4}{2!} = 10$$

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5!}{3!2!} = \frac{5 \cdot 4 \cdot 3!}{3!2!} = \frac{5 \cdot 4}{2!} = 10$$

$$\binom{5}{4} = \frac{5!}{4!(5-4)!} = \frac{5!}{4!1!} = \frac{5 \cdot 4!}{4!1!} = 5$$

$$\binom{5}{5} = \frac{5!}{5!(5-5)!} = \frac{5!}{5!0!} = 1$$

$\blacksquare$

Segueixen ara algunes fórmules relacionades amb els nombres combinatoris o coeficients binomials.

Recordem que $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$, per a n,k naturals, amb $n \geq k \geq 0$, amb $0! = 1$.

Hi ha unes propietats trivials: $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = n$, de comprovació immediata.

Indiquem només uns resultats que poden ser útils (d'entre els molts possibles).

Teorema 9.1 (simetria) *Es compleix:* $\binom{n}{k} = \binom{n}{n-k}$.

Demostració. Es poden plantejar demostracions aritmètiques, basades en la simple comprovació, o bé demostracions combinatòries, basades en el significat combinatori dels coeficients binomials que apareixen a la fórmula.

Mètode 1: directament. Es tracta de desenvolupar les fórmules.

Un simple càlcul demostraria la propietat:

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Mètode 2: per arguments combinatoris. Utilitzarem el significat combinatori dels coeficients binomials que apareixen a la fórmula; en concret, que $\binom{n}{k}$ és el nombre de subconjunts de k elements d'un conjunt de n elements.

Es pot formular un argument combinatori: escollir k elements d'un conjunt de n equival a no escollir-ne $n-k$, la resta (o, el que és equivalent, escollir-ne $n-k$ per a no ser seleccionats, per deixar-los fora!); el nombre de maneres de fer això és, respectivament, $\binom{n}{k}$ i $\binom{n}{n-k}$, que han de coincidir per l'argument anterior. També es pot veure de la manera següent: construint un conjunt de k elements d'entre n, resulta, al mateix temps, construït el complementari, de $n-k$ elements.

Exemple 9.4 Vegem com es poden obtenir alguns nombres binomials, sense calcular, a partir de nombres binomials ja calculats, utilitzant la propietat de simetria:

$$\binom{5}{3} = \binom{5}{5-3} = \binom{5}{2} = 10$$

$$\binom{5}{4} = \binom{5}{5-4} = \binom{5}{1} = 5$$

$$\binom{5}{5} = \binom{5}{5-5} = \binom{5}{0} = 1. \blacksquare$$

Exemple 9.5 Si n és senar, proveu que $\binom{n}{\frac{n-1}{2}} = \binom{n}{\frac{n+1}{2}}$. En efecte, aplicant la propietat de simetria, $\binom{n}{\frac{n-1}{2}} = \binom{n}{n-\frac{n-1}{2}} = \binom{n}{\frac{2n-n+1}{2}} = \binom{n}{\frac{n+1}{2}}$. $\blacksquare$

Teorema 9.2 (fórmula recursiva) *Es compleix:* $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Demostració. Es poden plantejar demostracions aritmètiques, basades en la simple comprovació, o bé demostracions combinatòries, basades en el significat combinatori dels coeficients binomials que apareixen a les fórmules.

Mètode 1: directament. Es tracta de desenvolupar les fórmules.

Un simple càlcul demostraria la propietat:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} =$$
$$= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{1}{k} + \frac{1}{n-k}\right) =$$
$$= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{n}{k(n-k)}\right) = \frac{n!}{k!(n-k)!}.$$

Mètode 2: per arguments combinatoris. Utilitzem el significat combinatori dels coeficients binomials que apareixen a la fórmula; en concret, que $\binom{n}{k}$ és el nombre de subconjunts de k elements d'un conjunt de n elements.

Considerem la primera fórmula. Suposem que $n \geq k \geq 0$. Sigui A un conjunt de cardinal $|A| = n$ i sigui $a \in A$ un element arbitrari, però fix. Ara considerem els subconjunts de cardinal k que no contenen a:

$P_0 = \{S \in \mathscr{P}_k(A) | \, a \notin S\}$

i el complementari a $\mathscr{P}_k(A)$:

$P_1 = \mathscr{P}_k(A) - P_0 = \{S \in \mathscr{P}_k(A) | \, a \in S\}$

Aleshores, $\mathscr{P}_k(A) = P_0 \cup P_1$, $P_0 \cap P_1 = \emptyset$ i, per tant, $|\mathscr{P}_k(A)| = |P_0 \cup P_1| = |P_0| + |P_1|$. Calculem cadascun d'aquests cardinals:

– Ja sabem que $|\mathscr{P}_k(A)| = \binom{n}{k}$.
– $|P_0|$ és el nombre de subconjunts de k elements que es poden formar a partir dels elements del conjunt $A - \{a\}$, conjunt de $n-1$ elements, ja que a n'està exclòs. O bé és el conjunt de les combinacions que es poden formar de k elements a partir d'un conjunt de $n-1$ elements disponibles. La resposta és $|P_0| = \binom{n-1}{k}$.
– $|P_1|$? Els elements de P_1 contenen l'element a fix i, en ser de cardinal k, es poden formar escollint $k-1$ elements d'entre tots els disponibles, llevat de a, que ja hi és. Per tant, fixat a, se'n poden triar $k-1$ d'entre $n-1$. És $|P_1| = \binom{n-1}{k-1}$.

Substituint, s'obté la igualtat buscada.

La fórmula $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ pot utilitzar-se en demostracions inductives. A nivell de programació, és la base per al càlcul recursiu dels nombres combinatoris.

Quina és la fórmula del binomi de Newton?

9.2. La fórmula del binomi de Newton

Teorema 9.3 *Siguin $x, y \in \mathbb{R}$, i sigui $n \in \mathbb{N}$. Aleshores:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j \tag{9.1}$$

Demostració. Diverses demostracions són possibles. Per exemple, **per inducció**, metodologia que s'ha presentat en un altre capítol. Vegem aquesta demostració per inducció:

Demostració inductiva de la fórmula del binomi de Newton

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k, \quad x, y \in \mathbb{R}, n \in \mathbb{N}$$

Equivalentment, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

Demostrem-la per inducció sobre n, amb valor inicial $n_0 = 1$ (també vàlid per a $n = 0$).

Pas base. Per a $n = 1$, es comprova immediatament, ja que

$$(x+y)^1 = \binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1.$$

Pas inductiu (segons la variant $(P(n) \Longrightarrow P(n+1))$, per a tot $n \geq 1$.). Suposem que la igualtat es compleix per a n, és a dir, que la *hipòtesi d'inducció* és

$$(x+y)^n \overset{(HI)}{=} \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Hem de provar:

$$(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k.$$

Per a això, multipliquem ambdós membres de la igualtat de la hipòtesi d'inducció (HI) per $x+y$:

$$
\begin{aligned}
(x+y)^{n+1} &= (x+y)^n(x+y) = (\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k)(x+y)\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k x + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k y\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1}\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=1}^{n+1}\binom{n}{k-1}x^{n-k+1}y^k\\
&= x^{n+1} + (\sum_{k=1}^{n}(\binom{n}{k} + \binom{n}{k-1})x^{n-k+1}y^k) + y^{n+1}\\
&\overset{(*)}{=} x^{n+1} + (\sum_{k=1}^{n}\binom{n+1}{k}x^{n-k+1}y^k) + y^{n+1}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{(n+1)-k}y^k
\end{aligned}
$$

Observem que s'ha utilitzat a (*) la identitat combinatòria que hem anteriorment:

$$\binom{r}{k} + \binom{r}{k-1} \overset{(*)}{=} \binom{r+1}{k}.$$

Exemple 9.6

$(a+b)^3 = \binom{3}{0}a^0b^3 + \binom{3}{1}a^1b^2 + \binom{3}{2}a^2b^1 + \binom{3}{3}a^3b^0 = b^3 + 3ab^2 + 3a^2b + a^3$. ■

Exemple 9.7 Quin és el coeficient de x^2y^3 en el desenvolupament de $(x+y)^5$? Observem que $n = 2+3 = 5$. A la fórmula del binomi de Newton, el terme apareix com $\binom{5}{2}x^2y^{5-2} = 10x^2y^3$. ■

Fórmules derivades de la fórmula del binomi de Newton

Prenent valors concrets per a x, y, s'obtenen fórmules especials. Vegem-e alguns exemples.

Exemple 9.8 Fent $x = y = 1$, resulta una fórmula per a la suma dels coeficients binomials $\sum_{k=0}^{n}\binom{n}{k} = (1+1)^n = 2^n$. És a dir:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n. ■$$

Exemple 9.9 *Suma alternada dels coeficients binomials*

Escollint $x = -1, y = 1$, resulta $0 = (-1+1)^n = \sum_{k=0}^{n}\binom{n}{k}(-1)^k$. ■

Exemple 9.10 *Noves fórmules per integració i derivació.*

Particularitzant a $y = 1$, podem considerar la fórmula resultant $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ en què ambdós membres són funcions derivables respecte de la variable x, i integrables. Derivant o integrant, s'obtenen noves identitats. ■

Demostració de la fórmula del cardinal del conjunt de les parts

Utilitzem aquest resultat per obtenir una demostració sobre el cardinal del conjunt de les parts d'un conjunt A de cardinal n.

Teorema 9.4 *A conjunt* $, |A| < \infty \Longrightarrow |\mathscr{P}(A)| = 2^{|A|}$.

Demostració. Aquesta és una demostració de característiques netament combinatòries.

En efecte, si $\mathscr{P}_k(A)$ és el conjunt de subconjunts de cardinal k, tenim que podem expressar $\mathscr{P}(A)$ com a reunió disjunta d'aquests subconjunts, és a dir, $\mathscr{P}(A) = \bigcup_{k=0}^{n} \mathscr{P}_k(A)$. Calculant els cardinals, és $|\mathscr{P}(A)| = |\bigcup_{k=0}^{n} \mathscr{P}_k(A)| = \sum_{k=0}^{n} |\mathscr{P}_k(A)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n$. Observeu que $\mathscr{P}_0(A) = \{\emptyset\}$, de cardinal $\binom{n}{0} = 1$, $\mathscr{P}_1(A) = \{\{a\}, \{b\}, \cdots\}$, conjunt dels subconjunts d'un element, i així successivament.

9.3. Problemes diversos

PROBLEMA 9.1

Sigui n un nombre natural.

Obtingueu una expressió de $\sum_{k=0}^{n} \binom{n}{k} 4^k$ *sense sumatoris.*

Anàlogament per a l'expressió $\sum_{k=4}^{n} \binom{n}{k} 7^k$, *per a* $n \geq 4$. *Sumeu*

$$S_1 = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^k} \qquad S_2 = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{\sqrt{3^k}} \qquad S_3 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 2^k.$$

Solució. *Idea de resolució*. Atesa la similitud amb la fórmula del binomi de Newton, vegem com podem convertir el problema en el d'aplicar la fórmula esmentada.

Anàlisi. L'expressió a sumar es pot escriure com un cas particular de la fórmula del binomi de Newton. En efecte, si a

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ fem $b=1$, aleshores, l'expressió de la dreta resulta

$$\sum_{k=0}^{n} \binom{n}{k} a^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^k,$$

que és del tipus de la del nostre problema. I és, doncs, $\sum_{k=0}^{n} \binom{n}{k} a^k = (a+1)^n$.

Resolució. Per tant, en el nostre problema, prenent $a=4$, $b=1$, resulta

$$\sum_{k=0}^{n} \binom{n}{k} 4^k = \sum_{k=0}^{n} \binom{n}{k} 4^k 1^{n-k} = (4+1)^n = 5^n.$$

Per a l'altra expressió es procedeix de manera similar (amb $a=7$, $b=1$):

$$\sum_{k=4}^{n} \binom{n}{k} 7^k = \sum_{k=0}^{n} \binom{n}{k} 7^k - \sum_{k=0}^{3} \binom{n}{k} 7^k = (7+1)^n - \sum_{k=0}^{3} \binom{n}{k} 7^k = 8^n - (\binom{n}{0} 7^0 +$$
$$+\binom{n}{1} 7^1 + \binom{n}{2} 7^2 + \binom{n}{3} 7^3) = 8^n - 1 - n7 - \frac{n(n-1)}{2} 7^2 - \frac{n(n-1)(n-2)}{6} 7^3.$$

Vegem les altres sumes:

$S_1 = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^k} = \sum_{k=0}^{n} \binom{n}{k} (\frac{1}{2})^k$. És un cas particular de la fórmula general, amb $a = \frac{1}{2}$, $b=1$. Per tant, $S_1 = (\frac{1}{2}+1)^n = (\frac{3}{2})^n$.

$S_2 = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{(\sqrt{3})^k} = \sum_{k=0}^{n} \binom{n}{k} (\frac{1}{\sqrt{3}})^k$. És un cas particular de la fórmula general, amb $a = \frac{1}{\sqrt{3}}$, $b=1$. Per tant, $S_1 = (\frac{1}{\sqrt{3}}+1)^n$.

$S_3 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 2^k = \sum_{k=0}^{n} \binom{n}{k} (-2)^k = (-2+1)^n = (-1)^n$, amb $a=-2$, $b=1$.

PROBLEMA 9.2

Sigui n un nombre natural qualsevol. Proveu que $6|7^n - 1$. *Apliqueu la fórmula del binomi de Newton.*

Podeu generar nous enunciats similars que es puguin resoldre pel mateix mètode?

Solució. *Idea per a la resolució*. Expressem $7 = 6+1$ amb l'objectiu de desenvolupar $7^n = (6+1)^n$ per la fórmula del binomi de Newton, i això amb l'objectiu últim d'obtenir així factors 6 i poder demostrar finalment que $7^n - 1 = 6k$ per a un determinat enter k.

Resolució. Per a $n = 0$, substituint resulta $6|7^0 - 1 = 1 - 1 = 0$. Suposem, per tant, que $n \geq 1$.

$$7^n - 1 = (6+1)^n - 1 = (\sum_{j=0}^{n} \binom{n}{j} 6^j 1^{n-j}) - 1 = (\sum_{j=0}^{n} \binom{n}{j} 6^j) - 1 = \binom{n}{0} 6^0 + (\sum_{j=1}^{n} \binom{n}{j} 6^j) - 1 = 1 + (6\sum_{j=1}^{n} \binom{n}{j} 6^{j-1}) - 1 = 6\sum_{j=1}^{n} \binom{n}{j} 6^{j-1} = 6k, \text{ amb } k = \sum_{j=1}^{n} \binom{n}{j} 6^{j-1} \in \mathbb{Z}.$$

Què passa si desenvolupem seguint l'ordre dels sumands $(1+6)^n$? S'obté el mateix, tot i que en un altre ordre dels sumands del desenvolupament, i resulta menys còmode per al que ens interessa, ja que seria $(1+6)^n = \sum_{j=0}^{n} \binom{n}{j} 1^k 6^{n-k}$.

Nous enunciats. Podem donar una quantitat important de resultats similars, que es demostrarien similarment:

$a|(a+1)^n - 1,\ a \geq 1$

$2|3^n - 1$

$3|4^n - 1$

$4|5^n - 1$

$5|6^n - 1$

...

$31|(32)^n - 1$

...

PROBLEMA 9.3

Sigui n un nombre natural qualsevol. Proveu que $4|9^n + 3$. *Apliqueu la fórmula del binomi de Newton*.

Observació. Es pot resoldre per inducció o altres mètodes.

Solució. *Objectiu*. Hem d'arribar a la conclusió que existeix $k \in \mathbb{Z}$ tal que $9^n + 3 = 4k$. Per a $n = 0$, resulta obvi per simple substitució: $9^n + 3 = 9^0 + 3 = 1 + 3 = 4$. Suposem, doncs, que $n \geq 1$.

Idea per a la resolució. Amb la idea d'aplicar la fórmula del binomi de Newton, i amb l'objectiu d'obtenir factors 4, considerem possibles descomposicions:

$9 = 4 + 5$, $9 = 4 \times 2 + 1$, $9 = 4 \times 3 - 3$ o altres. Això donarà lloc a diverses variants argumentals.

Vegem la primera $(9 = 4 + 5)$.

$$9^n + 3 = (4+5)^n + 3 = \sum_{j=0}^{n} \binom{n}{j} 4^j 5^{n-j} + 3 = \binom{n}{0} 4^0 5^{n-0} + \sum_{j=1}^{n} \binom{n}{j} 4^j 5^{n-j} + 3 = 5^n + 4\sum_{j=1}^{n} \binom{n}{j} 4^{j-1} 5^{n-j} + 3 = 5^n + 4k_1 + 3, \text{ amb } k_1 = \sum_{j=1}^{n} \binom{n}{j} 4^{j-1} 5^{n-j}.$$

Tornem a aplicar la fórmula del binomi de Newton a

$$5^n = (4+1)^n = \sum_{j=0}^{n} \binom{n}{j} 4^j 1^{n-j} = \sum_{j=0}^{n} \binom{n}{j} 4^j =$$

$$\binom{n}{0} 4^0 + \sum_{j=1}^{n} \binom{n}{j} 4^j = 1 + 4\sum_{j=1}^{n} \binom{n}{j} 4^{j-1} = 1 + 4k_2,$$

amb $k_2 = \sum_{j=1}^{n} \binom{n}{j} 4^{j-1}$.

Finalment, $9^n + 3 = (1 + 4k_2) + (4k_1 + 3) = 4k_1 + 4k_2 + 4 = 4(k_1 + k_2 + 1) = 4k$, amb $k = k_1 + k_2 + 1 \in \mathbb{Z}$.

És preferible la segona descomposició, ja que obtindrem el que volem amb una sola expressió, tot d'un cop.

Vegem la segona $(9 = 4 \times 2 + 1)$. Es procediria de manera similar:

$$9^n + 3 = (2 \cdot 4 + 1)^n + 3 = \sum_{j=0}^{n} \binom{n}{j} 2^j 4^j 1^{n-j} + 3 = \sum_{j=0}^{n} \binom{n}{j} 2^j 4^j + 3$$

$$= \binom{n}{0} 2^0 4^0 + \sum_{j=1}^{n} \binom{n}{j} 2^j 4^j + 3 = 1 + 4\sum_{j=1}^{n} \binom{n}{j} 4^{j-1} 2^j + 3 = 1 + 4m_1 + 3 = 4 + 4m_1 =$$

$4(1 + m_1) = 4k$, amb $m_1 = \sum_{j=1}^{n} \binom{n}{j} 4^{j-1} 2^j$ i $k = 1 + m_1 \in \mathbb{Z}$.

També amb la *tercera* es procediria anàlogament (exercici).

PROBLEMA 9.4

Proveu que, per a tot n natural, es compleix:

$3 | 2^{2n+1} + 1$.

Solució. *Què és el que hem de veure?* Que podem escriure $2^{2n+1} + 1 = 3\alpha$, per a algun α enter convenient. Aquesta és la idea que ha de guiar la resolució. Vegem que es pot fer per un mètode directe, tot i que són possibles diversos mètodes de resolució.

Per $n = 0$, per substitució en resulta directament la conclusió. Sigui $n \geq 1$.

En primer lloc, efectuem algunes manipulacions de la fórmula anterior per veure si en resulta alguna idea de resolució. És $2^{2n+1} + 1 = 2^{2n}2 + 1 = 2 \cdot (2^2)^n + 1 = 2 \cdot 4^n + 1$. Necessitem efectuar algun desenvolupament que introdueixi factors 3 a la fórmula; *una possible idea és fer la descomposició* $4 = 3 + 1$ *i després desenvolupar pel binomi de Newton, fórmula en la qual apareixeran factors 3*. Altres expressions possibles, tals com $4 = 2 + 2, 4 = 1 + 1 + 2$, no sembla que aportin res d'interessant amb relació al problema.

Així, amb l'objectiu de desenvolupar per la fórmula del binomi de Newton, escrivim $4 = 3+1$ i, per tant, $2\cdot 4^n + 1 = 2\cdot(3+1)^n + 1$. En conseqüència,

$$2^{2n+1}+1 = 2\cdot(3+1)^n + 1 = 2\cdot\sum_{j=0}^{n}\binom{n}{j}3^j 1^{n-j}+1 =$$

$$2\cdot\sum_{j=0}^{n}\binom{n}{j}3^j+1 = 2(1+\sum_{j=1}^{n}\binom{n}{j}3^j)+1 = 2(1+3\sum_{j=1}^{n}\binom{n}{j}3^{j-1})+1 = 2(1+3q)+1,$$

per a $q = \sum_{j=1}^{n}\binom{n}{j}3^{j-1}$, enter. Per tant, $2^{2n+1}+1 = 2(1+3q)+1 = 2+6q+1 = 3+6q = 3(1+2q) = 3q'$, múltiple de 3, amb $q' = 1+2q$.

Observació. Altres mètodes de resolució possibles: per inducció, per congruències, per classes de residus.

PROBLEMA 9.5

Sigui x un nombre real. Vegeu que, per a tot n natural no nul, es compleix: $x-1 | x^n - 1$.

Solució. Si $x = 1$, és obvi. Suposem $x \neq 1$.

La idea és aplicar la fórmula del binomi de Newton, per tal d'obtenir el factor $x-1$ en el desenvolupament de $x^n - 1$, que haurem de reescriure per tal que es pugui utilitzar la fórmula. L'escriurem en termes de $x-1$, amb l'objectiu que hi aparegui com a factor quan posteriorment es desenvolupi per la fórmula del binomi de Newton.

Fem $x = (x-1)+1$.

Així, tindrem:

$$x^n - 1 = ((x-1)+1)^n - 1 = (\sum_{j=0}^{n}\binom{n}{j}(x-1)^j 1^{n-j}) - 1 = (\sum_{j=0}^{n}\binom{n}{j}(x-1)^j) - 1 =$$

$$(\binom{n}{0}(x-1)^0 + \sum_{j=1}^{n}\binom{n}{j}(x-1)^j) - 1 = 1 + \sum_{j=1}^{n}\binom{n}{j}(x-1)^j - 1 = \sum_{j=1}^{n}\binom{n}{j}(x-1)^j =$$

$$\sum_{j=1}^{n}\binom{n}{j}(x-1)(x-1)^{j-1} = (x-1)\sum_{j=1}^{n}\binom{n}{j}(x-1)^{j-1}.$$

Ara, amb $q = \sum_{j=1}^{n}\binom{n}{j}(x-1)^{j-1} \in \mathbb{Z}$, és $x^n - 1 = (x-1)q$, múltiple de $x-1$.

Observació. Es pot demostrar per altres mètodes: per inducció, per la fórmula 10.1.

PROBLEMA 9.6

Sigui n un nombre natural. Demostreu:

$3|(3n+1)^{2348}+(3n+1)^{29}+1.$

Solució. En primer lloc, si $n=0$, per substitució a la fórmula es comprova $(3\cdot 0+1)^{2348}+(3\cdot 0+1)^{29}+1=3$. Suposem $n\geq 1$.

Utilitzarem la fórmula del binomi de Newton. L'***objectiu*** és veure que podem escriure $(3n+1)^{2348}+(3n+1)^{29}+1=3k$ per a un k enter adequat (natural, en aquest cas). Treballarem separadament en els dos primers sumands:

$$(3n+1)^{2348}=\sum_{j=0}^{2348}\binom{2348}{j}(3n)^j 1^{2348-j}=\sum_{j=0}^{2348}\binom{2348}{j}3^j n^j$$

Observem que els termes 3^j aporten factors 3, que ens calen, excepte en el cas $j=0$, ja que aleshores és $3^0=1$. Separem, per aquest motiu, el sumand corresponent. El mateix farem amb el desenvolupament de l'altre sumand, $(3n+1)^{29}$.

Així,

$$(3n+1)^{2348}=\sum_{j=0}^{2348}\binom{2348}{j}3^j n^j=\binom{2348}{0}3^0 n^0+\sum_{j=1}^{2348}\binom{2348}{j}3^j n^j=$$

$$1+3\sum_{j=1}^{2348}\binom{2348}{j}3^{j-1}n^j \text{ (observem que } j-1\geq 0).$$

Amb $k_1=\sum_{j=1}^{2348}\binom{2348}{j}3^{j-1}n^j\in\mathbb{Z}$, resulta $(3n+1)^{2348}=1+3k_1$, per a $k_1\in\mathbb{Z}$.

Anàlogament, tenim $(3n+1)^{29}=\sum_{j=0}^{29}\binom{29}{j}(3n)^j 1^{29-j}=\sum_{j=0}^{29}\binom{29}{j}3^j n^j=\binom{29}{0}3^0 n^0+$ $\sum_{j=1}^{29}\binom{2348}{j}3^j n^j=1+3\sum_{j=1}^{29}\binom{29}{j}3^{j-1}n^j=1+3k_2$, amb $k_2=\sum_{j=1}^{29}\binom{29}{j}3^{j-1}n^j\in\mathbb{Z}$.

Finalment, $(3n+1)^{2348}+(3n+1)^{29}+1=(1+3k_1)+(1+3k_2)+1=3k_1+3k_2+3=3(k_1+k_2+1)=3k$, amb $k=k_1+k_2+1$. Per tant, $(3n+1)^{2348}+(3n+1)^{29}+1$ és múltiple de 3.

PROBLEMA 9.7

Sigui n un nombre enter. Proveu que $2\nmid n\Rightarrow 2\nmid n^{23}$.

Solució. *Anàlisi de l'enunciat*. Observeu que és el mateix que dir:

"Si n és senar, aleshores n^{23} és senar".

"Si n és de la forma $n = 2k+1$, per a un k enter convenient, aleshores n^{23} és $n^{23} = 2k'+1$ per a un cert enter k'".

Mètode de demostració. Es pot fer una *demostració directa*, provant:

$\exists k(k \in \mathbb{Z} \wedge n = 2k+1) \Rightarrow \exists k'(k' \in \mathbb{Z} \wedge n^{23} = 2k'+1)$.

Hipòtesi (H): $\exists k(k \in \mathbb{Z} \wedge n = 2k+1)$

Tesi (T): $\exists k'(k' \in \mathbb{Z} \wedge n^{23} = 2k'+1)$

Esquema: H $\Rightarrow$ T

Aquesta implicació $\exists k(k \in \mathbb{Z} \wedge n = 2k+1) \Rightarrow \exists k'(k' \in \mathbb{Z} \wedge n^{23} = 2k'+1)$ és la que *guia* la demostració.

Idea de la resolució, concretada. Evidentment, la idea és que, en aplicació de la hipòtesi, substituirem i calcularem $n^{23} = (2k+1)^{23}$. En casos d'exponent alt, ja no és factible o recomanable efectuar manualment els càlculs corresponents: $(2k+1)\cdots(2k+1)$, atesa la possibilitat d'errors; en altres casos, ja no serà possible, per exemple ,si l'exponent és genèric, com seria a $2 \nmid n \Rightarrow 2 \nmid n^m$, per a m natural positiu.

En aquests casos, és convenient utilitzar la fórmula del binomi de Newton, que permet sistematitzar i facilitar el càlcul o desenvolupament.

Resolució. Com aplicar la hipòtesi? Substituint n per $2k+1$.

En aplicació de la hipòtesi, doncs, escrivim $n^{23} = (2k+1)^{23}$ i ara

$$n^{23} = (2k+1)^{23} = \sum_{j=0}^{23} \binom{23}{j} (2k)^j 1^{23-j} = \sum_{j=0}^{23} \binom{23}{j} 2^j k^j$$

No oblidem que perseguim expressar aquesta última fórmula com a "múltiple de 2 més 1". Formalment, tots els sumands tenen el factor 2^j, que donarà lloc a factors 2 i, per tant, sumands múltiples de 2, per a $j \geq 1$, però no per a $j = 0$, cosa que suggereix la descomposició:

$$n^{23} = \binom{23}{0} 2^0 k^0 + \sum_{j=1}^{23} \binom{23}{j} 2^j k^j = 1 + \sum_{j=1}^{23} \binom{23}{j} 2^{1+(j-1)} k^j$$

$$= 1 + \sum_{j=1}^{23} \binom{23}{j} 2 \cdot 2^{(j-1)} k^j = 1 + 2\sum_{j=1}^{23} \binom{23}{j} 2^{(j-1)} k^j = 1 + 2k',$$

amb $k' = \sum_{j=1}^{23} \binom{23}{j} 2^{(j-1)} k^j$, enter.

Per tant, n^{23} és senar.

Detallem l'estructura demostrativa. A través dels passos següents, encadenats:

P_1: $2 \nmid n$ (hi ha dues maneres de no ser parell: ser de la forma $2k+1$ i de la forma $2k-1$)

P_2: $\exists k(k \in \mathbb{Z} \wedge n = 2k+1)$ (reescriptura de la hipòtesi)

P_3: $\exists k(k \in \mathbb{Z} \wedge n^{23} = (2k+1)^{23})$

Càlculs intermedis (realitzats anteriorment):

$n^{23} = \cdots = 1 + 2k'$, amb $k' = \displaystyle\sum_{j=1}^{23} \binom{23}{j} 2^{(j-1)} k^j \in \mathbb{Z}$

P_4: $\exists k'(k' \in \mathbb{Z} \wedge n^{23} = 2k' + 1)$

P_5: $2 \nmid n^{23}$

Tenim: $P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow P_4 \Rightarrow P_5$

Finalment, $P_1 \Rightarrow P_5$

Ampliació: es podria generalitzar? Certament:

$\forall n(n \in \mathbb{Z} \rightarrow (2 \nmid n \rightarrow 2 \nmid n^{23}))$

$\forall n((n \in \mathbb{Z} \wedge 2 \nmid n) \rightarrow 2 \nmid n^{23})$

$\forall n \in \mathbb{Z}(2 \nmid n \rightarrow 2 \nmid n^{23})$ (semiformal)

$\forall n(2 \nmid n \rightarrow 2 \nmid n^{23})$ (suposant la pertinença de n a l'universal $U = \mathbb{Z}$)

Variant argumental: què passaria si expresséssim que un nombre senar és (també) de la forma $2k-1$. L'argument funciona de manera anàloga:

Sigui $n = 2q - 1$, per a un q enter adequat. Vegem que $n^{23} = 2q' - 1$ per a algun q' enter convenient (o $2q'' + 1$ per a algun enter q'').

$$n^{23} = (2q-1)^{23} = \sum_{j=0}^{23} \binom{23}{j} (2q)^j (-1)^{23-j} = \binom{23}{0} (2q)^0 (-1)^{23-0} +$$

$$\sum_{j=1}^{23} \binom{23}{j} (2q)^j (-1)^{23-j} = -1 + 2\sum_{j=1}^{23} \binom{23}{j} 2^{j-1} q^j (-1)^{23-j} = -1 + 2q',$$

amb l'enter $q' = \displaystyle\sum_{j=1}^{23} \binom{23}{j} 2^{j-1} q^j (-1)^{23-j}$. Per tant, $n^{23} = 2q' - 1$, senar.

Es podria provar per altres mètodes?

► ***Pel contrarecíproc***: $2|n^{23} \Rightarrow 2|n$. Ara no ho detallarem aquí, ja que no permet il·lustrar l'ús de la fórmula del binomi de Newton, que és el nostre objectiu en aquest capítol. Una idea possible és fer servir el lema d'Euclides: "Si un nombre primer divideix un producte de dos factors, ha de dividir algun dels factors", generalitzable a més factors.

El contrarecíproc també es podria demostrar per reducció a l'absurd, i resultaria de fet, com el desenvolupament següent.

► Es pot demostrar ***per reducció a l'absurd***. Neguem $2 \nmid n \Rightarrow 2 \nmid n^{23}$ o, millor encara, neguem $\forall n(2 \nmid n \rightarrow 2 \nmid n^{23})$ i arribem a una contradicció. En efecte, suposem que per, a algun n enter:

$2 \nmid n$ i $2|n^{23}$

Aleshores existeix k enter tal que $n = 2k+1$ i existeix k' enter tal que $n^{23} = 2k'$. És a dir, existeixen enters k, k' tals que $n = 2k+1$ i $n^{23} = 2k'$. Per tant, substituint i fent servir desenvolupaments anteriors:

$$2k' = n^{23} = (2k+1)^{23} = \sum_{j=0}^{23} \binom{23}{j} (2k)^j 1^{23-j} = 1 + 2k'', \text{ amb } k'' \in \mathbb{Z}.$$

Per tant, $2k' = 2k'' + 1$, d'on $2(k' - k'') = 1$, d'on 1 és parell, la qual cosa és una contradicció.

► Com a cas particular del resultat: "El producte de senars és senar", demostrat en altres contextos. En efecte, si n és senar, n^{23}, producte de senars, és senar.

PROBLEMA 9.8

Siguin a un nombre enter i m un nombre natural, $m \geq 1$. Demostreu $2 \nmid a \Rightarrow 2 \nmid a^m$.

Solució. És similar a l'exercici anterior 9.7. Només interessa observar que és gairebé obligat aquí, amb un exponent arbitrari, utilitzar la fórmula del binomi de Newton.

Vegem que, si existeix $k \in \mathbb{Z}$ tal que $a = 2k+1$, aleshores existeix $k' \in \mathbb{Z}$ tal que $a^m = 2k'+1$:

$$a^m = (2k+1)^m = \sum_{j=0}^{m} \binom{m}{j} (2k)^j 1^{m-j} = \sum_{j=0}^{m} \binom{m}{j} 2^j k^j = \binom{m}{0} 2^0 k^0 + \sum_{j=1}^{m} \binom{m}{j} 2^j k^j = 1 + \sum_{j=1}^{m} \binom{m}{j} 2^{1+(j-1)} k^j = 1 + \sum_{j=1}^{m} \binom{m}{j} 2 \cdot 2^{(j-1)} k^j = 1 + 2\sum_{j=1}^{m} \binom{m}{j} 2^{(j-1)} k^j = 1 + 2k', \text{ amb } k' = \sum_{j=1}^{m} \binom{m}{j} 2^{(j-1)} k^j, \text{ enter.}$$

Observació. Si s'ha demostrat el resultat "el producte de senars és senar", aleshores n'és un cas particular, amb el nombre senar repetit m vegades.

PROBLEMA 9.9

Sigui n un nombre enter. Proveu $3 \nmid n \Rightarrow 3 \nmid n^{3251}$.

Solució. *Mètode de demostració*. En fem una demostració directa.

Discussió preliminar. Però, per a això, hem de saber contestar a la pregunta: Si un nombre enter no és múltiple de 3, com es pot escriure o descriure? De quines maneres pot ser un nombre no múltiple de 3?

La idea és considerar la divisió entera de n per 3 i veure les possibilitats per al residu de la divisió: és $n = 3q + r$, amb $0 \leq r < 3$. Així, equivalentment, ja que r és enter, $0 \leq r \leq 3 - 1 = 2$. Per tant, $r = 0$ o $r = 1$ o $r = 2$. El cas $r = 0$, és a dir, $n = 3q$ correspon a la divisibilitat, és a dir, $3|n$. La resta de casos a no ser divisible per 3, és a dir, $3 \nmid n$. En efecte, vegem-ho, per exemple, per a $r = 1$: si fos $3|n$ amb $n = 3q+1$, seria $3k = n = 3q+1$ per a algun enter k, d'on $3(k-q) = 1$, d'on $3|1$, cosa absurda; anàlogament per a $r = 2$.

Resolució (per casos). Això donarà lloc a una *demostració per casos*. Apliquem la fórmula del binomi de Newton.

Cas 1. ($r = 1$). Sigui, doncs, $n = 3q+1$ per a algun q enter. Aquesta és l'expressió de la hipòtesi $3 \nmid n$ (un cas possible). Vegem que n^{3251} no és múltiple de 3.

$$n^{3251} = (3q+1)^{3251} = \sum_{k=0}^{3251} \binom{3251}{k} (3q)^k 1^{3251-k} = \sum_{k=0}^{3251} \binom{3251}{k} 3^k q^k =$$

$$\binom{3251}{0} 3^0 q^0 + \sum_{k=1}^{3251} \binom{3251}{k} 3^k q^k = 1 + \sum_{k=1}^{3251} \binom{3251}{k} 3^k q^k = 1 + \sum_{k=1}^{3251} \binom{3251}{k} 3 \cdot 3^{k-1} q^k =$$

$$1 + 3 \sum_{k=1}^{3251} \binom{3251}{k} 3^{k-1} q^k = 1 + 3q',$$

amb $q' = \sum_{k=1}^{3251} \binom{3251}{k} 3^{k-1} q^k$, $q' \in \mathbb{Z}$ (recordem que $\binom{n}{k}$ sempre és un nombre natural).

Resumint, $n^{3251} = 3q' + 1$ per a algun enter q'. Però aquest nombre, d'acord amb la discussió prèvia, no és múltiple de 3.

Cas 2. ($r = 2$). Per a algun enter q és $n = 3q+2$. Vegem que n^{3251} no és múltiple de 3.

$$n^{3251} = (3q+2)^{3251} = \sum_{k=0}^{3251} \binom{3251}{k} (3q)^k 2^{3251-k} = \binom{3251}{0} 3^0 q^0 2^{3251} +$$

$$\sum_{k=1}^{3251} \binom{3251}{k} 3^k q^k 2^{3251-k} = 2^{3251} + \sum_{k=1}^{3251} \binom{3251}{k} 3^k q^k 2^{3251-k} =$$

$$2^{3251} + \sum_{k=1}^{3251} \binom{3251}{k} 3 \cdot 3^{k-1} q^k 2^{3251-k} = 2^{3251} + 3 \sum_{k=1}^{3251} \binom{3251}{k} 3^{k-1} q^k 2^{3251-k} = 2^{3251} + 3q',$$

amb $q' = \sum_{k=1}^{3251} \binom{3251}{k} 3^{k-1} q^k 2^{3251-k}$, $q' \in \mathbb{Z}$.

Si fos $3|n^{3251}$, seria $n^{3251} = 3w$ per a algun enter w i, per tant, $3w = 2^{3251} + 3q'$, d'on $3(w-q') = 2^{3251}$, d'on $3|2^{3251}$, que és absurd, ja que 2^{3251} només té factors 2; 2^{3251} només és divisible per les corresponents potències de 2, 2^r, $0 \leq r \leq 3251$, i els simetritzats. Una altra manera d'argumentar-ho és aplicant el lema d'Euclides, generalitzat a un producte qualsevol de factors: "Si p és un nombre primer i $p|ab$, a,b enters, aleshores $p|a$ o $p|b$": en aquest cas, resultaria $3|2$, absurd.

Un altre mètode seria *el contrarecíproc*: $3|n^{3251} \Rightarrow 3|n$, i es pot utilitzar el lema d'Euclides.

PROBLEMA 9.10

Sigui $\theta \in \mathbb{R}$. Obtingueu expressions de

a) $\sin 2\theta$, $\cos 2\theta$ *en funció de* $\sin\theta$, $\cos\theta$.

b) $\sin 3\theta$, $\cos 3\theta$ *en funció de* $\sin\theta$, $\cos\theta$.

c) $\sin 5\theta$, $\cos 5\theta$ *en funció de* $\sin\theta$, $\cos\theta$.

Solució. És una aplicació de la coneguda fórmula de De Moivre. Si n és un nombre natural, $n \geq 1$ (de fet, és interessant a partir de $n = 2$), aleshores:

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

En els tres casos el mètode de resolució és similar. Però, a mesura que l'exponent creix, es fa necessari (o convenient) utilitzar la fórmula del binomi de Newton. Es tracta d'utilitzar la fórmula de De Moivre per a després igualar les respectives parts real i imaginària que apareixen.

Recordem que $i^2 = -1$.

a) La fórmula de De Moivre és:

$\cos 2\theta + i\sin 2\theta = (\cos\theta + i\sin\theta)^2$. Per tant,

$\cos 2\theta + i\sin 2\theta = (\cos\theta + i\sin\theta)^2 = \cos^2\theta + i2\cos\theta\sin\theta + i^2\sin^2\theta = (\cos^2\theta - \sin^2\theta) + i(2\cos\theta\sin\theta)$.

Igualant les parts reals i les parts imaginàries respectives, s'obté:

$$\cos 2\theta = \cos^2\theta - \sin^2\theta,$$

$$\sin 2\theta = 2\sin\theta\cos\theta.$$

b) És la mateixa idea que al primer apartat, però ja utilitzem la fórmula binomial.

$$\cos 3\theta + i\sin 3\theta = (\cos\theta + i\sin\theta)^3 = \sum_{k=0}^{3}\binom{3}{k}(\cos\theta)^k(i\sin\theta)^{3-k} =$$

$$\binom{3}{0}(\cos\theta)^0(i\sin\theta)^3 + \binom{3}{1}(\cos\theta)^1(i\sin\theta)^2 +$$

$$\binom{3}{2}(\cos\theta)^2(i\sin\theta)^1 + \binom{3}{3}(\cos\theta)^3(i\sin\theta)^0 =$$

$$-i\sin^3\theta - 3\cos\theta\sin^2\theta + 3i\cos^2\theta\sin\theta + \cos^3\theta =$$

$$(\cos^3\theta - 3\cos\theta\sin^2\theta) + i(3\cos^2\theta\sin\theta - \sin^3\theta).$$

Per tant, igualant les parts reals i imaginàries respectives:

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta,$$

$$\sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta.$$

c) $\cos 5\theta + i\sin 5\theta = (\cos\theta + i\sin\theta)^5 = \sum_{k=0}^{5}\binom{5}{k}(\cos\theta)^k(i\sin\theta)^{5-k} =$

$\binom{5}{0}(\cos\theta)^0(i\sin\theta)^5 + \binom{5}{1}(\cos\theta)^1(i\sin\theta)^{5-1} + \binom{5}{2}(\cos\theta)^2(i\sin\theta)^{5-2} +$

$\binom{5}{3}(\cos\theta)^3(i\sin\theta)^{5-3} + \binom{5}{4}(\cos\theta)^4(i\sin\theta)^{5-4} + \binom{5}{5}(\cos\theta)^5(i\sin\theta)^{5-5} =$

$(i\sin\theta)^5 + 5(\cos\theta)(i\sin\theta)^4 + 10\cos^2\theta\,(i\sin\theta)^3 + 10\cos^3\theta\,(i\sin\theta)^2 +$
$5\cos^4\theta\,(i\sin\theta)^1 + \cos^5\theta =$

$i\sin^5\theta + 5\cos\theta\sin^4 - i10\cos^2\theta\sin^3\theta - 10\cos^3\theta\sin\theta + 5i\cos^4\theta\sin\theta + \cos^5\theta =$

$(5\cos\theta\sin^4\theta - 10\cos^3\theta\sin\theta + \cos^5\theta) + i(\sin^5\theta - 10\cos^2\theta\sin^3\theta + 5\cos^4\theta\sin\theta).$

Per tant, igualant les parts reals i imaginàries respectives:

$\cos 5\theta = 5\cos\theta\sin^4\theta - 10\cos^3\theta\sin\theta + \cos^5\theta,$

$\sin 5\theta = \sin^5\theta - 10\cos^2\theta\sin^3\theta + 5\cos^4\theta\sin\theta.$

→ 10

La fórmula

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

En aquest capítol, es presenta una fórmula molt útil.

10.1. La fórmula

Teorema 10.1 *Siguin x, y nombres reals qualssevol, i sigui $n \geq 1$ un nombre natural arbitrari. Aleshores*

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \tag{10.1}$$

Demostració. Es pot demostrar directament, efectuant operacions a partir del membre de la dreta, amb les simplificacions conseqüents:

$$\begin{aligned}
&(x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}) \\
&= x(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}) \\
&- y(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}) \\
&= (x^n + x^{n-1}y + x^{n-2}y^2 + \cdots + x^2y^{n-2} + xy^{n-1}) \\
&- (yx^{n-1} + y^2x^{n-2} + \cdots + xy^{n-1} + y^2) = x^n - y^n. \blacksquare
\end{aligned}$$

Amb notació de sumatoris:

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k} = (x-y)\sum_{i=0}^{n-1} y^i x^{(n-1)-i} \tag{10.2}$$

Fórmules de predicats per a la fórmula anterior 10.2:

$$\forall x \in \mathbb{R} \forall y \in \mathbb{R} \forall n \in \mathbb{N} (n \geq 1 \to x^n - y^n = (x-y)\sum_{i=0}^{n-1} y^i x^{(n-1)-i})$$

$$\forall x \forall y \forall n((x \in \mathbb{R} \wedge x \in \mathbb{R} \wedge n \in \mathbb{N} \wedge n \geq 1) \to x^n - y^n = (x-y)\sum_{i=0}^{n-1} y^i x^{(n-1)-i})$$

Observeu que l'ordre dels sumands al terme de la dreta de la fórmula 10.1 s'obté amb la versió del sumatori $\sum_{i=0}^{n-1} y^i x^{(n-1)-i}$.

Encara hi ha una altra expressió possible per al sumatori de la fórmula 10.1: $\sum_{i+j=n-1} x^i y^j$.

També es poden escriure fórmules derivades, essencialment la mateixa, com per exemple:

$$x^{n+1} - y^{n+1} = (x-y)\sum_{k=0}^{n} x^k y^{n-k}.$$

Farem servir la fórmula 10.1 per a estudiar problemes de divisibilitat, de manera que x, y seran enters. Vegeu-ne algunes conseqüències en aritmètica:

a) Per a factoritzar, ja que permet afirmar que $x^n - y^n$ és factoritzable, amb $x - y$ com a factor (x, y enters).

b) I també que $1 - z^n$ és divisible per $1 - z$ (z enter).

Alguns exemples d'aplicació immediata

Exemple 10.1 Vegem un exemple en què recuperem una fórmula ben coneguda:

$$x^2 - y^2 = (x-y)(x^{2-1} + y^{2-1}) = (x-y)(x+y). \blacksquare$$

Vegem-ne alguns exemples d'aplicació:

Exemple 10.2

$$x^3 - y^3 = (x-y)(x^2 + xy + y^2)$$
$$x^4 - y^4 = (x-y)(x^3 + x^2y + xy^2 + y^3)$$
$$x^5 - y^5 = (x-y)(x^4 + x^3y + x^2y^2 + xy^3 + y^4)$$
$$x^6 - y^6 = (x-y)(x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + y^5)$$
$$x^8 - 2^8 = (x-2)(x^7 + x^6 2 + x^5 2^2 + x^4 2^3 + x^3 2^4 + x^2 2^5 + x^1 2^6 + 2^7). \blacksquare$$

Les fórmules del grup següent es poden veure com a casos particulars de la fórmula anterior o també com a fórmula de la suma d'una progressió geomètrica

(recordem que $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1 = \dfrac{x^{(n-1)+1} - 1}{x-1}$).

Exemple 10.3

$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$ (ja que $x^n - 1 = x^n - 1^n$)

$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$, ja que $x^5 - 1 = x^5 - 1^5$

$2^n - 1 = (2-1)(2^{n-1} + 2^{n-2} + \cdots + 2 + 1)$, ja que $2^n - 1 = 2^n - 1^n$

$7^n - 1 = (7-1)(7^{n-1} + 7^{n-2} + \cdots + 7 + 1)$, ja que $7^n - 1 = 7^n - 1^n$

$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$, ja que $x^7 - 1 = x^7 - 1^7$.

I a cada cas s'aplica la fórmula. ■

Com veurem, utilitzant aquesta fórmula, alguns problemes de divisibilitat resulten sorprenentment fàcils de resoldre. En efecte, amb aquesta fórmula:

$(x-y) | (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$ i, per tant,

$(x-y) | x^n - y^n$,

per a x, y enters, cosa que és un autèntic "generador" d'enunciats, com podem veure a continuació.

Exemple 10.4 Per a n natural:

a) $5 | 8^n - 3^n$ (ja que $5 = 8 - 3$, amb $x = 8$, $y = 3$);

$8^n - 3^n = (8-3)(8^{n-1} + 8^{n-2}3 + 8^{n-3}3^2 + \cdots + 8^2 3^{n-3} + 8 3^{n-2} + 3^{n-1})$

b) $11^n - 5^n$ és divisible per $11 - 5 = 6$, amb $x = 11$, $y = 5$);

$11^n - 5^n = (11-5)(11^{n-1} + 11^{n-2}5 + 11^{n-3}5^2 + \cdots + 11^2 5^{n-3} + 11 5^{n-2} + 5^{n-1})$

c) $6 | 7^n - 1$ (ja que $7 - 1 = 6$);

$7^n - 1 = 7^n - 1^n = (7-1)(7^{n-1} + 7^{n-2}1 + 7^{n-3}1^2 + \cdots + 7^2 1^{n-3} + 7 1^{n-2} + 1^{n-1})$

d) $9 | 10^n - 1$

$10^n - 1 = 10^n - 1^n = (10-1)(10^{n-1} + 10^{n-2}1 + 10^{n-3}1^2 + \cdots + 10^2 1^{n-3} + 10 1^{n-2} + 1^{n-1})$

e) $8 | 9^n - 1$

$9^n - 1 = 9^n - 1^n = (9-1)(9^{n-1} + 9^{n-2}1 + 9^{n-3}1^2 + \cdots + 9^2 1^{n-3} + 9 1^{n-2} + 1^{n-1})$

f) $2345^n - 1023^n$ és divisible per $2345 - 1023 = 1322$, és a dir, $1322 | 2345^n - 1023^n$.

g) $11 | 12^n - 1$. En efecte, podem escriure $12^n - 1 = 12^n - 1^n =$

$(12-1)(12^{n-1} + 12^{n-2}1 + 12^{n-3}1^2 + \cdots + 12^2 1^{n-3} + 12 1^{n-2} + 1^{n-1})$

$= (12-1)(12^{n-1} + 12^{n-2} + 12^{n-3} + \cdots + 12^2 + 12 + 1)$, múltiple de $12 - 1 = 11$.

Com hem vist en diversos exemples, s'observa que $a-1|a^n-1$, per a a enter i n natural, ja que

$$a^n - 1 = a^n - 1^n =$$
$$(a-1)(a^{n-1} + a^{n-2}1 + a^{n-3}1^2 + \cdots + a^2 1^{n-3} + a1^{n-2} + 1^{n-1})$$
$$= (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + \cdots + a^2 + a + 1).$$

De fet, és un cas particular de $(x-y)|x^n - y^n$. ■

Exemple 10.5 Fórmules derivades

Poden derivar-se diverses fórmules a partir de particularitzacions per a n, x, y. Per exemple:

a) $x^{2n} - y^{3n} = (x^2)^n - (y^3)^n$
$= (x^2 - y^3)(x^{2(n-1)} + x^{2(n-2)}y^3 + \cdots + x^2 y^{3(n-2)} + y^{3(n-1)}).$

Podem escriure el mateix desenvolupament per a $(x^n)^2 - (y^n)^3$, ja que $(x^n)^2 - (y^n)^3 = x^{2n} - y^{3n}$, de manera que

$$(x^n)^2 - (y^n)^3 = (x^2 - y^3)(x^{2(n-1)} + x^{2(n-2)}y^3 + \cdots + x^2 y^{3(n-2)} + y^{3(n-1)}).$$

b) $x^n - (-1)^n = (x - (-1))(x^{n-1} - x^{n-2} + \cdots + x(-1)^{n-2} + (-1)^{n-1})$
$= (x+1)(x^{n-1} - x^{n-2} + \cdots + x(-1)^{n-2} + (-1)^{n-1}).$

En particular, si n **és senar**, atès que $(-1)^n = -1$, resulta:

$$\boxed{x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + x^{n-1} - x^{n-2} + \cdots - x + 1)}\,.$$

c) Vegem-ne una més. Si a

$$c^n - d^n = (c-d)(c^{n-1} + c^{n-2}d + \cdots + cd^{n-2} + d^{n-1})$$

fem $c = \sqrt[n]{x}$, $d = \sqrt[n]{y}$, resulta

$$x - y = (\sqrt[n]{x} - \sqrt[n]{y})((\sqrt[n]{x})^{n-1} + (\sqrt[n]{x})^{n-2}(\sqrt[n]{y}) + \cdots + (\sqrt[n]{x})(\sqrt[n]{y})^{n-2} + (\sqrt[n]{y})^{n-1}).$$ ■

10.2. Exercicis sobre la fórmula

Alguns d'aquests problemes es resolen de manera immediata, cosa que no impedeix que no presentem demostracions per altres mètodes, encara que no siguin tan immediats, a fi d'il·lustrar una metodologia i que el lector pugui adquirir major capacitat.

Vegem un problema amb qüestions de resolució immediata:

PROBLEMA 10.1

Apliqueu la fórmula 10.1 per tal de demostrar:

a) $24|5^{2n} - 1$, *per a tot* $n \geq 1$ *natural.*

b) $6|2^{2n+1} - 2$, *per a tot* $n \geq 1$ *natural.*

c) $2|3^n - 1$, *per a tot* $n \geq 1$ *natural.*

d) $3|7^n - 4^n$, *per a tot* $n \geq 1$ *natural.*

e) $a|(a+1)^n - 1$, *per a tot enter* a *i tot natural* $n \geq 1$.

f) $(a+2)|(a+5)^n - 3^n$, *per a tot enter* a *i tot natural* $n \geq 1$.

Solució

a) Escrivim $5^{2n} - 1 = (5^2)^n - 1 = 25^n - 1 = 25^n - 1^n$. Aplicant la fórmula per a $x = 25$, $y = 1$, és $25^n - 1^n = (25-1)m$, per a m enter, és a dir, $5^{2n} - 1 = (25-1)m = 24m$, múltiple de 24.

b) Escrivim $2^{2n+1} - 2 = 2(2^{2n} - 1) = 2((2^2)^n - 1) = 2(4^n - 1)$. Apliquem la fórmula:

$4^n - 1 = 4^n - 1^n = (4-1)(4^{n-1} + 4^{n-2} + \cdots + 4^2 + 1) = 3(4^{n-1} + 4^{n-2} + \cdots + 4^2 + 1)$.
Així, $2^{2n+1} - 2 = 2 \cdot 3(4^{n-1} + 4^{n-2} + \cdots + 4^2 + 1) = 6(4^{n-1} + 4^{n-2} + \cdots + 4^2 + 1) = 6q$, múltiple de 6 (amb $q = 4^{n-1} + 4^{n-2} + \cdots + 4^2 + 1 \in \mathbb{Z}$).

c) És una aplicació immediata de la fórmula, amb $x = 3$, $y = 1$:

$3^n - 1 = 3^n - 1^n = (3-1)(3^{n-1} + 3^{n-2} + \cdots 3^2 + 3 + 1) = 2(3^{n-1} + 3^{n-2} + \cdots 3^2 + 3 + 1) = 2q$, múltiple de 2.

d) Apliquem la fórmula amb $x = 7$, $y = 4$. En resulta:

$7^n - 4^n = (7-4)(7^{n-1} + 7^{n-2} \cdot 4 + 7^{n-3} \cdot 4^2 + \cdots 7^2 \cdot 4^{n-3} + 7 \cdot 4^{n-2} + 4^{n-1})$.

Així, $7^n - 4^n = (7-4)q$, amb $q = 7^{n-1} + 7^{n-2} \cdot 4 + 7^{n-3} \cdot 4^2 + \cdots 7^2 \cdot 4^{n-3} + 7 \cdot 4^{n-2} + 4^{n-1}$, enter. Per tant, $7^n - 4^n = (7-4)q = 3q$, múltiple de 3.

e) S'aplica la fórmula amb $x = a+1$, $y = 1$. Tenim $(a+1)^n - 1 = (a+1)^n - 1^n = ((a+1)-1)q = aq$, múltiple de a.

f) Amb $x = a+5$, $y = 3$, en resulta $(a+5)^n - 3^n = ((a+5)-3)q = (a+2)q$, múltiple de $a+2$.

Atès que la fórmula 10.1 és una propietat que es formula en termes de $n \in \mathbb{N}$ (fixats x, y nombres reals), una possibilitat de mètode de prova és la inducció, com podem veure al problema següent.

PROBLEMA 10.2

Demostreu per inducció la fórmula: per a tot x, y nombres reals i per a tot n nombre natural, $n \geq 1$:

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k}.$$

Solució. Cal provar:

$$\forall x \forall y((x \in \mathbb{R} \wedge x \in \mathbb{R}) \to \forall n(n \in \mathbb{N} \to x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k}))$$

Considerem x, y nombres reals arbitraris, però fixos per a la demostració, i demostrem per inducció sobre $n \geq 1$ que

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k}$$

Per tant, la propietat $P(n)$ a demostrar és la igualtat

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k}, \text{ per a tot } n \geq 1,$$

de manera que el valor inicial de n és $n_0 = 1$. La demostració és per inducció simple o ordinària sobre n. S'ha de seguir l'esquema demostratiu habitual.

Pas bàsic. Cal provar que $P(1)$ $(n_0 = 1)$ és cert.

En aquesta igualtat a provar, vegem que el membre de la dreta (D), per a $n_0 = 1$, i el membre de l'esquerra coincideixen. En efecte:

$$E = x^1 - y^1 = x - y$$

$$D = (x-y)\sum_{k=0}^{1-1} x^k y^{(1-1)-k} = (x-y)x^0 y^{(1-1)-0} = x - y, \text{ i és } E = D.$$

Pas inductiu. Cal provar que $P(n) \Rightarrow P(n+1)$, per a tot $n \geq 1$. Aquest pas es concreta a demostrar la implicació:

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k} \Rightarrow x^{n+1} - y^{n+1} = (x-y)\sum_{k=0}^{(n+1)-1} x^k y^{((n+1)-1)-k}, \text{ és a dir:}$$

$$x^n - y^n \overset{HI}{=} (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k} \Rightarrow x^{n+1} - y^{n+1} = (x-y)\sum_{k=0}^{n} x^k y^{n-k}$$

Noteu que la suposició $x^n - y^n \overset{(HI)}{=} (x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k}$ és la hipòtesi d'inducció.

Efectuarem manipulacions a la fórmula $(x-y)\sum_{k=0}^{n} x^k y^{n-k}$ per tal de fer-hi aparèixer alguna subfórmula que permeti aplicar la hipòtesi d'inducció (HI). En efecte:

$$(x-y)\sum_{k=0}^{n} x^k y^{n-k} = (x-y)[\sum_{k=0}^{n-1} x^k y^{n-k} + x^n y^{n-n}]$$

$$= (x-y)[\sum_{k=0}^{n-1} x^k y y^{(n-1)-k} + x^n] = (x-y)y\sum_{k=0}^{n-1} x^k y^{(n-1)-k} + (x-y)x^n$$

$$= y(x-y)\sum_{k=0}^{n-1} x^k y^{(n-1)-k} + x^{n+1} - yx^n \overset{HI}{=} y(x^n - y^n) + x^{n+1} - yx^n = x^{n+1} - y^{n+1}$$

Observeu que la fórmula de la suma de la progressió geomètrica

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x-1},$$

per a $x \neq 1$, no és més que un cas particular de la fórmula d'aquest capítol (10.1). En efecte, es pot reescriure com a

$(x-1)(1 + x + x^2 + \cdots + x^n) = x^{n+1} - 1$ i és un cas particular de la fórmula amb $y = 1$. A l'exercici següent, es veu que, de la fórmula de la progressió geomètrica, en resulta la fórmula (10.1) del capítol.

PROBLEMA 10.3

Demostreu la fórmula (10.1) a partir de la fórmula:

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x-1}, \textit{ per a } x \neq 1, x \textit{ real i } n \textit{ nombre natural.}$$

Solució. També s'escriu $1 + x + x^2 + \cdots + x^{n-1} = \dfrac{x^n - 1}{x-1}$, per a $x \neq 1$.

Ara, fent $x = \frac{a}{b}$ $(b \neq 0,\ a \neq b)$, resulta:

$$1 + \frac{a}{b} + (\frac{a}{b})^2 + (\frac{a}{b})^3 + \cdots + (\frac{a}{b})^{n-1} = \frac{(\frac{a}{b})^n - 1}{\frac{a}{b} - 1}$$

$$1 + \frac{a}{b} + \frac{a^2}{b^2} + \frac{a^3}{b^3} + \cdots + \frac{a^{n-1}}{b^{n-1}} = \frac{\frac{a^n}{b^n} - 1}{\frac{a}{b} - 1}, \text{ d'on}$$

$$\frac{1}{b^{n-1}}(b^{n-1} + ab^{n-2} + a^2b^{n-3} + \cdots + a^{n-1}) = \frac{\frac{a^n - b^n}{b^n}}{\frac{a-b}{b}}$$

$$\frac{1}{b^{n-1}}(b^{n-1}+ab^{n-2}+a^2b^{n-3}+\cdots+a^{n-1})=\frac{\frac{a^n-b^n}{b^{n-1}}}{a-b}$$

$$b^{n-1}+ab^{n-2}+a^2b^{n-3}+\cdots+a^{n-1})=\frac{a^n-b^n}{a-b}$$

$$(a-b)(b^{n-1}+ab^{n-2}+a^2b^{n-3}+\cdots+a^{n-1})=a^n-b^n$$

Per als casos exclosos ($b \neq 0$, $a \neq b$), si substituïm a la fórmula, també se satisfà, de manera que és vàlida per a tot valor de a i b.

PROBLEMA 10.4

Sigui n un nombre natural qualsevol, $n \geq 1$. *Proveu que, si* $5^n - 1$ *és un nombre primer, aleshores n és un nombre primer.*

Solució. *Anàlisi preliminar*. Cal provar, per a un $n \geq 1$ natural arbitrari, però fix per a la demostració, que

$5^n - 1$ és primer $\Rightarrow n$ és primer

No sembla fàcil d'abordar directament. Vegem si podem demostrar el contrarecíproc, que seria:

n no és primer $\Rightarrow 5^n - 1$ no és primer

Una altra possibilitat és considerar la fórmula (per a $n \in \mathbb{N}$, $n \geq 1$)

$\forall n(5^n - 1$ és primer $\rightarrow n$ és primer) i demostrar-la per reducció a l'absurd: partim de la negació, que acaba essent equivalent a

$\exists n(5^n - 1$ és primer $\wedge\, n$ no és primer)

i arribem a un absurd.

Seguim la via del *contrarecíproc*. Expressem-lo d'una altra manera equivalent:

n és compost $\Rightarrow 5^n - 1$ és compost, com demostrarem *directament*.

Com aplicar la hipòtesi? Si n és compost, aleshores es pot expressar com $n = ab$, amb a, b naturals, factors propis, amb $1 \leq a \leq n$, $1 \leq b \leq n$. Com que a és factor propi, és $1 < a < n$ (si no fos així, seria $a = 1$ o $a = n$ i ,automàticament, en concordança, $b = n$ o $b = 1$, de manera que no seria una factorització pròpia). Aleshores també $1 < b < n$; en efecte, si fos $b = 1$, seria $n = ab = a \cdot 1 = a$, que no és possible; si fos $b = n$, seria $n = ab = an$, d'on $a = 1$, que no és possible. Per tant, en resum, $n = ab$, a, b naturals, amb $1 < a < n$ i $1 < b < n$.

Vegem que es pot escriure $5^n - 1 = cd$, com a producte de factors propis, c, d naturals, amb $0 < c < 5^n - 1$, $0 < d < 5^n - 1$, i així serà compost.

Què està guiant la resolució? Observeu que l'expressió $5^n - 1$ és la que apareix a la fórmula 10.1. Aquests factors sortiran previsiblement de l'aplicació de la fórmula. En efecte, utilitzant que $n = ab$, podem escriure:

$$5^n - 1 = 5^{ab} - 1 = (5^a)^b - 1 = (5^a)^b - 1^b = (5^a - 1)((5^a)^{b-1} + (5^a)^{b-2} + \cdots + 5^a + 1)$$

Expressant $d = (5^a)^{b-1} + (5^a)^{b-2} + \cdots + 5^a + 1$, $c = 5^n - 1$, resulta $5^n - 1 = (5^a - 1)d = cd$, producte de dos factors naturals. Si veiem que són propis, haurem acabat la demostració. Utilitzem que la funció exponencial 5^x és creixent i, per tant:

$1 < a < n \Rightarrow 5^1 < 5^a < 5^n \Rightarrow 5^1 - 1 < 5^a - 1 < 5^n - 1 \Rightarrow 1 < 5^a - 1 < 5^n - 1$, d'on resulta que $c = 5^a - 1$ és un factor propi de $5^n - 1$ i, automàticament, també ho és d. Queda demostrat que $5^n - 1$ és compost, i això completa la demostració.

Observació. Els papers de a i de b són intercanviables.

Observació. En aquesta última part, hem demostrat $1 < a < n \Rightarrow 1 < 5^a - 1 < 5^n - 1$ i, com que tenim $1 < a < n$, resulta $1 < 5^a - 1 < 5^n - 1$.

Observació. Per l'argumentació feta, es poden demostrar resultats anàlegs, com per exemple:

$2^n - 1$ és primer $\Rightarrow n$ és primer

$3^n - 1$ és primer $\Rightarrow n$ és primer

$7^n - 1$ és primer $\Rightarrow n$ és primer

Observació. En aquest cas especial, en comptes d'utilitzar la fórmula 10.1, es pot fer servir la de la suma d'una progressió geomètrica:

$x^n - 1 = (x-1)(1 + x + x^2 + \cdots + x^{n-1})$,

$\frac{x^n - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{n-1}$.

→ 11

Idees de resolució de problemes

Donem *alguns consells* sobre què fer quan ens enfrontem a un enunciat, a un problema que hem de resoldre. Totes les idees han aparegut al llarg del text.

- Què diu l'enunciat? En molts casos, és clar i explícit; en molts altres casos, se n'ha de fer una anàlisi per tal de saber exactament quines en són les afirmacions. Per exemple, què vol dir exactament: "el cub dels nombres enters senars és senar"? O "la suma de dos nombres enters senars és parell"? Hi ha estructures lògiques implícites i, per tant, amagades o no explicitades, o no suficientment explicitades: És un condicional?, per exemple. Està quantificat?
- Formalitzeu-lo. Si és un enunciat que està expressat verbalment en un percentatge elevat, és convenient formalitzar-lo i substituir part o tot l'enunciat per una fórmula de predicats.
- D'on són les variables que apareixen en un enunciat? De quin conjunt? Són nombres naturals, són nombres enters?
- Quina n'és l'estructura? És un condicional? És un bicondicional? Una equivalència? Una condició necessària? Una condició suficient? Una condició necessària i suficient? "... si, i només si, ..."?

Gran part dels enunciats són condicionals o bicondicionals, potser dintre de quantificadors universals. En el cas d'un condicional:

- Quina és la hipòtesi? Quina estructura té? És simple; és composta? Per exemple, $H_1 \wedge H_2$ seria una hipòtesi composta, conjunció de dues afirmacions. A la resolució, tingueu molta cura d'aclarir on s'aplica la hipòtesi o les diferents parts de la hipòtesi. En el curs de la demostració, vigileu constantment si encara hi ha alguna part de la hipòtesi que no s'hagi aplicat.
- Quina és la tesi? És simple o composta? És composta $T_1 \wedge T_2$, per exemple. Mireu d'establir alguna connexió entre hipòtesi i tesi; potser això us donarà alguna idea de per on seguir, i us permetrà establir una estratègia de demostració.

– És una equivalència entre dues afirmacions? En cas afirmatiu, què cal fer? Cal demostrar dues implicacions.
– És una equivalència d'unes quantes afirmacions? Cal provar que qualsevol equival a qualsevol altra. O, el que és el mateix, que qualsevol implica qualsevol altra. És possible que es pugui dissenyar una demostració circular d'implicacions que acabi provant les equivalències, sense necessitat de provar totes les implicacions possibles que en teoria caldrien.
– Està quantificat amb un quantificador universal? Si és de la forma $\forall x P(x)$, es pot demostrar per reducció a l'absurd o bé fixant x arbitrari i demostrant $P(x)$ per a aquest x.
– Està quantificat amb un quantificador existencial? En cas afirmatiu, es pot demostrar directament o per reducció a l'absurd.
– És un enunciat del tipus $\forall x P(x)$ i s'ha de provar que és fals? Cal aportar un contraexemple. O bé suposar que és cert i arribar a una contradicció (reducció a l'absurd).
– Quin és el mètode més recomanable de resolució? S'ha de veure sobre casos particulars.
– Quins mètodes recordeu? Si no veieu clar un mètode directe, penseu sempre en la resolució:

  a) reducció a l'absurd
  b) pel contrarecíproc
  c) per casos
  d) per inducció

Els mètodes es poden combinar i barrejar, i aplicar en una mateixa demostració més d'un mètode per a les diferents parts, de manera que hi coexisteixin diversos mètodes.

Descomposició en subproblemes i reducció d'un problema a un d'un altre tipus. La resolució per casos, en teoria, redueix el problema a una col·lecció de problemes, suposadament més fàcils que el conjunt; cada cas acota la variabilitat i permet concentrar-se en aquell cas, cosa que en principi en facilita la resolució. Un altre aspecte important amb el qual sempre s'ha de pensar és reduir un problema a un altre, d'una altra tipologia, que ja tinguem resolt, que sapiguem resoldre o que ens resulti més fàcil de resoldre.

Descomponeu un problema en subproblemes. Una equivalència en dues implicacions. Una igualtat de conjunts en dues inclusions. Una descomposició en casos: respecte de quin paràmetre, quins casos i que ho cobreixi tot.

Per inducció. També convé pensar en la possibilitat d'utilitzar inducció, però això només és possible –i pot no funcionar– per a una tipologia determinada d'enunciats. D'entrada, han de ser enunciats formulats en termes de nombres naturals, tot i que hi ha diverses modalitats. Un enunciat típic, demostrable per inducció, que denotem per $P(n)$ seria, per exemple:

"Per a tot nombre natural n, $n \geq 1$, $1+2+\cdots+n = \dfrac{n(n+1)}{2}$".

En canvi, el teorema de Pitàgores no seria demostrable per inducció.

Convé formular bé la demostració i explicitar-ne clarament l'estructura. Busqueu la manera d'aplicar la hipòtesi d'inducció (HI). Normalment, s'ha de fer alguna manipulació en una fórmula, que hi faci aparèixer una subfórmula, que sigui exactament la que apareix a la hipòtesi d'inducció, fet que ens ha de permetre aplicar la HI.

Tot enunciat que s'expressa en termes d'un nombre natural n és demostrable per inducció? No necessàriament. Vegem, per exemple, l'enunciat:

Demostreu: "Per a tot n nombre enter, $\mathrm{mcd}(2n+5, 3n+7) = 1$". Tindríem dificultats per demostrar-ho per inducció, pels problemes de relacionar l'enunciat per a n amb el mateix per a $n+1$, en el pas inductiu.

Avançant idees (del volum 2), per a problemes de divisibilitat, considerem els tres llenguatges: el llenguatge de la divisibilitat, el llenguatge de les congruències i el llenguatge de les classes de residu o congruències. També és un exemple de reducció de problemes d'una tipologia a una altra:

$m|a \Leftrightarrow a \equiv 0 \pmod{m} \Leftrightarrow \bar{a} = \bar{0}$ (a $\mathbb{Z}_m$)

De vegades, té l'avantatge d'una simplicitat més gran. O en el cas de les classes de congruències, que podem treballar algebraicament, operant amb classes de residus. També és una situació en la qual podem combinar mètodes: congruències amb casos, congruències amb inducció...

En general, intenteu resoldre el problema pel màxim de mètodes possibles. Observeu els enunciats següents, en què es demana resoldre el problema utilitzant diversos mètodes. Observeu només la idea, ja que alguns continguts relatius a l'enunciat són propis d'un altre context (volum 2).

1 Sigui n un nombre natural. Calculeu $\mathrm{mcd}(2n+7, 3n+10)$.

a) Obtenint els divisors positius comuns de $2n+7$ i de $3n+10$.
b) Aplicant el teorema d'Euclides.
c) Aplicant l'algorisme d'Euclides.

2 Demostreu que, per a tot nombre enter n és $6|n(n+1)(2n+1)$.

a) Per congruències i per casos.
b) Per congruències i inducció.
c) Per casos (divisió entera).
d) Per inducció.
e) Per classes de residus i inducció.
f) Per classes de residus i per casos.

g) Indirectament, utilitzant: $1^2+2^2+3^2+\cdots+n^2$

3 Demostreu que $4|9^n+3$ per a tot nombre natural.

a) Directament (binomi de Newton, $9 = 8+1$).

b) Per inducció.
c) Per congruències, directament.
d) Per congruències, per inducció.
e) Per classes de residus.

4 Si n és un nombre natural, proveu que $n^5 - n$ és múltiple de 5.

a) Per casos.
b) Per inducció.
c) Per congruències i per casos.
d) Per congruències i inducció.
e) Per classes de residus i per casos.
f) Per classes de residus i per inducció.

5 Demostreu que, per a tot n natural, es compleix $2|3^n - 1$.

a) Per inducció (fent servir $3 = 2+1$).
b) Directament, fent servir $x^n - y^n = (x-y)(x^{n-1} + x^{n-2})y + \cdots + xy^{n-2} + y^{n-1}$.
c) Directament, fent servir $3 = 2+1$ i la fórmula del binomi de Newton.
d) Per congruències, directament.
e) Per congruències i inducció.
f) Per classes de residus, directament.
g) Per classes de residus i inducció.

Parèntesis. No us deixeu parèntesis: pot ser letal. Una demostració pot derivar en incorreccions per aquesta causa i fer totalment inservible l'argumentació. I també càlculs diversos.

Redacció de la resolució. Un cop resolt un problema, és molt important explicar-ne correctament la resolució. Vegeu [ESQTRI], [ESQTRI2] i diverses referències de la bibliografia, les mateixes que segueixen a continuació.

Mètodes de resolució de problemes. També per a mètodes de resolució de problemes: [BLOC00], [CHPZ03], [CUPI01], [GUND2011], [HOUS09], [SMIT06], [SOLL05], [VELL94].

Bibliografia

[AHUL95] Aho, A.V. and Ullman, J.D. *Foundations of Computer Science*. Computer Science Press (Freeman), 1995.

[ALHU88] Albertson, M.O. and Hutchinson, J.P. *Discrete Mathematics with Algorithms*. John Wiley, 1988.

[APOST91] Apostol, M. *Calculus*, Vol. 1,2. Reverté, 1991.

[BENA93] Ben-Ari, M. *Mathematical Logic for Computer Science*. Springer, 2001.

[BECK10] Beck, M. and Geoghegan, R. *The Art of Proof. Basic Training for Deeper Mathematics*. Springer, 2010.

[BILB98] Bilbao, M., Castañeda, F. and PeralL, J.C. *Problemas de cálculo*. Pirámide, 1998.

[BLOC00] Bloch, E. *Proofs and Fundamentals: a First Course in Abstract Mathematics*. Springer, 2011.

[CHPZ03] Chartrand, G., Polimeni, A.D. and Zhang, P. *Mathematical Proofs. A Transition to Advanced Mathematics*. Addison-Wesley, 2003.

[CHIL84] Childs, L. *A Concrete Introduction to Higher Algebra*. Springer, 1984.

[CUPI01] Cupillari, A. *The Nuts and Bolts of Proofs*. Academic Press, 2010.

[DGRU90] De Guzman, M. and Rubio, B. *Problemas, conceptos y métodos del análisis matemático*. *Estrategias del pensamiento matemático*. Pirámide, 1990.

[ECCL97] Eccles, P.J. *An Introduction to Mathematical Reasoning: Numbers, Sets and Functions*. Cambridge University Press, 1997.

[ENDE01] Enderton, H.B. *A Mathematical Introduction to Logic*. HartCourt-Academic Press, 2001.

[ENGL98] Engel, A. *Problem-Solving Strategies*. Springer, 1998.

[ESQTRI] Esqué, P. and Trias, J. *Escriptura científica*, Versió 1.1, gener de 2012. Enllaç directe al document: `http://llati.upc.es/escripturacientifica/wp-content/uploads/escripturaCientificaVersio1-1_Gener2012.pdf`

[ESQTRI2] Esqué, P. and Trias, J. *Blog d'escriptura científica, inici: gener 2012*. `http://www-ma2.upc.edu/escripturacientifica/`

[EXNE96] Exner, G.R. *An Accompanigment to Higher Mathematics (Undergraduate Texts in Mathematics)*. Springer, 1996.

[GEMIG96] Gemignani, M.C. *Basic Concepts of Mathematics and Logics*. Dover, 1997.

[GERS97] Gerstein, L.J. *Introduction to Mathematical Structures and Proofs*. Springer, 1997.

[GOD68] Godement, R. *Algebra*. Hermann, 1968.

[GOTA] Goodrich, M.T. and Tamassia, R. *Algorith Design: Foundations, Analysis and Internet Examples*. John Wiley, 2002.

[GUND2011] Gunderson, D.S. *Handbook of Mathematical Induction*. *Theory and Applications*. CRC Press, Chapman & Hall, 2011.

[HAM00] Hamilton, A.G. *Logic for Mathematicians*. Cambridge University Press, 2001.

[HIGH] Higham, N. *Handbook of Writing for the Mathematical Sciences*. SIAM, 1998.

[HOUS09] Houston, K. *How to Think Like a Mathematician*. Cambridge University Press, 2009.

[JON98] Jones, G.A. and Jones, J.M. *Elementary Number Theory*. Springer, 1998.

[KALM86] Kalmanson, K. *An Introduction to Discrete Mathematics and Its Applications*. Addison Wesley, 1986.

[KOSH07] Koshy, T. *Elementary Number Theory with Applications*. Academic Press, 2007.

[KRAN97] Krantz, S.G. *Techniques of Problem Solving*. American Mathematical Society, 1997.

[KRAN02] Krantz, S.G. *Elements of Advanced Mathematics*. Chapman-Hall, 2002.

[LEVI07] Levitin, A. *The Design and Analysis of Algorithms*. Pearson, Addison Wesley, 2007.

[MEND66] Mendelson, E. *Introduction to Mathematical Logic*. CRC Press, Chapman-Hall, 2010.

[PLA06] Pla i Carrera, J. *Introducció a la metodologia de la Matemàtica*. Publicacions: Edicions UB, 2006.

[POLY81] Polya, G. *Cómo plantear y resolver problemas*. Trillas, 1981.

[POZO2013] Pozo, F., Parés, N. and Vidal, Y. *Matemáticas para la ingeniería*. Pearson, 2013.

[ROSE95] Rose, H.E. *A Course in Number Theory*. Oxford University Press, 1995.

[ROBB06] Robbins, N. *Beginning Number Theory*. Jones and Bartlett Publishers, 2006.

[ROSE00] Rosen, K.H. *Elementary Number Theory and Its Applications*. Addison-Wesley, 2000.

[ROSE03] Rosen, K.H. *Matemática discreta y sus aplicaciones*. McGraw-Hill, 2004.

[ROWR98] Ross, K.A and Wright, C.R.B. *Discrete Mathematics*. Prentice-Hall, 1998.

[RUIZ2014] Ruiz, J.L. (ed). *Problemes de fonaments matemàtics*, 2014, `http://www-ma2.upc.edu/fonamentsmatematics/` `http://www-ma2.upc.edu/fonamentsmatematics/index_archivos/fm-2014-2015-q1-problems-catala.pdf`

[SCHO08] Schöning, U. *Logic for Computer Scientists*. Birkkäuser, 1989-2008.

[SMIT06] Smith, D., Eggen, M. and ST. Andre, R. *A Transition to Advanced Mathematics*. Thomson, Brooks Cole, 2006.

[SOLL05] Sollow, D. *How to Read and Do Proofs: An Introduction to Mathematical Thought Processes*. Wiley, 2005.

[STEIN09] Stein, W. *Elementary Number Theory: Primes, Congruences, and Secrets. A Computational Approach*. Springer, 2009.

[VELL94] Velleman, D.J. *How to Prove it: A Structured Approach*. Cambridge University Press, 1994.

[ZEIT07] Zeitz, P. *The Art and Craft of Problem Solving*. John Wiley, 2007.