Apunts
de
Pre-Àlgebra

Curs 2000–2001 Q1-Q2

Vera Sacristán

Departament de Matemàtica Aplicada II
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

Índex

1 Introducció a la lògica matemàtica

Aquesta introducció a la lògica és força limitada, tant per la seva brevetat com pel seu biaix, ja que pretén ser simplement un reforç per a l'assignatura d'Àlgebra. Alguns temes bàsics es tracten molt superficialment, o ni tan sols no es tracten. S'intenta comentar una mica més tot allò que té a veure amb les demostracions, també des del punt de vista metodològic. A més, es procura que tots els exemples provinguin de les matemàtiques més elementals.

1.1 Proposicions i connectius

Introducció. L'objectiu de la lògica és l'estudi del raonament deductiu formal. Raonaments com ara

tots els homes són mortals,
Socrates és un home,

Socrates és mortal,

en què de dues premisses d'una certa forma en resulta una conclusió (sil·logismes), ja van ser estudiats per Aristòtil. Nosaltres no estem interessats particularment en els sil·logismes, però sí en les deduccions que es poden dur a terme combinant afirmacions com les anteriors.

Proposicions. Les frases més senzilles amb què començarem a treballar són les *proposicions* o *enunciats*, és a dir, frases per a les quals té sentit dir si són certes o falses. Per exemple, *el nombre 5 és primer* és una proposició, com tambe ho és *tots els polígons són convexos.* La frase *x és perpendicular a y* es converteix en una proposició cada cop que es pensen les variables x i y com dues rectes concretes, és a dir, és una forma proposicional que pren un valor de veritat o un altre segons els valors concrets de x i y. En canvi, la frase *el triangle de costats 2, 3, 4 i la paràbola $y = x^2$ són perpendiculars* no és una proposició, ja que el concepte de perpendicularitat no té sentit entre triangles i paràboles.

Connectius. Els enunciats es poden connectar, per tal de formar-ne d'altres de més complicats, mitjançant expressions del tipus *si ... aleshores ...* i similars. Per exemple, *si x és un nombre primer o y és un quadrat perfecte, aleshores $x \cdot y$ no és primer ni és un quadrat perfecte, sempre que x i y siguin diferents.*

Els enunciats es solen representar amb les lletres minúscules $p, q, r, \ldots$ A l'exemple anterior, podem considerar que els enunciats que s'hi combinen són els següents:

p: x és un nombre primer

q: y és un quadrat perfecte

r: $x \cdot y$ és un nombre primer

s: $x \cdot y$ és un quadrat perfecte

t: x i y són diferents

Les expressions que connecten els diversos enunciats s'anomenen *connectius* i els seus símbols són els següents:

negació	$\neg$	$\neg p$ es llegeix *no p*
conjunció	$\wedge$	$p \wedge q$ es llegeix *p i q*
disjunció	$\vee$	$p \vee q$ es llegeix *p o q*
condicional	$\rightarrow$	$p \rightarrow q$ es llegeix *si p aleshores q*
bicondicional	$\leftrightarrow$	$p \leftrightarrow q$ es llegeix *p si, i només si, q*

És possible pensar més connectius, tal com veurem més endavant, però aquests són els més freqüents. Amb aquesta terminologia, l'exemple que estavem tractant s'expressa

$$((p \vee q) \wedge t) \rightarrow ((\neg r) \wedge (\neg s)).$$

Tampoc no cal ser tan rígid amb els parèntesis, tot i que són convenients per tal d'evitar confusions.

1.2 Taules de veritat

Taules de veritat. Tal com hem dit, es tracta d'establir si enunciats com l'anterior (o d'altres de més complicats) són certs o falsos, en funció dels valors de veritat dels seus components. Amb aquest propòsit, es construeixen les anomenades taules de veritat. Els valors de veritat assignats a una proposició poden ser dos: *cert* o *fals*. Aquest fet es representa així, en una petita taula:

p
V
F

De vegades també s'empra la notació

p
1
0

En funció del valor de veritat de p, sabrem el de $\neg p$:

p	$\neg p$
V	F
F	V

Anàlogament, es poden construir les taules de veritat de la resta de connectius:

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

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

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Les taules corresponents a la negació i la conjunció no solen produir discussions, però no es pot dir el mateix de les de la disjunció i el condicional, que no resulten tan intuïtives. Pot ser aquest un bon moment per referir-nos als altres connectius (vegeu l'exercici 3) i també a principis suposadament tan intuïtius com el de no contradicció i el del terç exclòs (vegeu l'exercici 4).

A partir de les taules de veritat dels cinc connectius, es pot fabricar la taula de veritat de qualsevol altre enunciat més complicat. Per exemple, la taula de veritat de $((p \vee q) \wedge (\neg p \to r)) \to q$ és la següent:

p	q	r	$p \vee q$	$\neg p$	$\neg p \to r$	$(p \vee q) \wedge (\neg p \to r)$	$((p \vee q) \wedge (\neg p \to r)) \to q$
V	V	V	V	F	V	V	V
V	V	F	V	F	V	V	V
V	F	V	V	F	V	V	F
V	F	F	V	F	V	V	F
F	V	V	V	V	V	V	V
F	V	F	V	V	F	F	V
F	F	V	F	V	V	F	V
F	F	F	F	V	F	F	V

Exercici 1. Feu les taules de veritat dels enunciats següents:

a) $(p \vee (q \to r)) \leftrightarrow ((p \vee q) \to r)$

b) $((p \vee q) \wedge (p \to \neg r)) \to (r \to q)$

c) $(p \to (q \wedge r)) \wedge (q \vee p) \wedge (q \to r) \wedge \neg(q \wedge r)$

Les proposicions que, com la de l'apartat b de l'exercici anterior, sempre prenen el valor V s'anomenen tautologies, mentre que les que sempre prenen el valor F, com la de l'apartat c, s'anomenen contradiccions. Escriurem $\mathcal{T}$ per representar qualsevol tautologia i $\mathcal{C}$ per representar qualsevol contradicció. L'estudi de les tautologies resulta molt instructiu, com es veurà als exercicis 4 i següents.

Exercici 2. Useu les taules de veritat que calgui per esbrinar si són certes o no les afirmacions següents:

a) Si $2 + 3 = 5$, aleshores $2 = 5 - 3$ i $3 = 5 + 2$.

b) Si $2 + 3 = 6$ o bé $2 = 5 - 3$, aleshores $3 = 6 - 2$.

c) Si $2 + 3 = 5$, aleshores $2 = 6 - 3$ o bé $3 = 5 - 2$.

Exercici 3. Doneu nom i sentit a totes les taules de veritat que es poden formar combinant dos enunciats p i q, és a dir, estudieu tots els connectius binaris.

Exercici 4. Comproveu les tautologies següents. Es tracta de propietats importants de la negació:

a) Principi del terç exclòs: $p \vee \neg p$.

b) Principi de no contradicció: $\neg(p \wedge \neg p)$.

c) Principi de doble negació: $p \leftrightarrow \neg\neg p$.

Les tautologies com aquesta última, on apareix un bicondicional, es solen anomenar *equivalències*, ja que expressen que les dues proposicions lligades pel bicondicional prenen sempre el mateix valor de veritat. Les equivalències s'expressen mitjançant el símbol $\Leftrightarrow$. Per exemple, l'anterior s'escriu $p \Leftrightarrow \neg\neg p$ i es llegeix *p i $\neg\neg p$ són equivalents*. També s'escriu $\Rightarrow$ per expressar que un condicional és tautològic, cas en el qual s'anomena *implicació*. La tautologia $p \Rightarrow q$ també es llegeix *p és condició suficient per a q* o bé *q és condició necessària per a p*.

Exercici 5. Comproveu les equivalències següents. Es tracta de propietats importants de la conjunció:

a) Idempotència: $(p \wedge p) \Leftrightarrow p$.

b) Associativitat: $(p \wedge (q \wedge r)) \Leftrightarrow ((p \wedge q) \wedge r)$.

c) Commutativitat: $(p \wedge q) \Leftrightarrow (q \wedge p)$.

Exercici 6. Expresseu les propietats idempotent, associativa i commutativa per a la disjunció i comproveu-les.

Exercici 7. Verifiqueu les equivalències següents, que expressen propietats importants que relacionen la conjunció i la disjunció entre elles i amb la negació:

a) Absorció:

$$p \wedge (p \vee q) \Leftrightarrow p$$
$$p \vee (p \wedge q) \Leftrightarrow p$$

b) Distributivitat:

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$$

c) De De Morgan:

$$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$$
$$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$$

d) Sense nom:

$$p \Rightarrow p \vee q$$

Quina és la propietat anàloga per a la conjunció?

Exercici 8. Comproveu la validesa dels enunciats següents. Es tracta de les propietats bàsiques del condicional i el bicondicional.

a) Reflexivitat:

$$p \Rightarrow p$$
$$p \Leftrightarrow p$$

b) Transitivitat:

$$((p \rightarrow q) \wedge (q \rightarrow r)) \Rightarrow (p \rightarrow r)$$
$$((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \Rightarrow (p \leftrightarrow r)$$

c) Simetria:

$$(p \leftrightarrow q) \Leftrightarrow (q \leftrightarrow p)$$

d) Antisimetria:

$$(p \rightarrow q) \wedge (q \rightarrow p) \Leftrightarrow (p \leftrightarrow q)$$

L'exercici següent demostra algunes afirmacions ben conegudes com, per exemple, que *d'una contradicció es pot deduir qualsevol cosa* i d'altres de similars.

Exercici 9. Comproveu les equivalències següents:

a) $(p \wedge \mathcal{T}) \Leftrightarrow p$

b) $(p \vee \mathcal{T}) \Leftrightarrow \mathcal{T}$

c) $(p \wedge \mathcal{C}) \Leftrightarrow \mathcal{C}$

d) $(p \vee \mathcal{C}) \Leftrightarrow p$

e) $(\mathcal{T} \rightarrow p) \Leftrightarrow p$

f) $(p \rightarrow \mathcal{T}) \Leftrightarrow \mathcal{T}$

g) $(\mathcal{C} \rightarrow p) \Leftrightarrow \mathcal{T}$

h) $(p \to \mathcal{C}) \Leftrightarrow \neg p$

L'exercici següent exposa algunes propietats del condicional en relació amb els altres connectius, propietats que solen ser emprades en matemàtiques per facilitar la metodologia de les demostracions.

Exercici 10.

a) Estudieu la relació d'implicació entre les afirmacions següents:

   i) Si dues rectes són perpendiculars, aleshores es tallen.
   ii) Si dues rectes no es tallen , aleshores no poden ser perpendiculars.
   iii) Dues rectes qualssevol o bé es tallen o bé no són perpendiculars.
   iv) Si dues rectes es tallen, aleshores són perpendiculars.
   v) No és cert que si dues rectes es tallen aleshores siguin perpendiculars.
   vi) Dues rectes es tallen i no són perpendiculars.

b) Comproveu si són equivalents o no les proposicions següents:

   i) x és múltiple de 2 o de 3.
   ii) Si x no és parell, aleshores és múltiple de 3.
   iii) Si x no és múltiple de 3, aleshores és parell.
   iv) x és parell i múltiple de 3.

c) Relacioneu els enunciats següents:

   i) Si dues rectes es troben sobre un mateix pla, aleshores són paral·leles o bé es tallen.
   ii) Si dues rectes es troben sobre un mateix pla i no es tallen, aleshores són paral·leles.

Exercici 11. Comproveu les implicacions següents:

a) Modus ponens: $(p \wedge (p \to q)) \Rightarrow q$.

b) Modus tollens: $(\neg q \wedge (p \to q)) \Rightarrow \neg p$.

c) Sil·logisme disjuntiu: $(\neg p \wedge (p \vee q)) \Rightarrow q$.

Exercici 12. Quina relació hi ha entre la proposició $r \to (\neg p \to q)$ i la proposició $\neg r \to (q \to \neg p)$?

Exercici 13. Expliqueu perquè es pot expressar tota la lògica de proposicions fent servir tan sols dos connectius, com ara la negació i el condicional, o la negació i la conjunció. Comproveu també que el connectiu "ni ... ni ... "serveix, tot sol, per expressar tota la lògica de proposicions, veient que permet expressar la negació, la disjunció i la conjunció.

1.3 Predicats i quantificadors

En aquest apartat es dóna una visió a vol d'ocell de l'anomenat càlcul de predicats. L'interés es limita essencialment a la manipulació dels quantificadors.

Predicats. Considerem l'exemple següent: *si x és parell i y és senar, aleshores $x+y$ és senar.* Fins ara, hauríem descomposat aquesta proposició de la forma $(p \wedge q) \to r$, on

$$\begin{aligned} &p\colon\ x \text{ és parell} \\ &q\colon\ y \text{ és senar} \\ &r\colon\ x+y \text{ és senar} \end{aligned}$$

Aquest exemple s'hauria pogut estudiar millor considerant el que s'anomenen predicats, és a dir, frases que contenen "variablesçom, per exemple, $p(\ldots)$*: … és parell.* Cada predicat es simbolitza per una lletra minúscula seguida de les variables de les quals depèn, entre parèntesis. El nostre exemple s'escriuria, ara,

$$(p(x) \wedge \neg p(y)) \to \neg p(x+y).$$

Quantificadors. La gràcia dels predicats és que es poden combinar com les proposicions i, alhora, permeten jugar amb les seves variables, quantificant-les. Per exemple, donats els predicats

$$\begin{aligned} p(x) &= x \text{ és primer}, \\ q(x) &= x \text{ és quadrat perfecte}, \\ d(x,y) &= x \text{ i } y \text{ són diferents}, \end{aligned}$$

es poden expressar fàcilment les idees següents:

a) Si x i y són primers diferents, aleshores $x \cdot y$ no és un quadrat perfecte.

b) Per a cada nombre x, el nombre $x \cdot x$ és un quadrat perfecte.

c) Sempre que x i y són primers diferents, el nombre $x \cdot y$ no és quadrat perfecte.

d) Per a cada nombre x que no sigui ni quadrat perfecte ni primer, existeix algun y diferent de x i no quadrat tal que $x \cdot y$ és quadrat perfecte.

L'expressió *per a cada* es simbolitza amb el signe $\forall$, que s'anomena *quantificador universal,* mentre que l'expressió *existeix algun* es simbolitza per $\exists$, que s'anomena *quantificador existencial.* Aleshores, les frases anteriors s'escriuen així:

a) $\forall x\ \forall y\ (p(x) \wedge p(y) \wedge d(x,y)) \to \neg q(x \cdot y)$

b) $\forall x\ q(x \cdot x)$

c) $\forall x\ \forall y\ (p(x) \wedge p(y) \wedge d(x,y)) \to \neg q(x \cdot y))$

d) $\forall x\ ((\neg q(x) \wedge \neg p(x)) \to \exists y(d(x,y) \wedge \neg q(y) \wedge q(x \cdot y)))$

Per extensió, també aquestes noves frases s'anomenen predicats. Els predicats poden, doncs, tenir variables lliures o no tenirles (en aquest cas, es solen anomenar sentències).

Els sil·logismes, que hem esmentat al principi, també treballen amb quantificadors. Per exemple:

les funcions contínues no tenen asímptotes verticals,
algunes funcions racionals són contínues,

algunes funcions racionals no tenen asímptotes verticals.

Exercici 14. Si $s(x, y, z)$ denota el predicat $x + y = z$, mentre que $p(x, y, z)$ denota $xy = z$ i $m(x, y)$ denota $x < y$, expresseu les afirmacions següents:

a) Per a cada x i y, existeix un z tal que $z = x + y$.

b) No existeix cap x més petit que 0.

c) Per a cada x, $x + 0 = x$.

d) Per a cada x, $xy = y$ per a tot y.

e) Existeix un x tal que $xy = y$ per a tot y.

Exercici 15. Expresseu les afirmacions següents, dins l'univers dels nombres enters:

a) Hi ha nombres enters parells.

b) Cada enter és parell o senar.

c) Tots els primers són positius.

d) L'únic primer parell és el 2.

e) Només hi ha un primer parell.

f) No tots els enters són senars.

g) No tots els primers són senars.

h) Si un enter no és senar, aleshores és parell.

Exercici 16. Determineu si, a l'univers dels nombres enters, les proposicions següents són certes o no ho són:

a) $\forall x \; \exists y \; xy = 0$

b) $\forall x \; \exists! y \; xy = 1$

c) $\exists y \; \forall x \; xy = 1$

d) $\exists y \; \forall x \; xy = x$

Exercici 17. Com abans, tots els altres connectius es defineixen a partir del condicional i la negació. Com es definirà el quantificador existencial a partir de l'universal, la negació i el condicional?

Manipulació dels quantificadors. És convenient entendre les equivalències i implicacions que s'exposen a continuació.

a) El predicat $\forall x\ p(x)$ equival a $\forall y\ p(y)$, ja que es tracta simplement d'un canvi de nom. Per exemple, l'afirmació *tots els nombres naturals són positius* es pot escriure d'infinites maneres equivalents:

$$\begin{gathered}\forall x\ (x \in \mathbb{N} \to x \geq 0)\\ \forall y\ (y \in \mathbb{N} \to y \geq 0)\\ \forall z\ (z \in \mathbb{N} \to z \geq 0)\\ \cdots\cdots\cdots\end{gathered}$$

b) El predicat $\forall x\ \forall y\ p(x,y)$ equival a $\forall y\ \forall x\ p(x,y)$. Per exemple, és indiferent expressar la frase *si x és positiu i y és negatiu, aleshores x és més gran que y* de les dues maneres següents:

$$\begin{gathered}\forall x\ \forall y\ ((p(x) \wedge n(y)) \to x > y)\\ \forall y\ \forall x\ ((p(x) \wedge n(y)) \to x > y)\end{gathered}$$

c) En canvi, $\exists x\ \forall y\ p(x,y)$ implica, però no és equivalent, a $\forall y\ \exists x\ p(x,y)$. Per exemple, si $p(x,y)$ simbolitza el predicat *x és més gran que y,* aleshores una d'aquestes frases diu que hi ha un nombre més gran que tots els altres i l'altra diu que cada nombre en té un altre de més gran. És evident que no és el mateix.

d) El predicat $\neg(\forall x\ p(x))$ és equivalent a $\exists x\ \neg p(x)$. Crec que és prou intuitiu.

Exercici 18. Escriviu les equivalències anàlogues a les anteriors a,b i d per al quantificador existencial, i poseu-ne exemples clarificadors.

Exercici 19. Negueu les afirmacions següents, procurant d'entendre el seu sentit:

a) $\forall x, y \in \mathbb{N}\ x = y^2$

b) $\forall x \in \mathbb{N}\ \exists y \in \mathbb{R}\ x = y^2$

c) $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\ x \leq y$

d) $\forall x, y, z \in \mathbb{R}\ x \leq y \wedge y \leq z \Rightarrow x \leq z$

e) $\forall x, y \in \mathbb{R}\ (x > 0 \Rightarrow \exists n \in \mathbb{N}\ y \leq nx)$

f) $\forall \epsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R}\ |x| < \delta \Rightarrow x^2 < \epsilon$

Exercici 20. Expresseu, en termes de la lògica de predicats, les afirmacions següents:

a) Tots els triangles rectangles tenen els tres angles aguts.

b) No és cert que tots els triangles tinguin els tres angles aguts.

c) No és possible que dos nombres positius diferents siguin ambdós múltiples l'un de l'altre.

d) Si un nombre és positiu té arrel quadrada i si és negatiu no en té.

e) No existeixen nombres primers parells.

Exercici 21. Expresseu tots els predicats de l'exercici anterior de manera que cap no comenci amb una negació.

Exercici 22. Considereu la frase *si* $xy = x$ *per a cada* y, *aleshores* $x = 0$. Quina de les dues expressions següents la representa?

$$\forall x \ (\forall y \ xy = x \Rightarrow x = 0)$$
$$\forall x \ \forall y \ (xy = x \Rightarrow x = 0)$$

Exercici 23. Digueu quina relació hi ha (d'equivalència, d'implicació o cap) entre les parelles de predicats següents:

a) $\forall x \ p(x)$
   $\exists x \ p(x)$

b) $\forall x \ (p(x) \wedge q(x))$
   $\forall x \ p(x) \wedge \forall x \ q(x)$

c) $\exists x \ (p(x) \wedge q(x))$
   $\exists x \ p(x) \wedge \exists x \ q(x)$

d) $\forall x \ (p(x) \vee q(x))$
   $\forall x \ p(x) \vee \forall x \ q(x)$

e) $\exists x \ (p(x) \vee q(x))$
   $\exists x \ p(x) \vee \exists x \ q(x)$

f) $\forall x \ (p(x) \rightarrow q(x))$
   $\forall x p(x) \rightarrow \forall x q(x)$

g) $\exists x \ (p(x) \rightarrow q(x))$
   $\exists x \ p(x) \rightarrow \exists x \ q(x)$

h) $\forall x \ (p(x) \rightarrow \exists y q(y))$
   $\forall x p(x) \rightarrow \exists y q(y))$

1.4 Teories formals

Els matemàtics solen delimitar el seu camp de treball, decidint quins objectes i quines propietats els interessen, i solen demostrar els seus teoremes fent servir eines de la lògica a partir d'uns certs axiomes. Aquí se n'ofereixen alguns exemples, amb intenció tan sols informativa. El lector haurà de dirigir-se a la bibliografia si aquest petit esbós li desperta la curiositat.

Geometria afí del pla. Per tal d'estudiar-la, només calen els axiomes següents:

A1. Un pla és un conjunt de punts que conté, almenys, dues rectes diferentes; cada recta és, a la seva vegada, un conjunt de punts que conté, al menys, dos punts diferents.

A2. Donats dos punts diferents qualssevol del pla, existeix una recta, i només una, que els conté els dos.

A3. Per a cada recta r i cada punt p del pla, existex una, i només una, recta que conté p i és paral·lela a r.

Noteu que, per tal d'entendre el tercer axioma, cal una definició prèvia: dues rectes r i s són paral·leles si $r = s$ o bé $r \cap s = \emptyset$.

Geometria euclidiana. De fet, els axiomes anteriors són molt antics, els va postular Euclides. La seva geometria en tenia cinc:

P1. Es pot traçar una línia recta d'un punt a un altre punt.

P2. Un segment es pot perllongar de forma contínua.

P3. Es pot descriure un cercle amb qualsevol centre i qualsevol radi.

P4. Tots els angles rectes són iguals.

P5. Si una recta en talla dues altres formant angles interiors que sumen menys de dos angles rectes, aleshores les dues rectes es tallen pel cantó on es troben els angles interiors que no sumen dos angles rectes.

El cinquè postulat d'Euclides va semblar un teorema a tots els matemàtics fins el segle XIX. El frustrats intents de demostració van permetre observar que és equivalent a d'altres formulacions:

P51. Per un punt exterior a una recta es pot traçar una única paral·lela.

P52. La perpendicular i l'obliqua a una mateixa recta es tallen.

P53. Per tres punts qualssevol sempre es pot traçar una recta o una circumferència.

P54. Etc.

Geometries no euclidianes. La comprovació que el cinquè postulat no es dedueix dels altres va obrir les portes a noves geometries, una les quals, per exemple, postula que per un punt exerior a una recta es poden traçar al menys dues paral·leles (Lobachevski). A més, aquesta és una geometria convenient sobre l'esfera (on una recta és un cercle màxim) on, per exemple, la suma dels angles d'un triangle pot ser més gran que un angle pla.

Aritmètica de Peano. Es basa en cinc axiomes, que caracteritzen el conjunt dels nombres naturals:

N1. $0 \in \mathbb{N}$

N2. $n \in \mathbb{N} \Rightarrow s(n) \in \mathbb{N}$

N3. $\forall n, m \in \mathbb{N}\ s(n) = s(m) \Rightarrow n = m$

N4. $\forall n \in \mathbb{N}\ s(n) \neq 0$

N5. $(A \subset \mathbb{N},\ 0 \in A,\ x \in A \Rightarrow s(x) \in A) \Rightarrow A = \mathbb{N}$

Teoria de grups. Un grup és un conjunt dotat d'una operació interna binària associativa, amb element neutre i amb invers.

Teoria de conjunts. La teoria de conjunts intuitiva pateix de greus problemes. La paradoxa de Russell n'és la prova més òbvia: si anomenem C el conjunt de tots els conjunts que no es pertanyen a ells mateixos com a element, aleshores $C \in C \Leftrightarrow C \notin C$. La formalització de la teoria de conjunts va permetre l'eliminació de les contradiccions i també va donar lloc a discussions sobre la independència dels axiomes (axioma de l'elecció, hipòtesi del continu, ...).

1.5 Metodologia de la demostració

Per acabar, donarem exemples típics de diverses formes de demostració, molt freqüents en matemàtiques, que es justifiquen per tot el que hem après fins ara.

Demostració directa

Exemple: La geometria euclidiana permet demostrar que els angles interiors que una recta determina en tallar dues rectes paral·leles són iguals. A partir d'aquest teorema, demostrarem que la suma dels tres angles d'un triangle és un angle plà. Donat un triangle de vèrtex A, B, C, tracem per C una paral·lela al costat AB. Es formen dos angles nous, que anomenarem $\angle 1$ i $\angle 2$. Aleshores, $\angle 1 = \angle A$ i $\angle 2 = \angle B$ i, com que $\angle 1 + \angle C + \angle 2 =$ angle plà, ja està.

Comentari: Aquest tipus de demostració és, probablement, el més elegant, però molts cops és també el més difícil.

Demostració per casos

Exemple: Volem demostrar la propietat dels nombres reals que diu que l'operació consistent en obtenir el màxim de dos nombres és associativa, és a dir que, si a, b i

c són nombres reals, aleshores

$$\max(\max(a, b), c) = \max(a, \max(b, c)).$$

Es procedeix per casos, que són sis:
Cas 1. Si $a \geq b \geq c$, aleshores

$$\max(\max(a, b), c) = \max(a, c) = a \text{ i } \max(a, \max(b, c)) = \max(a, b) = a.$$

Cas 2. Si $a \geq c \geq b$, aleshores

$$\max(\max(a, b), c) = \max(a, c) = a \text{ i } \max(a, \max(b, c)) = \max(a, c) = a.$$

Cas 3. Si $b \geq a \geq c$, aleshores ...

Comentari: Cal assegurar-se que els casos cobreixen totes les possibilitats, ja que aquest tipus de demostració es basa en el principi del terç exclòs.

Demostració per reducció a l'absurd

Exemple: Volem demostrar que el conjunt dels nombres primers és infinit. Suposem que no ho fos. Hi hauria tan sols una quantitat finita de primers, que anomenarem $p_1, p_2, \ldots, p_n$. Sigui $p = p_1 \cdot \ldots \cdot p_n + 1$. D'una banda, p ja no seria primer i, per tant, seria divisible per algun primer i, d'altra banda, la seva expressió indica que no ho és. Contradicció.

Comentari: Aquest tipus de demostració es basa en el principi de reducció a l'absurd.

Demostració per contrarrecíproc

Exemple: Un nombre natural s'anomena perfecte si és igual a la suma de tots els seus divisors excepte ell mateix. Per exemple,

6 és perfecte, ja que $6 = 1 + 2 + 3$;
18 no és perfecte, ja que $18 \neq 21 = 1 + 2 + 3 + 6 + 9$;
28 és perfecte, ja que $28 = 1 + 2 + 4 + 7 + 14$.

Volem demostrar que si un nombre és perfecte aleshores té divisors propis. Suposem que no tingués divisors propis, és a dir, que fos primer. Aleshores, $p \geq 2$ i p té exactament dos divisors, 1 i p. Per tant, $p \geq 2 > 1$ i p no és perfecte.

Comentari: Les demostracions per contrarrecíproc es basen en l'equivalència del condicional $p \to q$ amb el $\neg q \to \neg p$. Les demostracions per contrarrecíproc també es poden veure com un tipus de demostració per reducció a l'absurd.

Demostració d'una equivalència

Exemple: Si x és un nombre enter, volem demostrar que x és parell si, i només si, x^2 és parell. La demostració té dues parts:
$\Rightarrow$. Si x és parell, es pot escriure $x = 2k$ per un cert $k \in \mathbb{Z}$. Aleshores, $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$ i x^2 és parell.
$\Leftarrow$. La demostració anterior no es pot reaprofitar en sentit invers, de manera que cal pensar una cosa nova. Es pot fer per contrarrecíproc: Si x no és parell, aleshores es pot escriure $x = 2k+1$ per a un cert $k \in \mathbb{Z}$. Llavors, $x^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2 + 2k) + 1$ i x^2 tampoc no és parell.

Comentari: Cal recordar que $p \leftrightarrow q$ és equivalent a $(p \rightarrow q) \wedge (p \leftarrow q)$.

Demostració per contraexemple

Exemple: És cert que tota funció contínua és derivable? No. Per exemple, la funció $f(x) = |x|$ és contínua i no és derivable a l'origen.

Comentari: Si l'afirmació anterior fos certa, la seva demostració no s'hauria pogut fer mitjançant un exemple. Tan sols l'existència es pot demostrar amb un exemple.

Demostració per inducció

Exemple: Volem demostrar que $1 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ $\forall n \geq 1$. En general, donat un predicat aplicable als nombres naturals, el principi d'inducció pot ajudar a la demostració de la sentència

$$\forall n \in \mathbb{N}\ p(n).$$

L'esmentat principi assegura que, demostrant tan sols dues coses:

1. $p(0)$
2. $p(n) \Rightarrow p(n+1)$

s'obté el resultat desitjat: $\forall n \in \mathbb{N}\ p(n)$.

En el cas de l'exemple, com que la propietat ha de valer per a tot $n \geq 1$, demostrem:

1. $p(1)$, ja que
$$\frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 6;$$
2. $1 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \Rightarrow 1 + 2^2 + \ldots + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$, ja que
$$\begin{aligned} 1 + 2^2 + \ldots + n + (n+1)^2 &= \tfrac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \tfrac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \tfrac{(n+1)(n+2)(2n+3)}{6}. \end{aligned}$$

Comentari: No n'hi ha prou amb comprovar uns quants casos. Vegeu sinó la igualtat $3n^2 + 6n + 3 = 3(3n^2 + 1)$, vàlida per a $n = 0, 1, 2$ i no per a $n = 3$.

Demostració "campi qui pugui"

Consisteix a començar pel final i barrejar-ho tot. És el tipus de demostracions que es solen llegir als examens. Però també és, de vegades, l'única forma d'abordar un problema, quan no queden més recursos.

Exemple: Volem demostrar que $1 - \frac{3}{n+1} = \frac{n^2 - 3n + 2}{n^2 - 1}$. Operem així:

$$\begin{array}{lrcl} ? & 1 - \frac{3}{n+1} & = & \frac{n^2-3n+2}{n^2-1} \\ ? & 1 & = & \frac{n^2-3n+2}{n^2-1} + \frac{3}{n+1} \\ ? & 1 & = & \frac{n^2-3n+2+3(n-1)}{n^2-1} \\ ? & 1 & = & \frac{n^2-1}{n^2-1} \\ \text{SÍ} & 1 & = & 1 \end{array}$$

Comentari: El perill d'aquestes demostracions és de fer algun pas cap avall que no es pugui desfer. Per exemple:

$$\begin{array}{lrcl}
? & x-y & = & y-x \\
? & (x-y)^2 & = & (y-x)^2 \\
? & x^2+y^2-2xy & = & y^2+x^2-2yx \\
\text{SÍ} & 0 & = & 0
\end{array}$$

Exercici 24. Trobeu l'error a la falsa demostració anterior.

Exercici 25. Demostreu o refuteu les afirmacions següents, fent constar el mètode emprat:

a) Un enter és senar si, i només si, el seu quadrat és senar.

b) La suma de dos enters parells és parell.

c) La suma d'un parell i un senar és senar.

d) Hi ha dos senars que sumen senar.

e) El quadrat de qualsevol enter és negatiu.

f) Hi ha nombres primers tals que el seu quadrat és parell.

g) No hi ha cap enter x tal que x^2+1 sigui negatiu.

h) La suma de qualssevol dos nombres primers és primer.

i) Existeixen dos primers tals que la seva suma és un nombre primer.

Exercici 26. Demostreu, per reducció a l'absurd, que $\sqrt{2}$ és irracional.

Exercici 27. Demostreu, per inducció, que $1+1\cdot 1!+2\cdot 2!+\cdots+(n-1)(n-1)! = n!$, per a tot $n>1$.

Exercici 28. Demostreu que els termes de la successió de Fibonacci

$$F_1=1; \quad F_2=1; \quad F_n=F_{n-1}+F_{n-2},\ n\geq 3$$

vénen donats per la fórmula següent:

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

2 Introducció a la teoria de conjunts

Aquesta introducció a la teoria de conjunts no és pas formal, sinó un repàs de qüestions que haurien de ser sabudes pels estudiants de secundària. Aquí tan sols es tracta d'exercitar-nos en la manipulació dels conjunts, repassar els conceptes bàsics associats a les relacions d'equivalència i d'ordre, recordar la terminologia associada als diversos tipus d'aplicacions i fer una revisió de les estructures algebraiques bàsiques.

2.1 Conjunts: definició, pertinenca, igualtat i inclusió

Definició d'un conjunt. Pertinença. Un conjunt és un agregat d'objectes per al qual cal que resulti molt clar quins objectes hi ha i quins no. En conseqüència, la manera més explícita de donar un conjunt és per *extensió,* és a dir, enumerant tots els seus elements. Per exemple,

$$A = \{\, 1, 2, 3, 4, 6, 12 \,\}.$$

Aquest mateix conjunt es podria descriure per *comprensió,* és a dir, expressant una propietat que caracteritzi els seus elements. A l'exemple anterior,

$$A = \{\, \text{divisors positius de } 12 \,\}.$$

Com és obvi, les definicions per extensió no són prou pràctiques si el conjunt a definir té molts elements o és infinit, fins i tot es pot prestar a confusió, com per exemple en escriure $B = \{\, 2, 4, \ldots \,\}$. Per la seva banda, les definicions de conjunts per comprensió es fan a partir de predicats, que ja coneixem del tema anterior. Així, es sol escriure

$$A = \{\, x \mid x \text{ és divisor de } 12 \,\}.$$

Tanmateix, cal recordar que hi ha predicats que no es poden emprar per a definir conjunts, com ara

$$C = \{\, x \mid x \notin x \,\}.$$

Recordeu que el símbol $\in$ indica la *relació de pertinença* i que la seva negació s'escriu $\notin$. Així, per exemple,

$$3 \in \{\, x \mid x \text{ és divisor de } 12 \,\} \qquad \text{i} \qquad 5 \notin \{\, \text{x} \mid \text{x és divisor de } 12 \,\}.$$

Conjunts notables. Alguns tipus de conjunts tenen nom propi, com ara el *conjunt buit,* o conjunt que no conté cap element, que es simbolitza $\emptyset$ o també $\{\,\}$; els conjunts d'un sol element, anomenats *singletons,* o els de dos elements, anomenats *parells.*

Igualtat entre conjunts. Tal com hem vist, un mateix conjunt pot definir-se de diverses maneres. Com saber, doncs, si dos conjunts donats són iguals? Dos conjunts *A i B són iguals* si contenen els mateixos elements, és a dir, si tots els elements de A són de B i tots els de B són de A:

$$A = B \iff \forall x \ (x \in A \Leftrightarrow x \in B).$$

Propietats. Les propietats més importants de la igualtat de conjunts són les següents:

Reflexiva:	$A = A$.
Simètrica:	$A = B \Rightarrow B = A$.
Transitiva:	$A = B$ i $B = C \Rightarrow A = C$.

Una relació que, com la igualtat, compleixi aquestes tres propietats es diu d'equivalència. Noteu que aquestes propietats corresponen a les que ja hem estudiat del bicondicional, a través del qual hem definit la igualtat.

Exercici 1. Ja sabem què vol dir que dos conjunts siguin iguals. Com expressarieu, ara, que dos conjunts són diferents? Feu-ho tant formalment com us sigui possible.

Exercici 2. Satisfà la relació de desigualtat alguna de les propietats d'una relació d'equivalència?

Inclusió entre conjunts. Tots els múltiples de 2 són nombres naturals. Això s'expressa dient que el conjunt dels nombres parells P *està inclòs* dins el conjunt dels nombres naturals $\mathbb{N}$: n'és un *subconjunt.* Es sol escriure

$$P \subset \mathbb{N} \quad \text{o també} \quad P \subseteq \mathbb{N}.$$

En general, un conjunt A està inclòs dins un altre conjunt B si tots els elements de A ho són de B:

$$A \subset B \Longleftrightarrow \forall x \ (x \in A \Rightarrow x \in B).$$

Propietats. Com que la inclusió es defineix a través del condicional, les propietats que en resulten són les següents:

Reflexiva:	$A \subset A$.
Antisimètrica:	$A \subset B$ i $B \subset A \Rightarrow A = B$.
Transitiva:	$A \subset B$ i $B \subset C \Rightarrow A \subset C$.

Les relacions que, com la inclusió, satisfan aquestes tres propietats s'anomenen d'ordre.

Exercici 3. Satisfà la inclusió la propietat de simetria?

Exercici 4. Expresseu formalment la relació de no inclusió. Quines propietats satisfà?

Exercici 5. Quina relació d'inclusió hi ha entre el conjunt buit i un altre conjunt qualsevol?

Parts d'un conjunt. Donat un conjunt A, es poden considerar tots els seus subconjunts. Per exemple, el conjunt $A = \{1, 2, 3, 4\}$ té, com a subconjunts:

$$\begin{gathered}\emptyset = \{\ \}, \\ \{1\}, \{2\}, \{3\}, \{4\}, \\ \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \\ \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \\ \{1,2,3,4\} = A.\end{gathered}$$

El conjunt que té per elements tots els subconjunts d'un conjunt A s'anomena *conjunt de les parts de* A i es denota $\mathcal{P}(A)$. És a dir,

$$\mathcal{P}(A) = \{ B \mid B \subset A \}, \quad \text{o sigui} \quad B \in \mathcal{P}(A) \Longleftrightarrow B \subset A.$$

Exercici 6. Caluleu $\mathcal{P}(\emptyset)$, $\mathcal{P}(\{a\})$, $\mathcal{P}(\{a, b\})$ i $\mathcal{P}(\{a, b, c\})$.

Exercici 7. Tenint en compte el resultat de l'exercici anterior i el de l'exemple, quants elements creieu que té $\mathcal{P}(A)$ si A en té n?
Exercici 8. Demostreu:

a) $X \subset Y \Longleftrightarrow \mathcal{P}(X) \subset \mathcal{P}(Y)$;

b) $\mathcal{P}(E) = \mathcal{P}(F) \Longrightarrow E = F$.

2.2 Operacions entre conjunts

Intersecció. Donats dos conjunts A i B, es pot considerar un nou conjunt, que s'anomena *intersecció* de A i B, format per tots els objectes que pertanyen a A i B alhora:

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

Per exemple, el conjunt dels múltiples de 6 és la intersecció del conjunt dels nombres parells i el dels múltiples de 3.
Pot passar que $A \cap B = \emptyset$, i aleshores es diu que A i B són *disjunts.* Per exemple, dues rectes paral·leles, considerades com conjunts de punts, són disjuntes.

Reunió. També es pot considerar el conjunt, anomenat *reunió* de A i B, format ajuntant els elements d'ambdós conjunts:

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

Per exemple, $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Tanmateix, no cal que els conjunts siguin disjunts per a considerar-ne la reunió (penseu en la definició de la disjunció!). Per exemple, $2\mathbb{Z} \cup 3\mathbb{Z}$.

Diferència. Finalment, també pot tenir interès el conjunt, anomenat *diferència* entre A i B, format pels elements de A que no pertanyen a B:

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

Per exemple, $\mathbb{R}^* = \mathbb{R} \setminus \{ 0 \}$.

Propietats. En primer lloc s'exposen les propietats més emprades de la intersecció:

Idempotència:	$A \cap A = A$.
Associativitat:	$A \cap (B \cap C) = (A \cap B) \cap C$.
Commutativitat:	$A \cap B = B \cap A$.
Conjunt buit:	$A \cap \emptyset = \emptyset$.

Exercici 9. Demostreu les propietats anteriors i enuncieu-ne les duals. Trobeu algun lligam amb les propietats que coneixeu de la conjunció i la disjunció?

Exercici 10. Estudieu el comportament de la diferència de conjunts respecte de les propietats anteriors.

Algunes propietats relacionen la intersecció amb la unió:

Absorció:	$A \cap (A \cup B) = A$.
Distributivitat:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Exercici 11. Demostreu les propietats anteriors i les seves duals. Digueu com es comporta la diferència. Concretament, pel que fa a l'absorció, estudieu els conjunts següents:

$$A \cap (A \setminus B)$$
$$A \cup (A \setminus B)$$
$$A \setminus (A \cap B)$$
$$A \setminus (A \cup B)$$
$$(A \cap B) \setminus A$$
$$(A \cup B) \setminus A$$

Pel que fa a la distributivitat:

$$(A \cap B) \setminus C$$
$$(A \cup B) \setminus C$$
$$A \setminus (B \cap C)$$
$$A \setminus (B \cup C)$$
$$A \cap (B \setminus C)$$
$$A \cup (B \setminus C)$$

Exercici 12. Demostreu les propietats següents, si són certes, o trobeu-ne un contraexemple:

a) $A \setminus B = A \Leftrightarrow A \cap B = \emptyset \Leftrightarrow B \setminus A = B$

b) $A \subset B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow A \setminus B = \emptyset$

Exercici 13. Donats tres conjunts, què creieu que vol dir que siguin disjunts dos a dos i perquè no és el mateix que dir que són disjunts?

Exercici 14. Compoveu si són certes o no les proposicions següents:

a) $A \subset B \subset C \iff A \cup B = B \cap C$

b) $(A \cup B) \subset (A \cup C) \Longrightarrow B \subset C$

c) $(A \cup B) \subset (A \cup C) \wedge (A \cap B) \subset (A \cap C) \Longrightarrow B \subset C$

Exercici 15. Compareu $\mathcal{P}(X \cap Y)$ amb $\mathcal{P}(X) \cap \mathcal{P}(Y)$. El mateix per a la reunió.

Complementari d'un conjunt. De vegades, fent matemàtiques, hom es mou dins un referent fix. Per exemple, quan parlem dels nombres parells, primers, quadrats perfectes, etc, sembla obvi que el referent és el conjunt dels nombres naturals. Aquest conjunt de referència s'anomena *univers* o *referent.* Algunes vegades pot tenir interès parlar del conjunt diferència entre l'univers i un conjunt donat. Per exemple, el conjunt dels nombres senars és la diferència entre l'univers $\mathbb{N}$ i el conjunt dels parells; el conjunt dels nombres compostos és la diferència entre l'univers i el conjunt dels primers, etc. Els conjunts així obtinguts s'anomenen *complementaris:* el conjunt dels nombres senars és el complementari del dels nombres parells dins l'univers dels naturals. En general, si dins un univers $\mathcal{U}$ es considera un conjunt $A \subset \mathcal{U}$, el seu complementari és

$$A^c = \mathcal{C}(A) = A' = \overline{A} = \mathcal{U} \setminus A = \{\, x \in \mathcal{U} \mid x \notin A \,\}.$$

Propietats. Com és obvi, aquest conjunt es construeix mitjançant la negació, de manera que les propietats són les previstes:

a) $A \cup A^c = \mathcal{U}$

b) $A \cap A^c = \emptyset$

c) $A^{cc} = A$

d) $(A \cap B)^c = A^c \cup B^c$
$(A \cup B)^c = A^c \cap B^c$
(Lleis de De Morgan)

Exercici 16. Comproveu les proposicions següents:

a) $A \subset B \iff B^c \subset A^c$

b) $(A \setminus B)^c = A^c \cup B$

c) $A \setminus B = A \cap B^c$

d) $A \setminus \mathcal{U} = \emptyset$

e) $A \cap \mathcal{U} = A$

f) $A \cup \mathcal{U} = \mathcal{U}$

g) $\emptyset^c = \mathcal{U}$

h) $\mathcal{U}^c = \emptyset$

Exercici 17. Simplifiqueu les expressions següents:

a) $(A \cap B^c) \cap (A^c \cap B^c)$

b) $(A \cap B \cap C) \cup ((A^c \cup B^c) \cup C^c)$

c) $(A \cap (A^c \cup B)) \cup (B \cap (B \cup C)) \cup B$

Operacions generalitzades. Donada una família de conjunts qualssevol $\{A_i\}_{i\in I}$, pot tenir interès estudiar la seva reunió o intersecció:

$$\begin{aligned} \textstyle\bigcup_{i\in I} A_i &= \{x \mid \exists i \in I \ x \in A_i\} \\ \textstyle\bigcap_{i\in I} A_i &= \{x \mid \forall i \in I \ x \in A_i\} \end{aligned}$$

Exercici 18. Expresseu de forma més senzilla els conjunts següents:

$$\bigcup_{i=1}^{\infty}[i-1, i) \qquad \bigcap_{i=1}^{\infty}\left(-\frac{1}{n}, \frac{1}{n}\right) \qquad \bigcap_{i=1}^{\infty}\left(0, \frac{1}{n}\right)$$

Exercici 19. Demostreu les lleis de De Morgan generalitzades:

$$\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c \qquad \left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c$$

Producte cartesià. El producte cartesià de dos conjunts A i B és el conjunt $A \times B$ que té com elements tots els parells ordenats formats per un primer element de A i un segon element de B:

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

D'aquesta manera, noteu que $A \times B \neq B \times A$.

Exercici 20. Escriviu $A \times B$ en els casos següents:

a) $A = \{a\}$ i $B = \{1, 2\}$.

b) $A = \{a, b\}$ i $B = \{1, 2\}$.

c) $A = \{a, b, c\}$ i $B = \{1, 2\}$.

d) $A = B = \{a, b, c, d\}$.

e) $A = [a, b] \subset \mathbb{R}$ i $B = [c, d] \subset \mathbb{R}$.

f) $A = \{x \in \mathbb{R} \mid |x| < 1\}$ i $B = \mathbb{R}$.

Exercici 21. Demostreu:

a) Distributivitat de $\times$ respecte de $\setminus$:

$$\begin{aligned} A \times (B \setminus C) &= (A \times B) \setminus (A \times C) \\ (A \setminus B) \times C &= (A \times C) \setminus (B \times C) \end{aligned}$$

b) Distributivitat de $\times$ respecte de $\cup$:

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C) \\ (A \cup B) \times C &= (A \times C) \cup (B \times C) \end{aligned}$$

c) Distributivitat de $\times$ respecte de $\cap$:

$$\begin{aligned} A \times (B \cap C) &= (A \times B) \cap (A \times C) \\ (A \cap B) \times C &= (A \times C) \cap (B \times C) \end{aligned}$$

Exercici 22. Demostreu:

a) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

b) $(A \cup B) \times (C \cup D) = (A \times C) \cup (A \times D) \cup (B \times C) \cup (B \times D)$

2.3 Relacions

Una relació binària dins un conjunt A és un subconjunt R del producte cartesià $A \times A$: $R \subseteq A \times A$. En lloc de $(x, y) \in R$, es sol escriure xRy, que es llegeix x *està relacionat amb* y. Per exemple, donat el conjunt $A = \{2, 3, 4, 5, 7, 9, 16, 18\}$, es poden considerar relacions com les següents:

$$\begin{aligned} xR_1y &\iff x \text{ és divisor de } y \\ xR_2y &\iff x \text{ és el quadrat de } y \\ xR_3y &\iff y - x = 2 \\ xR_4y &\iff x + y = 30 \end{aligned}$$

El resultat és el següent:

$$\begin{aligned} R_1 &= \{(2,2), (2,4), (2,16), (2,18), (3,3), (3,9), (3,18), \\ &\qquad (4,4), (4,16), (5,5), (7,7), (9,9), (9,18), (16,16), (18,18)\} \\ R_2 &= \{(4,2), (9,3), (16,4)\} \\ R_3 &= \{(2,4), (3,5), (5,7), (7,9), (16,18)\} \\ R_4 &= \emptyset \end{aligned}$$

Relacions d'equivalència. Una relació R es diu d'equivalència si és

$$\begin{array}{ll} \text{Reflexiva:} & \forall x \quad xRx. \\ \text{Simètrica:} & \forall x, y \quad xRy \Rightarrow yRx. \\ \text{Transitiva:} & \forall x, y, z \quad xRy \wedge yRz \Rightarrow xRz. \end{array}$$

Exercici 23. Demostreu que, dins el conjunt de les rectes del pla, la relació de paral·lelisme és d'equivalència i la de perpendicularitat no ho és.

Exercici 24. Considereu, dins el conjunt $\mathbb{Z}$, un nombre enter fixat, n. Demostreu que la relació $xRy \iff n \mid y - x$ és d'equivalència.

Exercici 25. Demostreu que la relació $(a,b)R(c,d) \iff a + d = b + c$ és d'equivalència a $\mathbb{N} \times \mathbb{N}$ i que la relació $(a,b)R(c,d) \iff ad = bc$ ho és a $\mathbb{Z} \times \mathbb{Z}$.

Classes d'equivalència i conjunt quocient. Si R és una relació d'equivalència al conjunt A, s'anomenen *classes d'equivalència* els subconjunts

$$[a] = \overline{a} = \{x \in A \mid xRa\}.$$

Noteu certes propietats de les classes d'equivalència, com ara:

$$\begin{array}{l} a \in [a] \\ [a] = [b] \iff aRb \\ [a] \cap [b] = \emptyset \iff a \not R b \end{array}$$

Les classes d'equivalència formen una partició del conjunt A, és a dir:

$$\begin{array}{l} \emptyset \neq [a] \subseteq A \quad \forall a \in A \\ [a] \cap [b] = \emptyset \quad \forall [a] \neq [b] \\ \bigcup_{a \in A} [a] = A \end{array}$$

Exercici 26. Formeu les classes d'equivalència corresponents a les relacions dels exercicis anteriors.

El *conjunt quocient* d'un conjunt A per una relació d'equivalència R és el conjunt de les classes d'equivalència que R determina sobre A:

$$A/R = \{[a] \mid a \in A\}.$$

Exercici 27. Quina relació d'equivalència sobre el conjunt de les fraccions permet definir el conjunt $\mathbb{Q}$ dels nombres racionals com a quocient?

Exercici 28. Comproveu que els conjunts quocients que determinen les relacions dels exercicis 23 a 25 són, respectivament, el conjunt de les direccions sobre el pla, el conjunt $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, el conjunt $\mathbb{Z}$ i el conjunt $\mathbb{Q}$.

Relacions d'ordre. Una relació R es diu d'ordre si és

$$\begin{array}{ll} \text{Reflexiva:} & \forall x \quad xRx. \\ \text{Antisimètrica:} & \forall x,y \quad xRy \wedge yRx \Rightarrow x=y. \\ \text{Transitiva:} & \forall x,y,z \quad xRy \wedge yRz \Rightarrow xRz. \end{array}$$

Exercici 29. Demostreu que, al conjunt dels nombres reals, la relació $xRy \iff x \leq y$ és d'ordre.

Exercici 30. Demostreu que, al conjunt dels nombre naturals, la relació definida per $xRy \iff x \mid y$ és d'ordre.

Exercici 31. Demostreu que, donat un conjunt A qualsevol, la relació $xRy \iff x \subseteq y$ és una relació d'ordre dins $\mathcal{P}(A)$.

Es diu que una relació d'ordre és *total* si tots els elements són comparables, és a dir, si

$$\forall x,y \quad xRy \vee yRx.$$

En cas contrari, es diu que l'ordre és *parcial.*

Exercici 32. Demostreu que l'ordre definit a l'exercici 29 és total, mentre que el de l'exercici 30 és parcial. Com ha de ser el conjunt A per tal que l'ordre de l'exercici 31 sigui total?

Elements distingits en una relació d'ordre. Sigui $(B,\leq)$ un conjunt ordenat. Considerem $A \subseteq B$, $a \in A$ i $b \in B$. Considereu les definicions següents:

$$\begin{array}{rcl} a \text{ és un mínim de } A & \iff & \forall x \in A \; a \leq x \\ a \text{ és un màxim de } A & \iff & \forall x \in A \; x \leq a \\ a \text{ és minimal dins } A & \iff & \neg\exists x \in A \; x \leq a \\ a \text{ és maximal dins } A & \iff & \neg\exists x \in A \; a \leq x \\ b \text{ és una fita inferior de } A & \iff & \forall x \in A \; b \leq x \\ b \text{ és una fita superior de } A & \iff & \forall x \in A \; x \leq b \\ b \text{ és l'ínfim de } A & \iff & b \text{ és la més gran de les fites inferiors de } A \\ b \text{ és el suprem de } A & \iff & b \text{ és la més petita de les fites superiors de } A \end{array}$$

Per exemple, si considereu l'interval real $[-1,1)$, podeu comprovar que té mínim (el nombre -1) però no té màxim. En canvi, té suprem (el nombre 1). De fites superiors en té moltes: per exemple, π, 312, 1, etc. En canvi, el conjunt $A = \{x \in \mathbb{R} \mid x = \frac{1}{n}, n \in \mathbb{N}\}$ té màxim però no té mínim, tot i tenir ínfim. La semirrecta positiva, $[0,\infty)$ té mínim, però no té ni màxim, ni suprem, ni cap fita superior. Per últim, el conjunt $A = \{2,3,6,9,12,36\}$, ordenat per divisibilitat, té màxim (el nombre 36) però no té mínim. En canvi, sí que té elements minimals (els nombres 2 i 3).
És important observar que el màxim (respectivament, mínim) d'un conjunt, si existeix, és únic. El suprem (resp. ínfim) d'un conjunt, si existeix, és unic. El màxim (mínim) si existeix, coincideix amb el suprem (ínfim). El suprem (ínfim), si existeix

i és un element del conjunt, aleshores és el màxim (mínim) del conjunt. El màxim (mínim), si existeix, és l'únic maximal (minimal).

Exercici 33. Considereu a $\mathbb{N}$ les relacions donades per

a) $x + y = 10$

b) $x \mid y$

c) $x \leq y$

i estudieu-ne les propietats. Per aquelles que siguin d'equivalencia, determineu-ne el conjunt quocient. Per aquelles que siguin d'ordre, determineu si l'ordre és total o parcial.

Exercici 34. Al conjunt dels segments del pla, es defineix la relació següent: *dos segments estan relacionats quan pertanyen a una mateixa recta.* Estudieu aquesta relació.

Exercici 35. Al conjunt $\mathbb{C}$ dels nombres complexos es defineix la relació

$$a + bi \preceq c + di \iff a < c \vee (a = c \wedge b \leq d).$$

Proveu que és un ordre. És total?

Exercici 36. Construcció d'un ordre a partir d'un preordre.
Si R és un *preordre* dins el conjunt A (una relació reflexiva i transitiva), la relació d'equivalència induïda per R és

$$a \equiv b \iff aRb \wedge bRa.$$

Proveu que $\equiv$ és, efectivament, una relació d'equivalència. Demostreu que la relació R indueix sobre $A/\equiv$ una relació d'ordre (cal demostrar, primer de tot, que està ben definida). Com aplicació, estudieu l'exemple següent:

$$\forall x, y \in \mathbb{Z}, \quad xRy \iff x \mid y.$$

Exercici 37. Estudieu les propietats de la relació següent sobre $\mathbb{N}$ i sobre $\mathbb{R}$:

$$xRy \iff \left[\frac{x}{2}\right] = \left[\frac{y}{2}\right].$$

Exercici 38. El mateix que a l'exercici anterior, ara per

$$xRy \iff \left[\sqrt{x}\right] = \left[\sqrt{y}\right].$$

4. APLICACIONS

Conceptes bàsics. Una aplicació f d'un conjunt A en un conjunt B s'ha de pensar com un mecanisme que permet, a partir de cada element de A, obtenir un element de B. S'escriu $f : A \to B$ i, per cada $x \in A$, l'element de B corresponent es denota $f(x)$ i s'anomena *imatge* de x per f. Formalment f és un subconjunt de $A \times B$ amb una peculiaritat: els parells (x, y), amb $x \in A$ i $y \in B$ que el formen han de ser tals que, per cada $x \in A$, hi hagi un únic parell (x, y) del subconjunt.

Exemples. La funció "elevar al quadrat"assigna a cada nombre enter un nombre natural: $f(x) = x^2, \ \forall x \in \mathbb{Z}$.

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{N} \\ & x & \mapsto & x^2 \end{array}$$

La funció "valor absolut"assigna a cada nombre real un nombre real positiu:
$g(x) = |x|, \ \forall x \in \mathbb{R}$.

$$\begin{array}{rccc} g: & \mathbb{R} & \to & \mathbb{R}^+ \\ & x & \mapsto & |x| \end{array}$$

La funció "multiplicar per dos"assigna a cada nombre natural un altre nombre natural: $h(x) = 2x, \ \forall x \in \mathbb{N}$.

$$\begin{array}{rccc} h: & \mathbb{N} & \to & \mathbb{N} \\ & x & \mapsto & 2x \end{array}$$

La funció "arrel quadrada positiva"assigna a cada real positiu un real positiu:
$t(x) = +\sqrt{x}, \ \forall x \in \mathbb{R}^+$.

$$\begin{array}{rccc} t: & \mathbb{R}^+ & \to & \mathbb{R}^+ \\ & x & \mapsto & +\sqrt{x} \end{array}$$

Considerem una aplicació $f : A \to B$. El conjunt A s'anomena *domini* de la funció f:

$$\mathrm{Dom} f = A.$$

El conjunt *imatge* o *recorregut* de f és

$$\mathrm{Im} f = f(A) = \{y \in B \mid y = f(x), x \in A\}.$$

La imatge de f és un subconjunt de B que pot no coincidir amb B.
Donat un element $y \in B$, s'anomena *anti-imatge* de y per f el conjunt

$$f^{-1}(y) = \{x \in A \mid f(x) = y\}.$$

L'anti-imatge d'un element $y \in B$ és un subconjunt de A que pot ser des del conjunt buit fins a tot A.

Exercici 39. Si f, g, h, t són les funcions dels exemples anteriors,

a) Calculeu Im f, $f(3)$, $f^{-1}(16)$ i $f^{-1}(2)$.

b) Calculeu Im g, $g(-\pi)$, $g(\pi)$ i $g^{-1}(7/3)$.

c) Calculeu Im h, $h(2)$, $h^{-1}(2)$ i $h^{-1}(3)$.

d) Calculeu Im t, $t(25)$ i $t^{-1}(3)$.

Exercici 40. Sigui f una funció real de variable real tal que $f(x-1) = x^2$. Calculeu $f(x+1)$.

Una aplicació $f : A \to B$ s'anomena *injectiva* si és tal que dos elements diferents de A sempre tenen imatges diferents:

$$\forall x, y \in A, \qquad f(x) = f(y) \Rightarrow x = y.$$

Una aplicació $f : A \to B$ s'anomena *exhaustiva* si cada element de B és imatge d'algun element de A:

$$\forall y \in B \ \exists x \in A \quad f(x) = y.$$

Una aplicació s'anomena *bijectiva* si és injectiva i exhaustiva.

Exercici 41. Estudieu si les funcions f, g, h i t són injectives, exhaustives o bijectives.

Exercici 42. Sigui $f : A \to B$ una aplicació. Demostreu les equivalències següents:

$$\begin{aligned} f \text{ és injectiva} &\iff \forall y \in B,\ f^{-1}(y) \text{ és el conjunt buit o un singletó} \\ f \text{ és exhaustiva} &\iff \forall y \in B,\ f^{-1}(y) \text{ és no buit} \\ f \text{ és bijectiva} &\iff \forall y \in B,\ f^{-1}(y) \text{ és un singletó} \end{aligned}$$

Composició d'aplicacions. Donades dues aplicacions $f : A \to B$ i $g : B \to C$, es pot considerar la seva composició. Es tracta d'una nova aplicació, $g \circ f : A \to C$, definida per $g \circ f(x) = g(f(x)) \ \forall x \in A$. En general, per efectuar la composició $g \circ f$, cal que $\mathrm{Im}\ f \subseteq \mathrm{Dom}\ g$.
Per exemple, si f i g són les funcions

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{N} \\ & x & \mapsto & x^2 \end{array} \qquad \begin{array}{rccc} g: & \mathbb{N} & \to & \mathbb{P} \\ & x & \mapsto & 2x \end{array}$$

aleshores $g \circ f$ és

$$\begin{array}{rccc} g \circ f: & \mathbb{Z} & \to & \mathbb{P} \\ & x & \mapsto & 2x^2 \end{array}$$

En canvi, si f i g són les funcions

$$\begin{array}{rccc} f: & \mathbb{C} & \to & \mathbb{R} \\ & x+iy & \mapsto & x \end{array} \qquad \begin{array}{rccc} g: & \mathbb{R}^+ & \to & \mathbb{R}^+ \\ & x & \mapsto & +\sqrt{x} \end{array}$$

aleshores és impossible dur a terme la composició $g \circ f$, ja que $\mathrm{Im}\ f = \mathbb{R} \not\subseteq \mathbb{R}^+ = \mathrm{Dom}\ g$.

Exercici 43. Donades les funcions $f(x) = x^2 - 1$, $g(x) = 3x - 1$ i $h(x) = \frac{1}{1+x^2}$, trobeu $f \circ f \circ f$, $(h \circ g) \circ f$ i $h \circ (g \circ f)$.

Exercici 44. Siguin $f(x) = x^2$ i $g(x) = 2^x$. Calculeu $g \circ f$ i $f \circ g$ i compareu els resultats.

Exercici 45. Demostreu que la composició d'aplicacions bijectives és bijectiva. Què passa si es componen dues aplicacions injectives o dues d'exhaustives? I una de cada?

La composició d'aplicacions té dues propietats fonamentals. En primer lloc, la composició és associativa:

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

En segon lloc, l'aplicació *identitat*, que aplica cada element del domini en ell mateix,

$$\begin{array}{rccc} I_A : & A & \to & A \\ & x & \mapsto & x \end{array}$$

es comporta com a element neutre de la composició: $f \circ I = I \circ f = f$.
En canvi, la composició d'aplicacions no és commutativa. En general (vegeu l'exercici 44), $f \circ g \neq g \circ f$. De fet, molts cops alguna de les dues composicions ni tan sols no té sentit.

Aplicació inversa. Donada una aplicació $f : A \to B$, que hem acordat pensar com un mecanisme que, donat un element $x \in A$, fabrica un $y \in B$, té sentit que ens plantegem quan aquest procés es pot "desfer", és a dir, quan és possible, donat $y \in B$, trobar l'element $x \in A$ del qual "provenia". Més formalment, direm que una aplicació $f : A \to B$ és *invertible* quan existeixi una aplicació $g : B \to A$ tal que

$$\begin{aligned} g \circ f &= I_A \\ f \circ g &= I_B \end{aligned}$$

Exercici 45. Demostreu que si f és invertible aleshores la seva inversa, g, és única. Per això, g es sol escriure f^{-1}. És g invertible?

Com és possible saber si una aplicació f és invertible? Si l'aplicació f no és injectiva, la seva inversió no és possible, ja que l'element $y \in B$ pot provenir de diversos $x \in A$. És el cas de la funció

$$\begin{array}{rccc} f : & \mathbb{R} & \to & \mathbb{R}^+ \\ & x & \mapsto & |x| \end{array}$$

Si l'aplicació f no és exhaustiva, la seva inversió tampoc no és possible, ja que l'element $y \in B$ pot no provenir de cap element $x \in A$. És el cas de la funció

$$\begin{array}{rccc} f : & \mathbb{N} & \to & \mathbb{N} \\ & x & \mapsto & 2x \end{array}$$

En canvi, si l'aplicació és bijectiva, el procés d'invertir-la sempre és possible, ja que a cada element $y \in B$ correspon un únic element $x \in A$ tal que $f(x) = y$. Per tant, $g(y) = x$. En resum,

$$f \text{ és invertible} \iff f \text{ és bijectiva.}$$

Exercici 46. Donada f, trobeu f^{-1}, si existeix, i digueu quin és el seu domini:

$$\begin{aligned} f(x) &= 2x - 1; \\ f(x) &= x^2; \\ f(x) &= \tfrac{1}{+\sqrt{x}}; \\ f(x) &= \tfrac{1}{x-5}. \end{aligned}$$

Equipotència. Si A i B són dos conjunts finits, és força obvi el fet que A i B tenen el mateix nombre d'elements si, i només si, és possible establir una bijecció entre ells. Aquesta idea permet generalitzar el concepte de "mateix nombre d'elements" a conjunts qualssevol, possiblement infinits: dos conjunts són *equipotents* si és possible establir una bijecció de l'un a l'altre.

Exercici 47. Demostreu que l'equipotència és una relació d'equivalència.

Exercici 48. Demostreu que el conjunt dels nombres naturals i el dels nombres parells són equipotents. Això descobreix una característica dels conjunts infinits: són equipotents a alguns dels seus subconjunts.

Exercici 49. Demostreu que $\mathbb{N}$ i $\mathbb{Z}$ són equipotents.

Exercici 50. Demostreu que $\mathbb{R}^+$ és equipotent a l'interval $[0,1]$. Demostreu que $\mathbb{R}$ és equipotent a l'interval $[0,1]$.

Exercici 51. Els conjunts equipotents a $\mathbb{N}$ s'anomenen numerables. Aquest exercici demostra que $\mathbb{R}$ no és numerable. Per això, com que $\mathbb{R}$ i $[0,1]$ són equipotents, tan sols cal que demostreu que $[0,1]$ no és equipotent a $\mathbb{N}$. Raoneu per reducció al absurd. Si $[0,1]$ i $\mathbb{N}$ fossin equipotents, es tindria una bijecció

$$\begin{array}{ccl} \mathbb{N} & \to & [0,1] \\ 0 & \mapsto & 0.a_1a_2a_3\ldots \\ 1 & \mapsto & 0.b_1b_2b_3\ldots \\ 2 & \mapsto & 0.c_1c_2c_3\ldots \\ 3 & \mapsto & 0.d_1d_2d_3\ldots \\ \vdots & & \vdots \end{array}$$

Formeu el nombre $x = 0.x_1x_2x_3x_4\ldots$, on $x_1 \neq a_1$, $x_2 \neq b_2$, $x_3 \neq c_3$, $x_4 \neq d_4$, i així successivament. Quina anti-imatge té el nombre x?

2.4 Operacions

Una operació binària interna sobre un conjunt A és una aplicació

$$* : A \times A \to A.$$

Es sol escriure $a * b$ en lloc de $*(a,b)$. Exemples d'operacions binaries internes són la suma de nombres naturals, el producte de nombres complexos o la intersecció de subconjunts d'un conjunt donat.

Propietats. Les operacions que estudiarem satisfan certes propietats. Per exemple, la suma de nombres enters és commutativa, ja que és el mateix sumar $a+b$ que $b+a$. En canvi, la diferència no ho és, ja que el resultat de l'operació $a-b$ no és el mateix que $b-a$. Aquestes són les propietats que ens interessarà estudiar:

Associativa:	$a*(b*c)=(a*b)*c \quad \forall a,b,c\in A.$
Commutativa:	$a*b=b*a \quad \forall a,b\in A.$
Element neutre:	$\exists e\in A\ \forall a\in A \quad e*a=a*e=a.$
Element simètric:	$\forall a\in A\ \exists a'\in A \quad a*a'=a'*a=e.$
Distributiva:	(de $*$ respecte de $\circ$)
	$a*(b\circ c)=(a*b)\circ(a*c) \quad \forall a,b,c\in A.$
	$(b\circ c)*a=(b*a)\circ(c*a) \quad \forall a,b,c\in A.$

Exercici 52. Considereu els conjunts següents, amb les operacions que s'indiquen, i estudieu quines de les propietats anteriors s'hi compleixen:

$$(\mathbb{N},+); \qquad (\mathbb{Z},+); \qquad (\mathbb{Q},+,\cdot); \qquad (\mathbb{R},+,\cdot); \qquad (\mathbb{C},+,\cdot).$$

Exercici 53. Si A és un conjunt donat qualsevol, estudieu les propietats de $(\mathcal{P}(A),\cup,\cap)$.

Exercici 54. Dins el conjunt $\mathbb{N}$ dels nombres naturals, estudieu les propietats de les operacions m.c.d i m.c.m.

Exercici 55. Demostreu que l'element neutre, si existeix, és unic.

Exercici 56. Demostreu que si $*$ és associativa i cada element té simètric, aleshores aquest és únic.

Tal com haureu observat als exercicis 52 i 53, les operacions definides sobre un conjunt poden satisfer unes propietats o unes altres, donant lloc a una determinada estructura. Les estructures més interessants són les següents:

Un *monoide* o *semigrup* és un conjunt dotat d'una operació associativa amb element neutre. El monoide s'anomena *abelià* o *commutatiu* si, a més, l'operació és commutativa.

Un *grup* és un conjunt dotat d'una operació associativa, amb element neutre i elements simètrics. El grup s'anomena *abelià* o *commutatiu* si, a més, l'operació és commutativa.

Un *anell* és un conjunt dotat de dues operacions. Amb la primera, habitualment anomenada suma, ha de tenir una estructura de grup; la segona, habitualment anomenada producte, ha de ser associativa; finalment, el producte ha de distribuir la suma. L'anell s'anomena *unitari* si, a més, el producte té element neutre. L'anell s'anomena *abelià* o *commutatiu* si, a més, el producte és commutatiu.

Un *cos* és un conjunt dotat de dues operacions. Amb la primera, habitualment anomenada suma, ha de tenir una estructura de grup; amb la segona, habitualment anomenada producte, i sense tenir en compte l'element neutre de la suma, també ha de tenir estructura de grup; finalment, el producte ha de distribuir la suma. El cos s'anomena *abelià* o *commutatiu* si el producte és commutatiu.

Una *àlgebra de Boole* és un conjunt dotat de dues operacions. Totes dues han de ser associatives, commutatives, distributives, amb element neutre i amb complements. El *complement* d'un element x és un altre element x' tal que $x+x'$ és igual a l'element neutre del producte i $x \cdot x'$ és igual a l'element neutre de la suma.

Exercici 57. Reprenent els exercicis 52 i 53, demostreu:

$(\mathbb{N}, +)$ és un semigrup commutatiu;

$(\mathbb{Z}, +)$ és un grup commutatiu;

$(\mathbb{Z}, +, \cdot)$ és un anell unitari commutatiu;

$(\mathbb{Q}, +, \cdot)$ és un cos commutatiu;

$(\mathbb{R}, +, \cdot)$ és un cos commutatiu;

$(\mathbb{C}, +, \cdot)$ és un cos commutatiu;

$(\mathcal{P}(A), \cup, \cap)$ és una àlgebra de Boole.

Exercici 58. Considerem el conjunt $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ (vegeu l'exercici 28). Demostreu que la suma i el producte de $\mathbb{Z}$ indueixen sobre $\mathbb{Z}_n$ una suma i un producte ben definits. És a dir, que si $[a_1] = [a_2]$ i $[b_1] = [b_2]$, aleshores $[a_1 + b_1] = [a_2 + b_2]$. A continuació, demostreu que $(\mathbb{Z}_n, +, \cdot)$ és un anell unitari commutatiu i que, si p és primer, $(\mathbb{Z}_p, +, \cdot)$ és un cos. Doneu un exemple en el qual $(\mathbb{Z}_n, +, \cdot)$ no és un cos.

Bibliografia

Aleksandrov, Kolmogorov, Laurentiev y otros. La matemática, su contenido, métodos y significado. Alianza ed., 1973.

Barnes, Mack. Una introducción algebraica a la lógica matemática. EUNIBAR, 1977.

Boyer. Historia de la matemática. Alianza ed., 1986.

Sainz, Serarols, Pérez. Algebra, vol. 1. Ed. Politec, 1990.

Smullyan. ¿Cómo se llama este libro? Ed. Cátedra, 1978.