TREBALL DE FI DE GRAU

Grau en Matemàtiques

Títol: Teoremes de representació per a àlgebres de Boole finites i reticles distributius finits

Autor: Jordi Massó Cuscó

Director: Jaume Martí i José Luis Ruiz

Departament: Departament de Matemàtiques

Convocatòria: 2018-2019

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya

Facultat de Matemàtiques i Estadística

Treball de Final de Grau

Teoremes de representació per a àlgebres de Boole finites i reticles distributius finits

Jordi Massó Cuscó

Tutors del treball

Jaume Martí Farré i José Luis Ruiz Muñoz

4 de setembre de 2019

Índex

Introducció

Un dels problemes centrals de les matemàtiques és el de la classificació. Per a cada tipus d'objecte, tenim la corresponent noció d'isomorfisme i ens interessa saber sota quines circumstàncies dos objectes d'aquest tipus són isomorfs. A vegades, podem trobar a cada classe d'isomorfia un invariant canònic, que pertany a una família ben coneguda, i que ens serveix per establir quan dos objectes són isomorfs: ho són si, i només si, els invariants canònics de les seves classes són el mateix. En casos més complexos, serà més complicat trobar invariants com a tal i parlarem de propietats que hauran de satisfer ambdós objectes per mantenir la noció d'isomorfisme.

D'aquesta manera, per cada tipus d'objecte necessitarem definir el concepte d'isomorfisme i trobar les diferents propietats o axiomes que ens permetin establir si qualsevol parell d'objectes són isomorfs o no. L'estructura dels teoremes de classificació serà:

> A, B pertanyen a la mateixa *classe d'isomorfia* si, i només si, satisfan les mateixes *propietats canòniques* o tenen els mateixos *invariants canònics.*

A continuació il·lustrarem aquest concepte amb un parell d'exemples.

Per començar, considerarem K un cos commutatiu i ens interessarem pels espais vectorials de dimensió finita sobre K. En aquest cas, el teorema de classificació ens diu que si E i F són $K-$espais vecorials de dimensió finita, aleshores $E \simeq F$ si, i només si, $\dim_K(E) = \dim_K(F)$.

Sense anar massa més lluny, podem trobar un altre exemple prenent com a tipus d'objectes els grups cíclics. En aquest cas, el teorema de classificació dels quals ens diu que dos grups cíclics G i G' són isomorfs si, i només si, $|G| = |G'|$, és a dir, si tenen el mateix cardinal.

Vist això, ens podem plantejar una qüestió que va una mica més enllà. A banda de classificar un conjunt d'objectes com a isomorfs entre si, existeix un representant canònic amb el que estiguem familiaritzats? És a dir, volem trobar un objecte conegut al qual es puguin reduir tots els objectes amb qui comparteixi invariant canònic.

La resposta es troba en els anomenats teoremes de representació, els quals presenten habitualment una estructura similar a la següent:

A és *isomorf* a X representant canònic si, i només si, A satisfà un seguit *d'axiomes o propietats.*

Tornant als exemples anteriors, podem trobar resultats de representació força interessants.

En el cas dels espais vectorials, a cada classe d'isomorfia tenim un $K-$espai vectorial canònic: K^n. El resultat que ens diu que si E és un $K-$espai vectorial de dimensió finita n, aleshores és isomorf a K^n és el teorema de representació.

En el cas dels grups cíclics, el teorema de representació ens dóna informació sobre l'objecte canònic al qual el grup cíclic serà isomorf: els enters en cas de tenir cardinal infinit i els enters mòdul n en cas de tenir cardinal $n < \infty$. Formalment, ens diu que donat G un grup cíclic:

i) G finit d'ordre $n \Longrightarrow G \simeq \mathbb{Z}_n$

ii) G infinit $\Longrightarrow G \simeq \mathbb{Z}$

Així doncs, hem pogut comprovar que els teoremes de representació són resultats més forts que els teoremes de classificació en el sentit que, dins una teoria, ens diuen que qualsevol objecte és isomorf a un d'una determinada família d'objectes ben coneguts (els espais K^n a la teoria d'espais vectorials sobre K o els grups $\mathbb{Z}_n$ i $\mathbb{Z}$ a la teoria de grups cíclics).

En aquest treball, ens centrarem en demostrar-ne dos de concrets enunciats a continuació, el de Stone per àlgebres de Boole finites i el de Birkhoff per reticles distributius finits.

Teorema de Representació de Stone: Sigui B una àlgebra de Boole finita, $A = \mathrm{At}(B)$ el conjunt dels àtoms de B, aleshores és isomorfa a $\mathcal{P}(A)$ representant canònic, és a dir

$$(B, \wedge, \vee) \cong_b (\mathcal{P}(A), \cap, \cup).$$

Teorema de Representació de Birkhoff: Sigui L un reticle distributiu finit, $\mathcal{J}(L)$ el conjunt d'elements irreductibles respecte la unió, aleshores és isomorf a $\mathcal{I}(\mathcal{J}(L))$ representant canònic definit com el conjunt d'ideals d'aquest últim conjunt, és a dir,

$$(L, \wedge, \vee) \cong (\mathcal{I}(\mathcal{J}(L)), \cap, \cup).$$

A més, en aquest cas, el teorema de representació també es podrà entendre com una caracterització dels reticles distributius finits: un reticle finit serà distributiu si, i només si, és isomorf al representant canònic esmentat prèviament.

D'aquesta manera, l'objectiu principal del treball serà, com ja hem comentat, demostrar els teoremes de representació de Stone i de Birkhoff, tot entenent els conceptes claus d'àlgebra de Boole i reticle distributiu a partir de diferents exemples.

Com es veurà més endavant, les àlgebres de Boole són, en particular, reticles distributius. Per tant, n'hi hauria prou amb demostrar el teorema de Birkhoff i deduir que el de Stone n'és un corol·lari. De totes maneres, per raons didàctiques i històriques, hem preferit començar demostrant el teorema de Stone ja que els conceptes involucrats en aquesta són més senzills i després demostrar el cas general, el teorema de Birkhoff.

Dit això, procedirem a comentar l'estructura del treball i què es tracta en cada capítol, deixant de banda les referències emprades. A la introducció de cada secció ja es proporcionarà la bibliografia bàsica que s'hagi utilitzat per entendre i redactar els conceptes i idees que hi apareixen.

Capítol 1: Al primer capítol introduirem breument els conceptes bàsics que ens permetran comprendre a la perfecció l'estructura de conjunt parcialment ordenat i la seva representació gráfica pel seu diagrama de Hasse. A partir d'uns quants exemples bastant simples, presentarem les nocions d'element maximal, màxim i suprem (anàlogament d'element minimal, mínim i ínfim) d'aquests conjunts. Tot i ser una secció que presenta conceptes extensament treballats durant el grau, he considerat interessant recordar breument algunes definicions sobre les quals s'aixecaran les bases del treball.

Capítol 2: Al segon capítol entrarem més a fons en les definicions de reticle ordenat i reticle algebraic, veient-ne l'equivalència cap a un únic concepte de reticle, i presentarem uns quants exemples de reticles força coneguts, així com la representació gràfica i la taula d'operacions d'algun d'ells. Veurem els diferents tipus de morfismes entre reticles per acabar definint amb més precisió la noció d'isomorfisme, fonamental per poder enunciar i demostrar els teoremes de representació objectiu del treball, i continuarem estudiant els subreticles ideal i filtre tot veient-ne un seguit d'exemples i propietats. Per acabar, definirem els conceptes de reticle distributiu i reticle modular, demostrarem un seguit de teoremes que els relacionen i els caracteritzen i veurem la definició i un parell de propietats dels elements atòmics i els elements irreductibles.

Capítol 3: Al tercer capítol particularitzarem la definició de reticle distributiu per arribar a la d'àlgebra de Boole, obtenint així totes les eines necessàries per demostrar el primer dels dos teoremes de representació, el de Stone. Veurem un seguit d'exemples d'àlgebres de Boole, entre ells el que en serà el representant canònic, i refinarem algun dels conceptes i definicions ja presentades en el capítol anterior, sempre amb la intenció d'adaptar-les al nou context en el que ens trobem.

Capítol 4: Al quart capítol el dedicarem a enunciar i demostrar el teorema de representació de Stone. Començarem enunciant i comprovant un parell de resultats importants que ens permetran que la demostració final del teorema sigui més elegant i menys feixuga i acabarem amb un parell d'exemples que ens permetran veure una aplicació més directa del teorema.

Capítol 5: Al cinquè i últim capítol el dedicarem a enunciar i demostrar el teorema de representació restant, el de Birkhoff. Com en el capítol anterior, destinarem les primeres línies a plantejar i demostrar un seguit de proposicions fonamentals per poder entendre el procés i arguments que segueix la demostració del teorema final. Per acabar, veurem un corol·lari que ens relacionarà el teorema amb les múltiples caracteritzacions dels reticles distributius mitjançant un exemple i construirem unes famílies molt especials d'objectes sobre els quals es pot aplicar de manera una mica més complexa el teorema.

Capítol 1

Conceptes previs

Aquest capítol es presenta com un petit escalfament per preparar-nos per la teoria que desenvoluparem al llarg del treball. Farem una breu introducció del concepte de relació, en particular d'aquelles a les que anomenarem relacions d'ordre, i establirem les bases per definir aquelles col·leccions d'elements que tenen una "màxima fita inferiorï una "mínima fita superior"a les quals anomenarem reticles. Les referències principals són [1] i [2].

Siguin A i B dos conjunts, una relació R d'A a B és un subconjunt del producte cartesià $A \times B$. En cas que els dos conjunts siguin el mateix, direm que R és una relació en A i entendrem (A, R) com el conjunt amb la relació. Si $(a, b) \in R$, escriurem $a \, R \, b$ i direm que l'element a està relacionat amb l'element b mitjançant la relació R. En cas contrari, escriurem $a \not R \, b$.

Una relacó R en un conjunt A pot tenir les següents propietats:

i) R és **reflexiva** si $a \, R \, a$ per a tot $a \in A$.

ii) R és **simètrica** si $a \, R \, b$ implica $b \, R \, a$ per a tot $a, b \in A$.

iii) R és **antisimètrica** si $a \, R \, b$ i $b \, R \, a$ implica $a = b$ per a tot $a, b \in A$.

iv) R és **transitiva** si $a \, R \, b$ i $b \, R \, c$ implica $a \, R \, c$ per a tot $a, b, c \in A$.

Una relació R en un conjunt A és un **ordre parcial** si és reflexiva, antisimètrica i transitiva. En tal cas, (A, R) s'anomena **conjunt parcialment ordenat**.

Les relacions d'ordre parcial descriuen situacions jeràriquiques i acostumem a escriure $\leq$ o $\subseteq$ enlloc de R. Els conjunts finits parcialment ordenats es poden representar gràficament pel seu **diagrama de Hasse**.

Exemple 1.1:

i) A la figura 1.1 es pot veure el diagrama de Hasse del conjunt $(\mathcal{P}(\{1,2,3\}), \subseteq)$, on $\mathcal{P}(S)$ denota les parts de S, és a dir, el conjunt de tots els subconjunts de S i $\subseteq$ significa "inclòs o igual que".

ii) Per altra banda, podem veure a la figura 1.2 el diagrama de Hasse de $(\{1,2,3,4,5\}, \leq)$, on $\leq$ significa "menor o igual que".

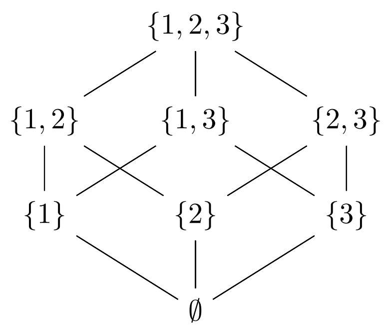


Figura 1.1: $(\mathcal{P}(\{1,2,3\}), \subseteq)$

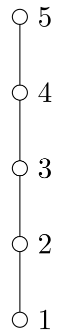


Figura 1.2: $(\{1,2,3,4,5\}, \leq)$

La diferència entre aquests dos exemples queda recollida en la següent definició.

Una relació d'ordre parcial $\leq$ en A s'anomena un **ordre lineal** si per cada $a, b \in A$, aleshores $a \leq b$ o bé $b \leq a$. En tal cas, $(A, \leq)$ s'anomena **conjunt totalment ordenat** o **cadena**. En els exemples vistos anteriorment, $(\{1,2,3,4,5\}, \leq)$ és una cadena però $(\mathcal{P}(\{1,2,3\}), \subseteq)$ no ho és.

Sigui $(A, \leq)$ un conjunt parcialment ordenat, diem que l'element $a \in A$ és el màxim d'A si per a tot $x \in A$, $x \leq A$. De la mateixa manera, diem que $b \in A$ és el mínim d'A si $b \leq x$ per a tot $x \in A$. Diem que l'element $c \in A$ és maximal si "no n'hi ha cap més gran", és a dir, $c \leq x \Longrightarrow c = x$ per a tot $x \in A$. Anàlogament, $d \in A$ s'anomena minimal si $x \leq d \longrightarrow x = d$ per a tot $x \in A$.

Tot i que $(A, \leq)$ tindrà com a molt un element màxim i un element mínim, pot ser que no hi hagi cap, un o molts elements maximals i minimals.

Exemple 1.2: El següent conjunt representat mitjançant el seu diagrama de Hasse (Figura 1.3) presenta a com el seu mínim i el seu element minimal, b i d com elements maximals però no hi ha cap màxim.

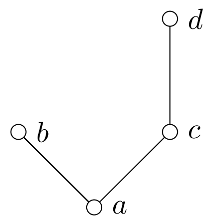


Figura 1.3

Sigui $(A, \leq)$ un conjunt parcialment ordenat i $B \subseteq A$,

i) $a \in A$ és fita superior de B si $b \leq a$ per a tot $b \in B$.

ii) $a \in A$ és fita inferior de B si $a \leq b$ per a tot $b \in B$.

iii) El màxim d'entre totes les fites inferiors de B, en cas d'existir, s'anomena ínfim de B i s'escriu $\inf B$.

iv) El mínim d'entre totes les fites superiors de B, en cas d'existir, s'anomena suprem de B i s'escriu $\sup B$.

Exemple 1.3: Sigui $(A, \leq) = (\mathbb{R}, \leq)$ i B l'interval $[0, 3)$, aleshores $\inf B = 0$ i $\sup B = 3$. Així, el suprem (o l'ínfim) d'un conjunt pot pertànyer o no al conjunt. De la mateixa manera, prenent $B' = \mathbb{N}$, $\inf B' = 1$ però el suprem de B' no existeix.

El següent resultat es tracta d'un axioma addicional (equivalent a l'axioma de l'elecció) utilitzat amb bastanta freqüència en arguments matemàtics. No pot ser ni provat ni refutat, simplement és indecidible.

Lema 1.4 (Zorn): Sigui $(A, \leq)$ un conjunt parcialment ordenat tal que cada cadena d'elements en A té una fita superior en A, aleshores A té com a mínim un element maximal.

Capítol 2

Reticles

En aquest capítol estudiarem més detalladament els reticles, veient-ne diverses definicions equivalents, profietats i exemples. Les referències principals per aquesta part són [1], [3] i [4]. A banda, també veurem els diferents tipus d'aplicacions que es poden construir entre reticles, definirem els conceptes de subreticle ideal i filtre i posarem el focus en els reticles modulars i, sobre tot, distributius. Les referències emprades són [3] altra vegada i [5]. Per acabar, presentarem els elements atòmics i irreductibles (tan per la unió com per la intersecció) utilitzant com a referència essencialment [1].

Un conjunt parcialment ordenat $(L, \leq)$ s'anomena **reticle** si per cada parella d'elements $x, y \in L$ hi ha un suprem i un ínfim. En aquest cas, es pot veure fàcilment que les següents propietats són equivalents:

i) $x \leq y$

ii) $\sup(x, y) = y$

iii) $\inf(x, y) = x$

Algebràicament, un reticle $(L, \wedge, \vee)$ és un conjunt L amb dues operacions binaries $\wedge$ (intersecció o producte) i $\vee$ (unió o suma) que satisfan les següents propietats per a tot $x, y, z \in L$:

(L1)	$x \wedge y = y \wedge x,$	$x \vee y = y \vee x,$	lleis de commutativitat
(L2)	$x \wedge (y \wedge z) = (x \wedge y) \wedge z,$	$x \vee (y \vee z) = (x \vee y) \vee z,$	lleis d'associativitat
(L3)	$x \wedge (x \vee y) = x,$	$x \vee (x \wedge y) = x,$	lleis d'absorció
(L4)	$x \wedge x = x,$	$x \vee x = x,$	lleis d'idempotència

De fet, les lleis d'idempotència no deixen de ser res més que una aplicació de les lleis d'absorció, $x \wedge x = x \wedge (x \vee (x \wedge x)) = x$. Així, parlarem només de les tres lleis dels reticles algrebraics.

A més, notem que qualsevol forma que pugui derivar-se d'aquestes seguirà sent vàlida si intercanviem $\wedge$ i $\vee$ (més endavant també $\leq$ i $\geq$). Això ens porta al principi de dualitat, resultat que ens resultarà molt útil atès que ens permetrà només haver de verificar la meitat dels resultats.

Proposició 2.1 (Principi de dualitat): Qualsevol "fórmula"que impliqui les operacions $\wedge$ i $\vee$ que sigui vàlida en un reticle $(L, \wedge, \vee)$ seguirà sent-ho si intercanviem $\wedge$ per $\vee$ i $\vee$ per $\wedge$ a tot arreu a la fórmula. Aquest procés d'intercanvi s'anomena dualització.

La relació entre els reticles ordenats i els reticles algebraics es segueix del següent teorema.

Teorema 2.2:

i) Sigui $(L, \leq)$ un reticle ordenat, si definim

$$x \wedge y := \inf(x, y) \qquad x \vee y := \sup(x, y),$$

aleshores $(L, \wedge, \vee)$ és un reticle algebraic.

ii) Sigui $(L, \wedge, \vee)$ un reticle algebraic, si definim

$$x \leq y :\Longleftrightarrow x \wedge y = x,$$

aleshores $(L, \leq)$ és un reticle ordenat.

Prova:

i) Sigui $(L, \leq)$ un reticle ordenat, per a tot $x, y, z \in L$ tenim:

(L1) $x \wedge y = \inf(x, y) = \inf(y, x) = y \wedge x$,
$x \vee y = \sup(x, y) = \sup(y, x) = y \vee x$.

(L2) $x \wedge (y \wedge z) = x \wedge \inf(y, z) = \inf(x, \inf(y, z)) = \inf(x, y, z) = \inf(\inf(x, y), z) = \inf(x, y) \wedge z = (x \wedge y) \wedge z$,
$x \vee (y \vee z) = x \vee \sup(y, z) = \sup(x, \sup(y, z)) = \sup(x, y, z) = \sup(\sup(x, y), z) = \sup(x, y) \vee z = (x \vee y) \vee z$.

(L3) $x \wedge (x \vee y) = x \wedge \sup(x, y) = \inf(x, \sup(x, y)) = x$,
$x \vee (x \wedge y) = x \vee \inf(x, y) = \sup(x, \inf(x, y)) = x$.

ii) Sigui $(L, \wedge, \vee)$ un reticle algebraic, per tot $x, y, z \in L$ tenim:

- Per (L4), $x \wedge x = x$ i $x \vee x = x \Longrightarrow x \leq x$, és a dir, $\leq$ és reflexiva.
- Si $x \leq y$ i $y \leq x$, aleshores $x \wedge y = x$ i $y \wedge x = y$. Aleshores, per (L1), $x \wedge y = y \wedge x \Longrightarrow x = y$, és a dir, $\leq$ és antisimètrica.
- Si $x \leq y$ i $y \leq z$, aleshores $x \wedge y = x$ i $y \wedge z = y$. Aleshores, utilitzant (L2), $x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z \Longrightarrow x \leq z$, és a dir, $\leq$ és transitiva.

Hem vist que $(L, \leq)$ té estructura de conjunt parcialment ordenat, ens falta veure que per a cada parell d'elements $x, y \in L$ hi ha un suprem i un ínfim. Tenim que $x \wedge (x \vee y) = x \Longrightarrow x \leq x \wedge y$ i de manera similar $y \leq x \vee y$.

Sigui $z \in L$ amb $x \leq z$ i $y \leq z$, aleshores $(x \vee y) \vee z = x \vee (y \vee z) = x \vee z = z \Longrightarrow (x \vee y) \leq z$. D'aquesta manera, $\sup(x, y) = x \vee y$ i, similarment, $\inf(x, y) = x \wedge y$. Així, $(L, \leq)$ és un reticle ordenat.

Aquest teorema ens permet establir una relació d'un a un entre reticles ordenats i reticles algebraics. De fet, utilitzarem el terme reticle per ambdós conceptes indistintament. El nombre $|L|$ d'elements de L denota la **cardinalitat** o l'**ordre** del reticle.

2.1 Construcció de reticles

Sigui N un subconjunt d'un conjunt parcialment ordenat, aleshores $\bigvee_{x \in N} x$ i $\bigwedge_{x \in N} x$ denoten el suprem i l'ínfim de N, respectivament, en cas de que existeixin.

Si un reticle L conté un element minimal (o maximal) respecte $\leq$, aleshores aquest és únicament determinat i s'anomena **element zero** (**element unitat** respectivament) denotat per 0 (per 1). Aquests dos elements s'anomenen **fites universals** i, en cas d'existir, L s'anomena **fitat**.

En aquest cas, podem afirmar que qualsevol $x \in L$ satisfà $0 \leq x \leq 1$, $0 \wedge x = 0$, $0 \vee x = x$, $1 \wedge x = x$ i $1 \vee x = 1$.

Exemple 2.3: A continuació (Taula 2.1) veurem un seguit d'exemples de reticles prenent M com un conjunt de nombres qualsevol, $\mathbb{N}$ com el conjunt $1, 2, ...$ dels nombres naturals i V un espai vectorial.

Conjunt	$\leq$	$x \wedge y$	$x \vee y$	0	1
M	ordre lineal	$\min(x,y)$	$\max(x,y)$	$\inf M$	$\sup B$
$\mathbb{N}$	"divideix"	$\mathrm{mcd}(x,y)$	$\mathrm{mcm}(x,y)$	1	no existeix
$\mathcal{P}(M)$	$\subseteq$	$X \cap Y$	$X \cup Y$	$\emptyset$	M
tots els subespais de V	$\subseteq$	$X \cap Y$	$X + Y$	$\{\mathbf{0}\}$	V

Taula 2.1: Exemples de reticles

Exemple 2.4: A la Figura 2.1 presentem els diagrames de Hasse de tots els reticles de, com a màxim, 5 elements. La notació emprada per a cada un d'ells serà V_i^n, entenent-lo com el i-èssim reticle de n elements.

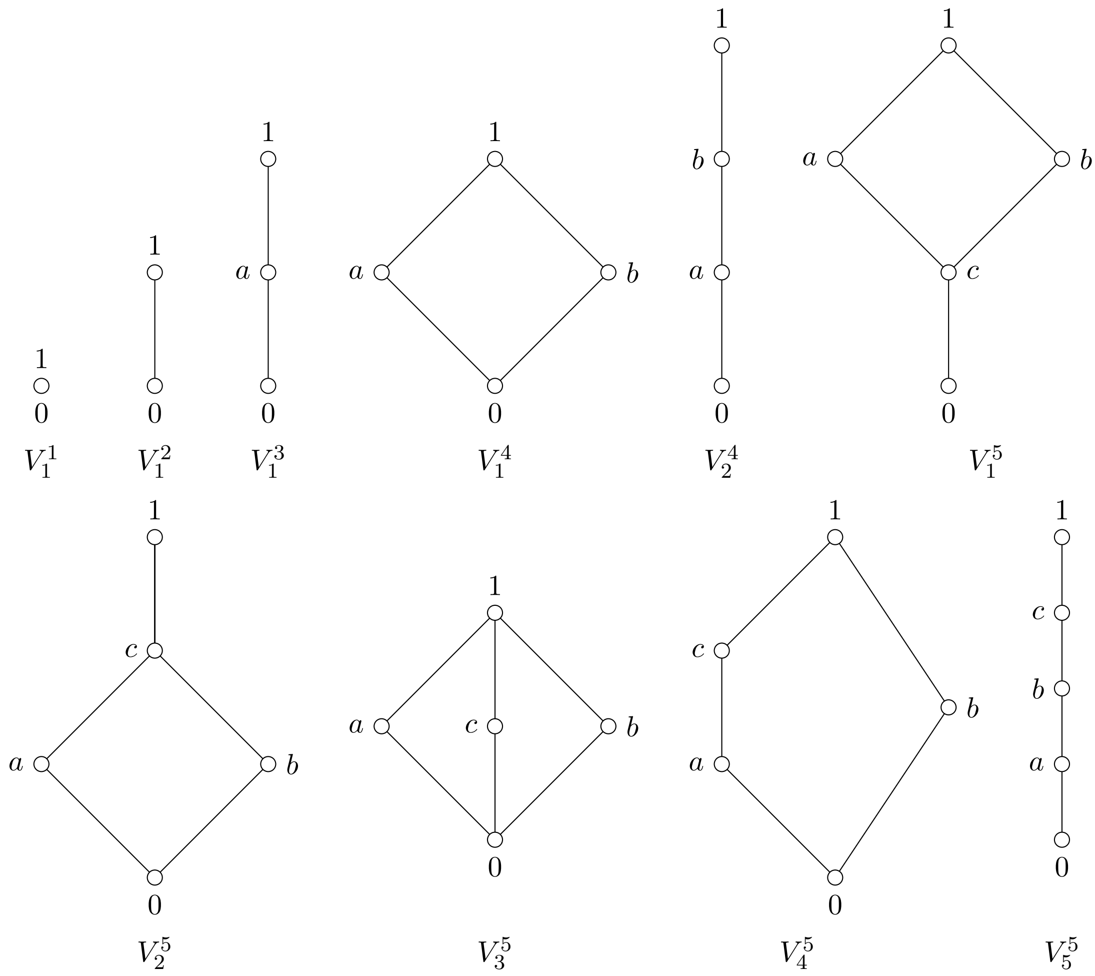


Figura 2.1

Exemple 2.5: A la següent figura (Figura 2.2) veurem el diagrama de Hasse d'un dels molts reticles amb 7 elements acompanyat de les seves **taules d'operacions** (Taula 2.2), les quals ens mostren $x \wedge y$ i $x \vee y$ per a tot x, y del reticle.

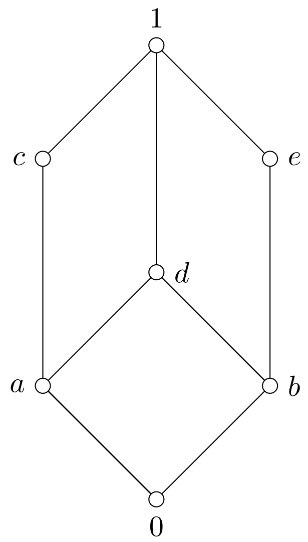


Figura 2.2: V_1^7

$\wedge$	0	a	b	c	d	e	1
0	0	0	0	0	0	0	0
a	0	a	0	a	a	0	a
b	0	0	b	0	b	b	b
c	0	a	0	c	0	0	c
d	0	a	b	a	b	d	d
e	0	0	b	0	0	e	c
1	0	a	b	c	d	e	1

$\vee$	0	a	b	c	d	e	1
0	0	a	b	c	d	e	1
a	a	a	d	c	d	1	1
b	b	d	b	1	d	e	1
c	c	c	1	c	1	1	1
d	d	d	d	1	d	1	1
e	e	1	e	1	1	e	1
1	1	1	1	1	1	1	1

Taula 2.2: Taules d'operacions de V_1^7

Lema 2.6: En cada reticle L, les operacions $\wedge$ i $\vee$ són isòtones, és a dir, $y \leq z \Longrightarrow x \wedge y \leq x \wedge z$ i $x \vee y \leq x \vee z$.

Teorema 2.7: Els elements d'un reticle qualsevol satisfan les següents desigualtats anomenades desigualtats distributives.

$$x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z),$$
$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z).$$

Prova: De $x \wedge y \leq x$ i $x \wedge y \leq y \leq y \vee z$ obtenim $x \wedge y \leq x \wedge (y \vee z)$. Similarment, obtenim $x \wedge z \leq x \wedge (y \vee z)$. D'aquesta manera, $x \wedge (y \vee z)$ és una fita superior per ambdós elements $x \wedge y$ i $x \wedge z$ i, per tant, $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$. La segona igualtat esdevé certa pel principi de dualitat.

També és possible construir reticles nous a partir de reticles ja existents formant subestructures, imatges homomòrfiques i productes. Un subconjunt S d'un reticle L s'anomena **subreticle** de L si, i només si, S és "tancat"respecte $\wedge$ and $\vee$ (és a dir, $s_1, s_2 \in S \Longrightarrow s_1 \wedge s_2 \in S$ i $s_1 \vee s_2 \in S$). Notem que un subconjunt S d'un reticle L pot ser un reticle respecte l'ordre parcial de L sense ser un subreticle de L. A continuació veurem uns exemples que ho il·lustren.

Exemple 2.8:

i) Tot subconjunt d'un sol element d'un reticle L és un subreticle de L.

ii) Per cada parell d'elements x, y d'un reticle L, l'interval

$$[x, y] = \{a \in L \mid x \leq a \leq y\}$$

és un subreticle de L.

iii) Sigui L el reticle de tots els subconjunts d'un espai vectorial V i S el subconjunt de tots els subespais de V, aleshores S és un reticle respecte la inclusió però no és un subreticle de L.

2.2 Morfismes de reticles

Siguin L i M reticles, aleshores direm que l'aplicació $f: L \longrightarrow M$:

i) És un **morfisme que preserva la unió** si $f(x \vee y) = f(x) \vee f(y)$ per a tot $x, y \in L$;

ii) És un **morfisme que preserva la intersecció** si $f(x \wedge y) = f(x) \wedge f(y)$ per a tot $x, y \in L$;

iii) És un **morfisme d'ordre** si $x \leq y \Longrightarrow f(x) \leq f(y)$ per a tot $x, y \in L$;

Així, direm que f és un morfisme de reticles si és preserva alhora la unió i la intersecció. Els morfismes (de reticles) injectius i exhaustius s'anomenen també monomorfismes i epimorfismes respectivament, mentres que un morfisme bijectiu s'anomena **isomorfismes de reticles**. Si existeix un isomorfisme de L a M, aleshores diem que L i M són **isomorfs** i ho denotem per $L \cong M$. En la majoria dels casos, és convenient identificar els reticles isomorfs.

Per altra banda, direm que f és un **isomorfisme d'ordre** si es satisfà la condició $x \leq y$ a $L \Longleftrightarrow f(x) \leq f(y)$ a M per a tot $x, y \in L$. És necessàriament bijectiu utilitzant les propietats reflexives i antisimètriques de $\leq$, primer a L i després a M.

$$\begin{aligned} f(x) = f(y) &\iff f(x) \leq f(y) \ \ \& \ \ f(y) \leq f(x) \\ &\iff x \leq y \ \ \& \ \ y \leq x \\ &\iff x = y \end{aligned}$$

Nota: El recíproc no és necessàriament cert, no totes les aplicacions bijectives entre conjunts ordenats són isomorfismes d'ordre.

Proposició 2.9: Si f és un morfisme de L a M, aleshores $f(L)$ és un subreticle de M i s'anomena imatge homomòrfica de L per f.

Prova: Volem veure que per a tot $m_1, m_2 \in f(L) \subset M$, $m_1 \wedge m_2 \in f(L)$ i $m_1 \vee m_2 \in f(L)$. Expressant $m_1 = f(l_1)$ i $m_2 = f(l_2)$ amb $l_1, l_2 \in L$, tenim que $m_1 \wedge m_2 = f(l_1) \wedge f(l_2) = f(l_1 \wedge l_2) \in f(L)$ ja que f és un morfisme (en particular, un morfisme que preserva la unió) i $l_1 \wedge l_2 \in L$. Anàlogament, veiem que $m_1 \vee m_2 \in f(L)$.

Proposició 2.10: Tots els morfismes que preserven la unió (o la intersecció) són morfismes d'ordre. Malgrat això, el recíproc no és generalment cert.

Prova: Siguin $x, y \in L$ tals que $x \leq y$, volem veure que $f(x) \leq f(y)$, essent $f : L \longrightarrow M$ un morfisme que preserva la unió (anàlogament es veuria per la intersecció). Tenim que $f(x) \leq f(y) \iff f(x) \vee f(y) = f(y) \iff f(x \vee y) = f(y)$, la qual cosa és certa ja que $x \vee y = y$ per ser $x \leq y$. Que el recíproc no és generalment cert ho veurem mitjançant el següent exemple.

Exemple 2.11: Siguin L_1, L_2 i L_3 els reticles amb diagrama de Hasse de la Figura 2.3 respectivament,

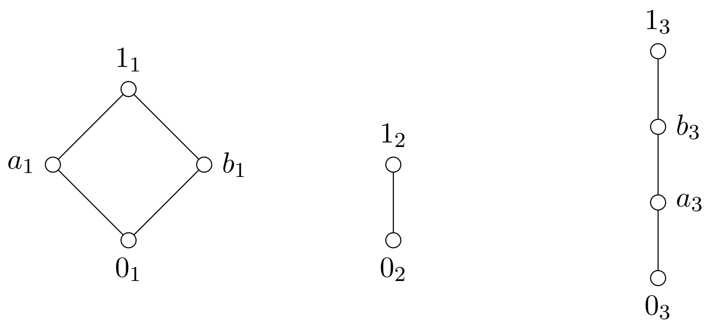


Figura 2.3

Definim els tres morfismes d'ordre següents:

$$\begin{aligned} &f : L_1 \longrightarrow L_2; \quad f(0_1) = f(a_1) = f(b_1) = 0_2, \ f(1_1) = 1_2; \\ &g : L_1 \longrightarrow L_2; \quad g(0_1) = 0_2, \ g(1_1) = g(a_1) = g(b_1) = 1_2; \\ &h : L_1 \longrightarrow L_3; \quad h(0_1) = 0_3, \ h(a_1) = a_3, \ h(b_1) = b_3, \ h(1_1) = 1_3. \end{aligned}$$

Observem que f un morfisme que preserva la unió però no un morfisme de reticles

$$f(a_1 \wedge b_1) = f(0_1) = 0_2 = f(a_1) \wedge f(b_1), \text{ etc.}$$

$$f(a_1 \vee b_1) = f(1_1) = 1_2 \quad \text{i} \quad f(a_1) \vee f(b_1) = 0_2.$$

De manera anàloga i per dualitat, podem veure que g és un morfisme que preserva la intersecció però tampoc és un morfisme de reticles. Per últim, es veu fàcilment que h no és ni una cosa ni l'altra.

$$h(a_1 \wedge b_1) = h(0_1) = 0_3 \quad \text{i} \quad h(a_1) \wedge h(b_1) = a_3 \wedge b_3 = a_3$$

$$h(a_1 \vee b_1) = h(1_1) = 0_3 \quad \text{i} \quad h(a_1) \vee h(b_1) = a_3 \vee b_3 = b_3$$

Siguin L i M dos reticles, el conjunt de parells ordenats $\{(x, y) \mid x \in L, y \in M\}$ amb les operacions $\vee$ i $\wedge$ definides per

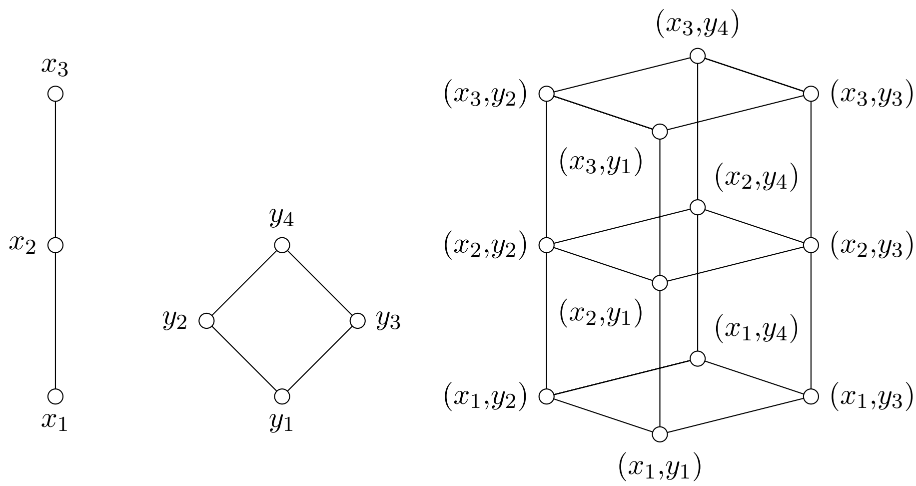
$$(x_1, y_1) \vee (x_2, y_2) = (x_1 \vee x_2, y_1 \vee y_2),$$

$$(x_1, y_1) \wedge (x_2, y_2) = (x_1 \wedge x_2, y_1 \wedge y_2),$$

és el producte directe de L i M, en símbols $L \times M$, també conegut com **reticle producte**. L'ordre parcial a $L \times M$ ve definit per

$$(x_1, y_1) \leq (x_2, y_2) \Longleftrightarrow x_1 \leq x_2 \text{ i } y_1 \leq y_2.$$

Exemple 2.12: També podem descriure el reticle producte gràficament en termes dels diagrames de Hasse tal i com podem veure a la Figura 2.4 a continuació:



L $\qquad$ M $\qquad$ $L \times M$

Figura 2.4

2.3 Ideals i filtres

Sigui L un reticle, un subconjunt no buit J de L s'anomena **ideal** si

i) $x, y \in J \Longrightarrow x \vee y \in J$

ii) $x \in L, y \in J$ i $x \leq y \Longrightarrow x \in J$

Qualsevol ideal J d'un reticle L serà un subreticle ja que $x \vee y \leq x$ per a tot $x, y \in L$.

Anàlogament i per dualitat, anomenarem a qualsevol subconjunt no buit G de L **filtre** si

i) $x, y \in G \Longrightarrow x \wedge y \in G$

ii) $x \in L, y \in G$ i $x \geq y \Longrightarrow x \in G$

Un ideal (o filtre) d'un reticle L s'anomena **propi** si no hi coincideix.

Proposició 2.13: Sigui L un reticle que conté l'element unitat, l'ideal $J \subset L$ és propi $\Longleftrightarrow 1 \notin J$.

Prova: Per veure la implicació cap a la dreta suposem que $1 \in J$. Com que J és ideal, $\forall x \in L, y \in J$ tal que $x \leq y$ es té que $x \in J$. D'aquesta manera, com que $1 \in J$ i $\forall x \in L, x \leq 1$, tenim que $x \in J$ $\forall x \in L$, la qual cosa és una contradicció amb el fet que J sigui propi. La implicació cap a l'esquerra és trivial.

Nota: Observem que, per dualitat, sigui L un reticle que conté l'element zero, tindrem que el filtre $G \subset L$ és propi $\Longleftrightarrow 0 \notin G$.

Donats un reticle L amb $x \in L$ i un subconjunt arbitrari S de L, definim

$$\downarrow S = \{y \in L \mid (\exists x \in S)\ y \leq x\} \text{ i } \uparrow S = \{y \in L \mid (\exists x \in S)\ y \geq x\},$$

$$\downarrow x = \{y \in L \mid y \leq x\} \text{ i } \uparrow x = \{y \in L \mid y \geq x\}.$$

Els ideals (o filtres) de la forma $\downarrow x$ (o $\uparrow x$) s'anomenen **principals**. El conjunt de tots els ideals (o filtres) de L es denota per $\mathcal{I}(L)$ (o per $\mathcal{F}(L)$) satisfent la inclusió d'ordre habitual.

Lema 2.14: Sigui L un reticles amb $x, y \in L$ i M un altre reticle amb $M \in \mathcal{I}(L)$, aleshores les següents condicions són equivalents:

i) $x \leq y$

ii) $\downarrow x \subseteq \downarrow y$

iii) $y \in M \Longrightarrow x \in M$

Exemple 2.15:

i) Considerem el següent reticle (Figura 2.5). En aquest cas, els conjunts $\{c\}, \{a, b, c, d, e\}$ i $\{a, b, d, f\}$ són ideals mentres que $\{e, f, g\}$ i $\{c, e, g\}$ són filtres. A més, $\{b, d, e\}$ no és ideal atès que $\downarrow \{b, d, e\} = \{a, b, c, d, e\}$ i $\{a, b, d, f\}$ no és fitre al ser $\uparrow \{a, b, d, f\} = \{a, b, d, e, f, g\}$.

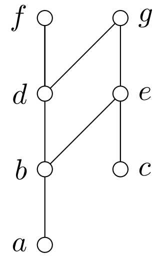


Figura 2.5

ii) A continuació (Figura 2.6) podem observar L i $\mathcal{I}(L)$ en un cas senzill.

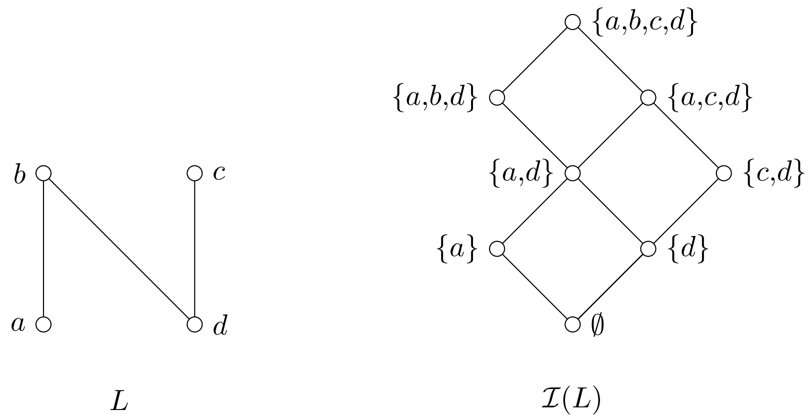


Figura 2.6

2.4 Reticles distributius i modulars

Sigui L un reticle, direm que es tracta d'un **reticle distributiu** si per a tot $x, y, z \in L$ es satisfà

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Aquestes igualtats s'anomenen lleis distributives. Pel principi de dualitat, les dues igualtats són equivalents i, per tant, serà suficient exigir-ne només una.

Sigui L un reticle, direm que es tracta d'un **reticle modular** si per a tot $x, y, z \in L$ es satisfà

$$(x \wedge y) \vee (x \wedge z) = x \wedge ((x \wedge y) \vee z) = x \wedge (y \vee (x \wedge z)),$$
$$(x \vee y) \wedge (x \vee z) = x \vee ((x \vee y) \wedge z) = x \vee (y \wedge (x \vee z)).$$

Aquestes igualtats s'anomenen lleis modulars i, de la mateixa manera que amb les distributives, són equivalents dues a dues pel principi de dualitat. A més, si el reticle satisfà qualsevol de les dues identitats següents també podrem dir que és modular.

$$x \vee (y \wedge z) = (x \vee y) \wedge z \text{ per a tot } x \leq z$$

$$x \wedge (y \vee z) = (x \wedge y) \vee z \text{ per a tot } x \geq z.$$

Exemple 2.16: Com a exemples més habituals, tenim els reticles $(\mathcal{P}(M), \cap, \cup)$ i $(\mathbb{N}, \text{gcd}, \text{lcm})$ ja esmentats anteriorment. A més, dels reticles de 5 elements vists a la Figura 2.1, destaquem els anomenats reticle diamant $V_3^5 = M_3$ i reticle pentagon $V_4^5 = N_5$. Aquests són els reticles no distributis més petits, essent V_3^5 modular i V_4^5 no. Els podem tornar a veure a la Figura 2.7.

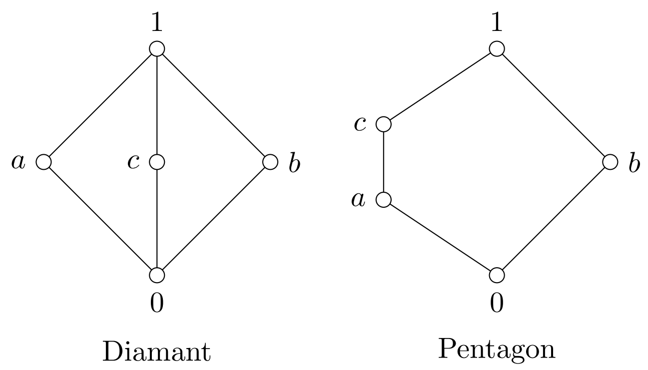


Figura 2.7

És clar que cap dels dos és distributiu atès que, a V_3^5, $a \vee (b \wedge c) = a \vee 0 = a \neq 1 = (a \vee b) \wedge (a \vee c)$; mentres que, a V_4^5, $a \vee (b \wedge c) = a \vee 0 = a \neq c = 1 \wedge c = (a \vee b) \wedge (a \vee c)$. Per altra banda, V_4^5 tampoc és modular atès que $a \vee (b \wedge (a \vee c)) = a \vee (b \wedge c) = a \vee 0 = a \neq c = 1 \wedge c = (a \vee b) \wedge (a \vee c)$.

A continuació estudiarem més a fons una altra condició equivalent a aquestes lleis que ens permetrà caracteritzar els reticles distributius i modulars d'una manera més geomètrica a partir del diamant i del pentàgon.

Per a cada parell d'elements $x, y \in L$, sempre es compleix que $x \leq x \vee y$ i $x \wedge y \leq x$. D'aquesta manera, podem construir els subreticles $[x, x \vee y]$ i $[x \wedge y, x]$ per definir $f_x : [x \wedge y, x] \longrightarrow [x, x \vee y]$ tal que $f_x(z) = z \vee x$ i $g_y : [x, x \vee y] \longrightarrow [x \wedge y, x]$ tal que $g_y(z) = z \wedge y$.

Aquestes funcions són clarament morfismes d'ordre però no són necessàriament morfismes de reticles ni, en general, inverses l'una de l'altra. De fet, en un reticle L, diem que per $a, b \in L$ es satisfà l'isomorfisme del diamant si les funcions f_x i g_y definides anteriorment són isomorfismes dels subreticles $[x, x \vee y]$ i $[x \wedge y, x]$.

Proposició 2.17: Un reticle L és modular si, i només si, per a tot $x, y \in L$ es satisfà l'isomorfisme del diamant.

Prova: Per veure la implicació cap a l'esquerra, prenem $x, y, z \in L$ tals que $x \leq z$ i, per tant, $y \leq x \vee y \leq z \vee y$. Així, $x \vee y \in [y, y \vee z]$ i $g_z(x \vee y) = (x \vee y) \wedge z$. Atès que f_y és la funció inversa de g_z, $x \vee y = f_y((x \vee y) \wedge z)$. Per altra banda, tenim $y \wedge z \leq x \vee (y \wedge z) \leq z \vee (y \wedge z) = z$. Per tant, $x \vee (y \wedge z) \in [y \wedge z, z]$ i tenim $f_y(x \vee (y \wedge z)) = y \vee x \vee (y \wedge z) = y \vee x = f_y((x \vee y) \wedge z)$. Al ser f_y una aplicació injectiva, $x \vee (y \wedge z) = (x \vee y) \wedge z$ i el reticle L és modular.

Per veure la implicació cap a la dreta, prenem $x, y \in L$ i considerem $z \in [x, x \vee y]$ de tal manera que $f_x \circ g_y(z) = x \vee (y \wedge z)$. Com que $z \in [x, x \vee y]$, tenim $x \leq z$ i, per les lleis modulars, $f_x \circ g_y(z) = x \vee (y \wedge z) = (x \vee y) \wedge z = z$ atès que $z \leq (x \vee y)$. Anàlogament, considerem $z \in [x \wedge y, y]$ de tal manera que $g_y \circ f_x(z) = y \wedge (x \vee z) = (z \vee x) \wedge y$. Com que $z \leq y$, per les lleis modulars, $g_y \circ f_x(z) = (z \vee x) \wedge y = z \vee (x \wedge y) = z$ atès que $z \geq (x \wedge y)$. D'aquesta manera, f_x, g_y són inverses l'una de l'altra i, per tant, isomorfismes.

Teorema 2.18: Un reticle L és modular si, i només si, no conté cap subreticle isomorf al pentagon.

Prova: La implicació cap a la dreta és trivial ja que, de no ser així, el subreticle isomorf al pentagon ens donaria immediatament un contraexemple de la llei modular.

Per veure la implicació cap a l'esquerra, suposarem que el reticle L no és modular. Per tant, existeixen $x, y, z \in L$ amb $x \leq z$ tals que $x \vee (y \wedge z) \neq (x \vee y) \wedge z$. Siguin $a = x \vee y$, $b = (x \vee y) \wedge z$, $b' = x \vee (y \wedge z)$, $c = y$ i $d = y \wedge z$, veurem que $\{a, b, b', c, d\}$ configura un subreticle isomorf al pentagon.

Primer de tot hem de veure que són diferents entre ells i que compleixen la relació d'ordre desitjada. Notem abans que si $x \leq y$, aleshores $x \leq y \wedge z$ i $x \vee (y \wedge z) = y \wedge z = (x \vee y) \wedge z$ de tal manera que la nostra hipòtesis no és certa. Anàlogament, si $y \leq z$, tenim que $x \vee y \leq z$ i $(x \vee y) \wedge z = x \vee y = x \vee (y \wedge z)$, arribant a la mateixa contradicció.

Sabem que b i b' són diferents per hipòtesi. A més, com que $x \vee y \geq x$ i $x \vee y \geq y \geq y \wedge z$, tenim $x \vee y \geq x \vee (y \wedge z)$. Per altra banda, $z \geq x$ i $z \geq y \wedge z$, d'on en resulta que $z \geq x \vee (y \wedge z)$. En resum, tenim $b = (x \vee y) \wedge z \geq x \vee (y \wedge z) = b'$. També podem veure fàcilment que $d = y \wedge z \leq x \vee (y \wedge z) = b'$ i $a = x \vee y \geq (x \vee y) \wedge z = b$, essent $d \neq b'$ i $a \neq b$ per evitar contradiccions. D'aquesta manera, ja hem vist $a \geq b \geq b' \geq d$, tots diferents entre si.

A banda, $a = x \vee y \geq y \geq y \wedge z = d$ amb $a \neq c, c \neq d$ i tenim $a \geq c \geq d$. Només falta veure que b, c no mantenen cap relació d'ordre i b', c tampoc. Si $b' \leq c$, tenim $x \leq y$ contradicció. Si $b \geq c$, tenim $y \leq z$ una altra contradicció. Per tant, no pot existir cap relació d'ordre entre ells i, en efecte, $\{a, b, b', c, d\}$ és un subreticle isomorf al pentagon.

Teorema 2.19: Un reticle L és distributiu si, i només si, no conté cap subreticle isomorf al diamant o al pentagon.

Prova: Com abans, la implicació cap a la dreta és trivial. Per veure la implicació cap a l'esquerra suposarem que el reticle no és distributiu. Si el reticle tampoc és modular, pel teorema anterior existeix un subreticle isomorf al pentagon i ja estem. Així, suposem que el reticle és modular.

Atès que L no és distributiu, podem trobar $x, y, z \in L$ tals que $(x \vee y) \wedge (x \vee z) \wedge (y \vee z) \neq (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. Siguin $a = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$, $e = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$, $b = (x \wedge a) \vee e$, $c = (y \wedge a) \vee e$, $d = (z \wedge a) \vee e$, veurem que $\{a, b, c, d, e\}$ configura un subreticle isomorf al diamant.

Per començar, veiem que $x \vee y \geq x \wedge y, x \wedge z, y \wedge z$, per tant, $x \vee y \geq e$. El mateix succeeix per $y \vee z$ i $z \vee x$, així tenim que $a \geq e$. Afirmem que $b \vee c = b \vee d = c \vee d = a$ i que $b \wedge c = b \wedge d = c \wedge d = e$ de tal manera que $a \geq b, c, d \geq e$. Suposem que $d = e$, aleshores $a = b \vee d = b$ i $a = b \vee c = c$, però aleshores $b \wedge c = a$ i arribem a una contradicció.

De manera similar podem veure $b \neq e, c \neq e, b \neq a, c \neq a, d \neq a$, la qual cosa ens indica que b, c, d són diferents dos a dos i no estableixen cap relació d'ordre entre ells. Així, efectivament $\{a, b, c, d, e\}$ es tracta d'un subreticle isomorf al diamant. Anem a veure que les afirmacions anteriors són certes.

Tenim que $b = (x \wedge a) \vee e = (x \wedge (x \vee y) \wedge (x \vee z) \wedge (y \vee z) \vee e = (x \wedge (y \vee z)) \vee e = e \vee (x \wedge (y \vee z))$. Com que $e \leq y \vee z$, per les lleis modulars tenim que $b = (e \vee x) \wedge (y \vee z)$ i, utilitzant que $e \vee x = x \vee (y \wedge z)$ obtenim $b = (x \vee (y \wedge z)) \wedge (y \vee z)$.

Així, $b \wedge c = (x \vee (y \wedge z)) \wedge (y \vee z) \wedge (y \vee (x \wedge z)) \wedge (x \vee z) = (x \vee (y \wedge z)) \wedge (y \vee (x \wedge z)) = ((y \wedge z) \vee x) \wedge (y \vee (x \wedge z))$. Com que $y \wedge z \leq y \vee (x \wedge z)$, $b \wedge c = (y \wedge z) \vee (x \wedge (y \vee (x \wedge z))) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = e$. Similarment podem veure $b \wedge d = c \wedge d = e$ i $b \vee c = b \vee d = c \vee d = a$ i ja hem acabat.

Exemple 2.20: El reticle amb el següent diagrama de Hasse (Figura 2.8) no podrà ser distributiu al contenir el diamant $\{0, a, b, d, 1\}$ però sí que serà modular.

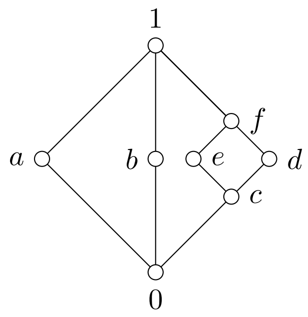


Figura 2.8

Teorema 2.21: Un reticle L és distributiu si, i només si, per a tot $x, y, z \in L$ es satisfà la regla de cancel·lació $x \wedge y = x \wedge z$, $x \vee y = x \vee z$ implica $y = z$.

Prova: Veiem primer la implicació cap a la dreta. Si tenim $x \wedge y = x \wedge z$ i $x \vee y = x \vee z$, aleshores

$$y = y \vee (x \wedge y) = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z) = (x \vee z) \wedge (y \vee z) = (x \wedge y) \vee z,$$

la qual cosa implica que $z \leq y$. De manera similar, es pot veure que $y \leq z$ i, per tant, es satisfà la regla de cancel·lació.

Per veure la implicació cap a l'esquerra, suposem que el reticle L no és distributiu. Aleshores, pel teorema anterior, podem trobar un subreticle $\{a, b, c, d, e\}$ isomorf al diamant. Aleshores, $b \vee c = b \vee d$ i $b \wedge c = b \wedge d$ però $c \neq d$. Per tant, la regla de cancel·lació falla.

2.5 Elements atòmics i irreductibles

Sigui L un reticle amb element minimal i maximal, aleshores direm que es tracta d'un **reticle complementat** si per a cada $x \in L$ existeix, com a mínim, un element y tal que $x \wedge y = 0$ i $x \vee y = 1$. Cada un d'aquests y s'anomena **complementari** de x.

Sigui L un reticle distributiu, aleshores cada $x \in L$ té, com a màxim, un complementari al qual denotem per x'. Per veure aquesta unicitat, suposem que existeixen dos complements y_1 i y_2.

Aleshores, $x \wedge y_1 = 0 = x \wedge y_2$ i $x \vee y_1 = 1 = x \vee y_2$; per tant, per la regla de cancel·lació, $y_1 = y_2$.

Sigui L un reticle amb element minimal, aleshores $x \in L$ s'anomena **àtom** si $x \neq 0$ i, per a tot $y \in L$, $0 < y \leq x$ implica $y = x$.

Per altra banda, direm que $x \in L$ és un element **irreductible respecte la unió** (altrament serà **reductible respecte la unió**) si, per a tot $y, z \in L$

$$x = y \vee z \Longrightarrow x = y \text{ o } x = z.$$

Els elements **irreductibles respecte la intersecció** es defineixen anàlogament per dualitat i denotem per $\mathcal{J}(L)$ el conjunt d'elements irreductibles respecte la unió de L i per $\mathcal{M}(L)$ el d'elements irreductibles respecte la intersecció.

Exemple 2.22: Si considerem el reticle $L = (\mathbb{N}, \mathrm{mcd}, \mathrm{mcm})$, els seus àtoms seran aquells $x \in L, x \neq 1$ tals que per a tot $y \in L$ amb $\mathrm{mcd}(x, y) = y$ impliqui $x = y$. Aquests són clarament els nombres primers, atès que $\mathrm{mcd}(p, y) = y$ implica $p = y \cdot k$ però com que p és primer, $k = 1$ i $p = y$.

Lema 2.23: Cada àtom x d'un reticle L amb element minimal és irreductible.

Prova: Suposem $x = y \vee z$ i $x \neq y$. Aleshores, com que $x = \sup(y, z)$, y és necessàriament menor que x i, per tant, $y = 0$ i $x = z$.

Lema 2.24: Sigui L un reticle distributiu i $x \in L$ un element irreductible tal que $x \leq y \vee z$, aleshores $x \leq y$ o $x \leq z$.

Prova: El fet que $x \leq y \vee z$ és equivalent a $x = x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Atès que x és irreductible, tenim que $x = x \wedge y$ o $x = x \wedge z$, la qual cosa es tradueix a $x \leq y$ o $x \leq z$.

Siguin $x \in [a, b] = \{v \in L \mid a \leq v \leq b\}$ i $y \in L$ tal que $x \wedge y = a$ i $x \vee y = b$, aleshores y s'anomena **complementari relatiu** de x respecte $[a, b]$. Si tots els intervals $[a, b]$ d'un reticle L són complementats, aleshores direm que L es tracta d'un **reticle relativament complementat**.

Per altra banda, si L té element minimal i cada interval $[0, b]$ és complementat, aleshores direm que L es tracta d'un **reticle seccionalment complementat**. Per últim, un **reticle complementat** L és un reticle fitat (amb element mínim 0 i element màxim 1) en el qual cada element $x \in L$ té un complement, és a dir, existeix $y \in L$ tal que $x \wedge y = 0$ i $x \vee y = 1$.

Lema 2.25: Cada element irreductible respecte la unió x d'un reticle L distributiu i complementat és un àtom.

Prova: Sigui $y \in L$, $y \leq x$ i y' un complementari de y, aleshores, atès que $x \leq y \vee y' = 1$ i $x \nleq y$ tenim que $x \leq y'$. Així, $y \leq x \leq y'$ i $y = y \wedge y' = 0$ o x és un àtom.

Capítol 3

Àlgebres de Boole

En aquest capítol definirem el concepte d'àlgebra de Boole i en veurem un seguit d'exemples, entre ells el que serà el representant canònic. També veurem propietats i elements interessants que ens donaran totes les eines necessàries per demostrar el teorema de Stone. Les referències principals són [4], [7] i [10].

Un reticle distributiu complementat s'anomena **àlgebra de Boole**. A partir d'ara, denotarem un conjunt B amb dues operacions binàries $\vee$ and $\wedge$, amb element minimal 0, amb element maximal 1 i amb l'operació unitària del complementari $'$ per $\mathcal{B} = (B, \vee, \wedge, 0, 1,')$ o, per simplificar, B.

Una estructura A és una subàlgebra d'una àlgebra de Boole B si $A \subseteq B$, $0 \in A$, $1 \in A$ i les operacions $\vee, \wedge,'$ són les restriccions de les operacions pròpies de B a A.

Exemple 3.1:

i) Per qualsevol conjunt B, es defineix l'**àlgebra potència** com $P(B) = (\mathcal{P}(B), \cup, \cap, ^-, \emptyset, B)$, on per a cada $X \subseteq B, \bar{X} = B \setminus X$ que, en particular, és una àlgebra de Boole.

ii) Més generalment, donat un conjunt B, una **àlgebra de conjunts** sobre B és una subàlgebra de l'àlgebra potència $P(B)$. Així, una col·lecció $\mathcal{B}$ de subconjunts de B és l'univers d'una àlgebra de conjunts sobre B si, i només si, $\emptyset, \mathcal{B}$ són elements de B i, per a tot $X, Y \in \mathcal{B}$ es compleix que $X \cup Y, X \cap Y, B \setminus X \in \mathcal{B}$.

iii) Sigui X un conjunt qualsevol, un subconjunt a de X es considera que és cofinit en X si $X \setminus a$ és finit. Definim

$$A = \{a \subseteq X \ : \ a \text{ és cofinit}\}.$$

Aleshores, A és una àlgebra de conjunts sobre X, anomenada **àlgebra cofinita o dels complements finits** sobre X. Per veure que per a tot $a, b \in A$, $a \cup b$ i $a \cap b$ pertanyen a A, s'utilitza que la unió d'un nombre finit de conjunts finits és finita i les lleis de De Morgan que presentem a continuació.

Teorema 3.2 (Les lleis de De Morgan): Per a tot $x, y \in B$ àlgebra de Boole, tenim que

$$(x \wedge y)' = x' \vee y' \quad \text{i} \quad (x \vee y)' = x' \wedge y'.$$

Prova: Per dualitat, només serà necessari verificar una de les dues igualtats. Atès que A és una àlgebra de Boole i, per tant, un reticle distributiu, tenim que

$$(x \wedge y) \vee (x' \vee y') = (x \vee x' \vee y') \wedge (y \vee x' \vee y') = (1 \vee y') \wedge (1 \vee x') = 1 \wedge 1 = 1,$$

la qual cosa implica que $x' \vee y'$ és el complementari de $x \wedge y$.

Teorema 3.3: En una àlgebra de Boole B tenim que, per a tot $x, y \in B$

$$x \leq y \underset{\text{i)}}{\Longleftrightarrow} y' \leq x' \underset{\text{ii)}}{\Longleftrightarrow} x \wedge y' = 0 \underset{\text{iii)}}{\Longleftrightarrow} x' \vee y = 1.$$

Prova:

i) $x \leq y \Longleftrightarrow x \vee y = y \Longleftrightarrow x' \wedge y' = (x \vee y)' = y' \Longleftrightarrow y' \leq x'$.

ii) $y' \leq x' \Longleftrightarrow x' \wedge y' = y' \Longleftrightarrow x \wedge (x' \wedge y') = x \wedge y') \Longleftrightarrow 0 = x \wedge y'$.

iii) $x \wedge y' = 0 \Longleftrightarrow x' \vee y = (x \wedge y')' = 0' = 1$.

Siguin B_1, B_2 dues àlgebres de Boole, aleshores l'aplicació $f : B_1 \longrightarrow B_2$ s'anomena **morfisme booleà** de B_1 a B_2 si f és un morfisme de reticles i per a tot $x \in B$ tenim que $f(x') = (f(x))'$.

De la mateixa manera que amb els morfismes de reticles, podem definir monomorfismes, epimorfismes i isomorfismes booleans. Si hi ha un isomorfisme booleà entre B_1 i B_2 escriurem $B_1 \cong_b B_2$.

Proposició 3.4: Sigui $f : B_1 \longrightarrow B_2$ un morfisme booleà, aleshores:

i) $f(0) = 0, f(1) = 1$.

ii) per a tot $x, y \in B_1$ tals que $x \leq y$, $f(x) \leq f(y)$.

iii) $f(B_1)$ és una àlgebra de Boole i una subàlgebra de Boole de B_2.

Prova:

i) Sigui $x \in B_1$ qualsevol, $f(x \wedge x') = f(x) \wedge f(x') = f(x) \wedge f(x)' = 0$. Anàlogament, podem veure $f(1) = 1$.

ii) Siguin $x, y \in B_1$ tals que $x \leq y$, tenim que $x \wedge y = x$. D'aquesta manera, $f(x) \wedge f(y) = f(x \wedge y) = f(x)$ i, per tant, $f(x) \leq f(y)$.

Exemple 3.5: Sigui $M = 1, \ldots, n$, aleshores $\{0,1\}^n$ i $\mathcal{P}(M)$ són àlgebres de Boole i l'aplicació

$$\begin{array}{rccc} f: & \{0,1\}^n & \longrightarrow & \mathcal{P}(M) \\ & (i_1, \ldots, i_n) & \longmapsto & \{k \mid i_k = 1\} \end{array}$$

és un isomorfisme de booleà.

Com hem fet als reticles, $x \in B$ serà un àtom si $x \neq 0$ i, per a tot $y \in B$, $0 < y \leq x$ implica $y = x$. Denotarem com $\mathrm{At}(B)$ al conjunt dels àtoms de B i direm que B és una àlgebra atòmica si per a tot element $y \in B$ diferent de 0 existeix algun àtom x tal $y \leq x$.

Exemple 3.6:

i) Una àlgebra potència $\mathcal{P}(X)$ o l'àlgebra dels complements finits sobre X són àlgebres atòmiques i els seus àtoms són els conjunts unipuntuals $\{x\}$ amb $x \in X$.

ii) Un altre exemple d'àlgebra atòmica és qualsevol àlgebra de Boole finita B, atès que si $x > 0$ i no existeix cap àtom per sota de x, aleshores hi hauria una successió infinita estrictament decreixent $x_0 = x > x_1 > x_2 > \ldots$ a $B \setminus \{0\}$.

Capítol 4

Teorema de representació de Stone

En aquest capítol demostrarem el primer dels teoremes objectiu del treball, el teorema de representació de Stone. Aquest essencialment ens diu que qualsevol àlgebra de Boole finita és isomorfa a les parts del conjunt dels seus àtoms, és a dir que $(B, \wedge, \vee) \cong_b (\mathcal{P}(\mathrm{At}(B)), \cap, \cup)$. Les referències utilitzades són [1] i [4].

Abans d'enunciar-lo formalment i demostrar-lo en si, veurem un parell de proposicions que ens seran útils a l'hora de demostrar el resultat final.

Proposició 4.1: Sigui B una àlgebra de Boole, $a \in B$ un àtom satisfà les següents propietats:

i) $a \neq 0$ i, per a tot $x \in B$, $a \leq x$ o $a \leq x'$

ii) $a \neq 0$ i, per a tot $x, y \in B$, $a \leq x \wedge y$ si, i només si $a \leq x$ i $a \leq y$

iii) $a \neq 0$ i, per a tot $x, y \in B$, $a \leq x \vee y$ si, i només si $a \leq x$ o $a \leq y$

Prova:

i) Com hem vist al teorema 4.2, $a \leq x \iff a \wedge x' = 0 \iff a \nleq x'$, per tant, a no pot ser menor o igual que un element i el seu conjugat alhora, però ho ha de ser a un dels dos.

ii) Al ser $x \wedge y$ l'ínfim de $\{x, y\}$, $a \leq x \wedge y$ si, i només si, $a \leq x$ i $a \leq y$.

iii) El fet que $a \leq x \vee y$ és equivalent a $a = a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y)$ de tal manera que a és igual al suprem de $\{a \wedge x, a \wedge y\}$. Si suposem que $a \neq a \wedge x$, aleshores necessàriament $a \wedge x$ és menor que a i, per ser a un àtom, $a \wedge x = 0$. Per altra banda, $a \wedge y = a$, la qual cosa és equivalent a $a \leq y$.

Proposició 4.2: Sigui L un reticle qualsevol, aleshores es satisfan les següents implicacions:

i) L és una àlgebra de Boole $\Longrightarrow L$ és un reticle relativament complementat.

ii) L és un reticle relativament complementat $\Longrightarrow L$ és un reticle seccionalment complementat.

iii) L és un reticle finit i seccionalment complementat $\Longrightarrow$ qualsevol $a \in L, a \neq 0$ pot ser expressat com una unió finita de àtoms.

Prova:

i) Sigui L una àlgebra de Boole i $a \leq x \leq b$, definim $y = b \wedge (a \vee x')$. Aleshores, y és un complementari de x a $[a, b]$ atès que

$$x \wedge y = x \wedge (b \wedge (a \vee x')) = x \wedge ((b \wedge a) \vee (b \wedge x')) = (x \wedge a) \vee (x \wedge (b \wedge x')) = a \vee 0 = a,$$

$$x \vee y = x \vee (b \wedge (a \vee x')) = x \vee ((b \wedge a) \vee (b \wedge x')) = (x \vee a) \vee (x \vee (b \wedge x')) = x \vee b = b.$$

Així doncs, L és relativament complementat.

ii) Si L és relativament complementat, aleshores $[a, b]$ és complementat per a tot $a, b \in L$. En particular, això succeeix per $a = 0$, és a dir, $[0, b]$ és complementat i L seccionalment complementat.

iii) Siguin $\{p_1, \ldots, p_n\}$ el conjunt d'àtoms tals que $p_i \leq a \in L$ per a tot $i \in \{1, \ldots, n\}$ i $b = p_1 \vee \cdots \vee p_n$. Aleshores, $b \leq a$ i suposarem $b \neq a$ de tal manera que b tindrà un complementari, anomenem-lo c, en $[0, a]$. Sigui p un àtom tal que $p \leq c$, aleshores $p \in \{p_1, \ldots, p_n\}$ i $p = p \wedge b \leq c \wedge b = 0$ i ens trobem amb una contradicció. Per tant, $a = b = p_1 \wedge \cdots \wedge p_n$.

Vists aquests dos resultats, ja podem enunciar el teorema de representació de Stone pel cas finit.

Teorema 4.3 (Representació de Stone): Sigui B una àlgebra de Boole finita, $A = \mathrm{At}(B)$, aleshores és isomorfa a $\mathcal{P}(A)$, és a dir

$$(B, \wedge, \vee) \cong_b (\mathcal{P}(A), \cap, \cup).$$

Prova: Sigui $v \in B$ un element qualsevol, definim $A(v) := \{a \in A \mid a \leq v\}$. Així, $A(v) \subseteq A$ i podem definir

$$\begin{array}{rccc} h: & B & \longrightarrow & \mathcal{P}(A) \\ & v & \longmapsto & A(v) \end{array}$$

Veurem que l'aplicació h es tracta d'un isomorfisme booleà, començant per comprovar que es tracta d'un morfisme booleà. Sigui $a \in B$ un àtom i $v, w \in B$ dos elements qualsevols, tenim que:

i) $a \in A(v') \iff a \leq v' \iff a \not\leq v \iff a \in A \setminus A(v)$, essent la segona equivalència conseqüència de la proposició 5.1 ii). D'aquesta manera, tenim que $h(v') = h(v)'$

ii) $a \in A(v \wedge w) \iff a \leq v \wedge w \iff a \leq v$ i $a \leq w \iff a \in A(v) \cap A(w)$, essent la segona equivalència conseqüència de la proposició 5.1 iii). D'aquesta manera, tenim que $h(v \wedge w) = h(v) \wedge h(w)$.

iii) $a \in A(v \vee w) \iff a \leq v \vee w \iff a \leq v$ o $a \leq w \iff a \in A(v) \cup A(w)$, essent la segona equivalència conseqüència de la proposició 5.1 iv). D'aquesta manera, tenim que $h(v \vee w) = h(v) \vee h(w)$

Com que B és finit, podem utilitzar la proposició 5.2 per demostrar que l'aplicació és bijectiva i, per tant, un isomorfisme. Sabem que qualsevol $v \in B$ pot ser expressat com una unió finita d'àtoms, $v = a_1 \vee \cdots \vee a_n$, amb tots ells satisfent $a_i \leq v$. Siguin v, w tals que $h(v) = h(w)$ – és a dir, $A(v) = A(w)$ – aleshores $a_i \in A(v)$ i $a_i \in A(w)$. D'aquesta manera, $a_i \leq w$ i $v \wedge w = (a_1 \vee \cdots \vee a_n) \wedge w = (a_1 \wedge w) \vee \cdots \vee (a_n \wedge w) = w$. Per tant, $w \leq v$ i, intercanviant els rols de v i w, obtenim $v = w$. Així doncs, hem vist que h és injectiva.

Per veure que h és també exhaustiva, hem de demostrar que per a cada $C \in \mathcal{P}(A)$ existeix algun $v \in B$ tal que $h(v) = C$. Sigui $C = \{c_1 \ldots c_n\}$ i $v = c_1 \vee \cdots \vee c_n$, aleshores $C \subseteq A(v)$ i, així, $C \subseteq h(v)$. Per contra, si $a \in h(v)$, aleshores a és un àtom amb $a \leq v = c_1 \vee \cdots \vee c_n$. Així, $a \leq c_i$ per algun $i \in \{1, \ldots, n\}$ i, per tant, $a = c_i \in C$ i $h(v) \subseteq C$. Així doncs, hem vist que $h(v) = C$ i que h és exhaustiva.

Corol·lari 4.4: El cardinal de qualsevol àlgebra de Boole B és sempre de la forma 2^n, essent n el nombre de àtoms de B. A més, qualsevol parell d'àlgebres de Boole finites amb mateix cardinal són isomorfes.

Exemple 4.5:

i) Per a cada àlgebra de Boole $B \neq \{0\}$, existeix alguna $n \in N$ tal que $B \cong_b \{0,1\}^n = \mathbb{B}^n$. En el cas $n = 2$ i $B = \{a, b, c, d\}$, podem construir els diagrames de Hasse següents

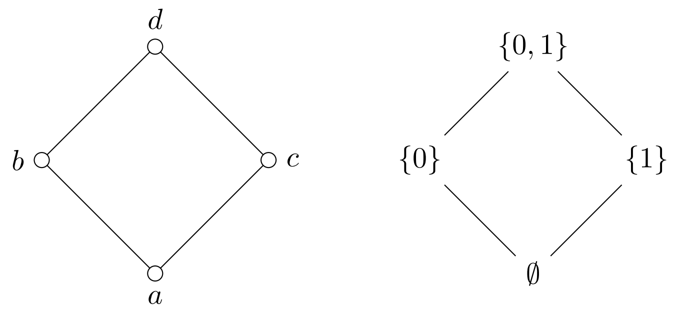


Figura 5.1: $B \cong_b \mathbb{B}^n$

ii) El reticle dels divisors de 42, és a dir, l'àlgebra de Boole $B = (\{1, 2, 3, 6, 7, 14, 21, 42\})$, té $8 = 2^3$ elements i és isomorf al reticle potència $\mathcal{P}(\{a, b, c\})$. Els diagrama de Hasse resultants seran

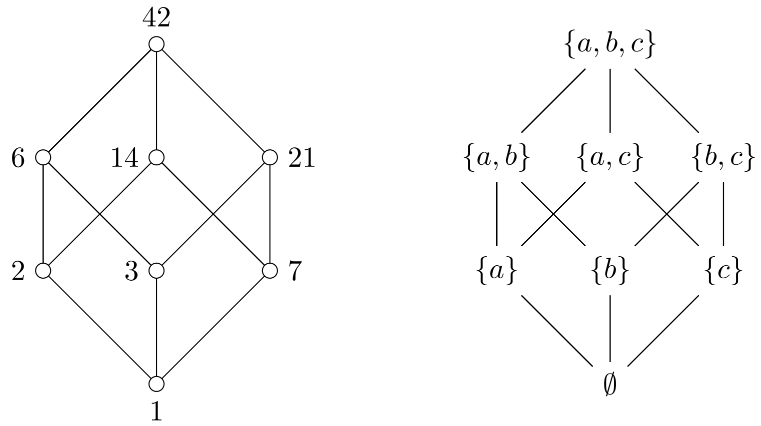


Figura 5.2: $B \cong_b \mathcal{P}(\{a, b, c\})$

Nota: La identificació d'una àlgebra de Boole arbitrària amb l'àlgebra potència no és sempre possible en el cas infinit. De manera similar al teorema de representació vist anteriorment, es pot veure que tota àlgebra de Boole atòmica i completa és isomorfa a l'algebra potència i, encara més, que qualsevol àlgebra de Boole és isomorfa a una àlgebra de conjunts.

Capítol 5

Teorema de representació de Birkhoff

En aquest capítol demostrarem el segon dels teoremes objectius del treball, el teorema de representació de Birkhoff. Aquest, essencialment ens diu que qualsevol reticle distributiu finit és isomorf al conjunt de tots els ideals del conjunt de tots els elements irreductibles respecte la unió, és a dir, $L \cong \mathcal{I}(\mathcal{J}(L))$. Les referències principals són [3] i [5].

Abans d'enunciar-lo formalment i demostrar-lo en si, veurem un seguit de proposicions que ens seran útils a l'hora de provar el resultat final.

Proposició 5.1: Sigui $f : L \longrightarrow M$ una aplicació entre els reticles L i M,

i) Les següents condicions són equivalents:

   a) f preserva l'ordre

   b) $f(x \vee y) \geq f(x) \vee f(y)$ per a tot $x, y \in L$

   c) $f(x \wedge y) \leq f(x) \wedge f(y)$ per a tot $x, y \in L$

   En particular, si f és un morfisme de reticles, aleshores preserva l'ordre.

ii) f és un isomorfisme de reticles si, i només si, f és un isomorfisme d'ordre.

Prova:

i) Comencem veient l'equivalència entre a) i b). Tenim que per a tot $x, y \in L$, $x, y \leq x \vee y$. Com que f preserva l'ordre, també és cert que $f(x), f(y) \leq f(x \vee y)$ i, per tant, $f(x) \vee f(y) \leq$

$f(x \vee y)$. Recíprocament, siguin $x, y \in L$ tals que $x \leq y$, tenim que $x \vee y = y$. D'aquesta manera, $f(x \vee y) = f(y) \geq f(x) \vee f(y) \geq f(x)$.

De manera similar, veurem l'equivalència entre a) i c) i així ja haurem acabat. Ara, utilitzem que $x, y \geq x \wedge y$ i que, com que f preserva l'ordre, tenim que $f(x), f(y) \geq f(x \wedge y)$. D'aquesta manera, es compleix que $f(x) \wedge f(y) \geq f(x \wedge y)$. Per altra banda, siguin $x, y \in L$ tals que $x \leq y$, tenim que $x \wedge y = x$. Així, $f(x \wedge y) = f(x) \leq f(x) \wedge f(y) \leq f(y)$.

ii) Per veure la implicació cap a la dreta, suposem que f és un morfisme de reticles. D'aquesta manera, $x \leq y \Longrightarrow x \vee y = y \Longrightarrow f(x \vee y) = f(y) \Longrightarrow f(x) \vee f(y) = f(y) \Longrightarrow f(x) \leq f(y)$, per tant, f és un morfisme d'ordre.

Recíprocament, assumim que f és un morfisme d'ordre i, per tant, un morfisme bijectiu. Per l'apartat i) i per dualitat, serà suficient demostrar que $f(x \vee y) \leq f(x) \vee f(y)$ per a tot $x, y \in L$. Com que f és exhaustiva, podem garantir que existeix $z \in L$ tal que $f(z) = f(x) \vee f(y)$. Així, $f(x) \leq f(z)$ i $f(y) \leq f(z)$, d'on es segueix que $x \leq z$ i $y \leq z$ per tractar-se f d'un morfisme d'ordre. D'aquesta manera, $x \vee y \leq z$ i $f(x \vee y) \leq f(z) = f(x) \vee f(y)$ tal i com volíem demostrar.

Proposició 5.2: Sigui L un reticle finit, aleshores:

i) Siguin $a, b \in L$ amb $a \nleq b$, existeix $x \in \mathcal{J}(L)$ tal que $x \leq a$ i $x \nleq b$

ii) $a = \bigvee\{x \in \mathcal{J}(L) \mid x \leq a\}$ per a tot $a \in L$

Prova:

i) Sigui $S = \{x \in L \mid x \leq a \text{ i } x \nleq b\}$, el conjunt S és no buit ja que conté, com a mínim, l'element a. Atès que L és finit, existeix un element minimal x de S que expressarem com $x = c \vee d$ amb $c < x$ i $d < x$. Per la minimalitat de x, c i d no poden pertànyer al conjunt i tenim que $c < x \leq a$ i $d < x \leq a$, és a dir, $c \leq a$ i $d \leq a$. Així, $c, d \notin S$ implica que $c \leq b$ i $d \leq b$, però aleshores $x = c \vee d \leq b$ el qual és una contradicció. D'aquesta manera, hem vist que $x \in \mathcal{J}(L)$ tal i com volíem demostrar.

ii) Sigui $T = \{x \in \mathcal{J}(L) \mid x \leq a\}$, a és clarament una fita superior de T. Considerem c una fita superior qualsevol de L i suposem $a \nleq c$. Aleshores, $a \nleq a \wedge c$ i, per l'apartat anterior, existeix $x \in \mathcal{J}(L)$ amb $x \leq a$, $x \nleq a \wedge c$. Per tant, $x \in T$ i $x \leq c$ atès que c és una fita superior de T. Així, x és una fita inferior de $\{a, c\}$ i, conseqüentment, $x \leq a \wedge c$, la qual cosa és una contradicció. D'aquesta manera, $a \leq c$ i $a = \bigvee T$ a L tal i com volíem demostrar.

Proposició 5.3: Siguin L un reticle finit i $x \in L$, $x \neq 0$, aleshores les següents condicions són equivalents:

i) x és irreductible respecte la unió

ii) si $y, z \in L$ i $x \leq y \vee z$, aleshores $x \leq y$ o $x \leq z$

iii) per a tot $k \in \mathbb{N}$, si $a_1, \ldots, a_k \in L$ i $x \leq a_1 \vee \cdots \vee a_k$, aleshores $x \leq a_i$ per algun $i \in \{1, \ldots, k\}$

Prova: Per veure que i) implica ii), considerem $x \in \mathcal{J}(L)$ i $y, z \in L$ tals que $x \leq y \vee z$. Aquest fet és equivalent a $x = x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Com que x és irreductible, tenim que $x = x \wedge y$ o $x = x \wedge z$, la qual cosa es tradueix a $x \leq y$ o $x \leq z$.

El fet que ii) impliqui iii) es veu per inducció sobre k, iniciant aquesta amb el cas $k = 2$ corresponent a l'hipòtesi inicial. Que iii) implica ii) és trivial.

Així, només ens queda demostrar que ii) implica i). Suposem $x = y \vee z$, en particular tenim $x \leq y \vee z$ i, per hipòtesis $x \leq y$ o $x \leq z$. D'aquesta manera, com que $x = y \vee z$, $x \geq y$ i $x \geq z$ i, per tant, $x = y$ o $x = z$.

Teorema 5.4 (Representació de Birkhoff): Siguin L un reticle distributiu finit, $\mathcal{J}(L)$ el conjunt d'elements irreductibles respecte la unió i $\mathcal{I}(\mathcal{J}(L))$ el conjunt d'ideals d'aquest últim conjunt, aleshores l'aplicació $\eta : L \longrightarrow \mathcal{I}(\mathcal{J}(L))$ definida per

$$\eta(a) = \{x \in \mathcal{J}(L) \mid x \leq a\}$$

és un isomorfisme de L a $\mathcal{I}(\mathcal{J}(L))$.

Prova: Veiem primer breument que η aplica de L a $\mathcal{I}(\mathcal{J}(L))$. Sigui $a \in L$, tenim que $x, y \in \eta(a) \Longrightarrow x, y \leq a \Longrightarrow x \vee y \leq a \Longrightarrow x \vee y \in \eta(a)$. Prenent ara $x \in L$ i $y \in \eta(a)$, $x \leq y \Longrightarrow x \leq a \Longrightarrow x \in \eta(a)$. D'aquesta manera, hem vist que $\eta(a) \in \mathcal{I}(\mathcal{J}(L))$.

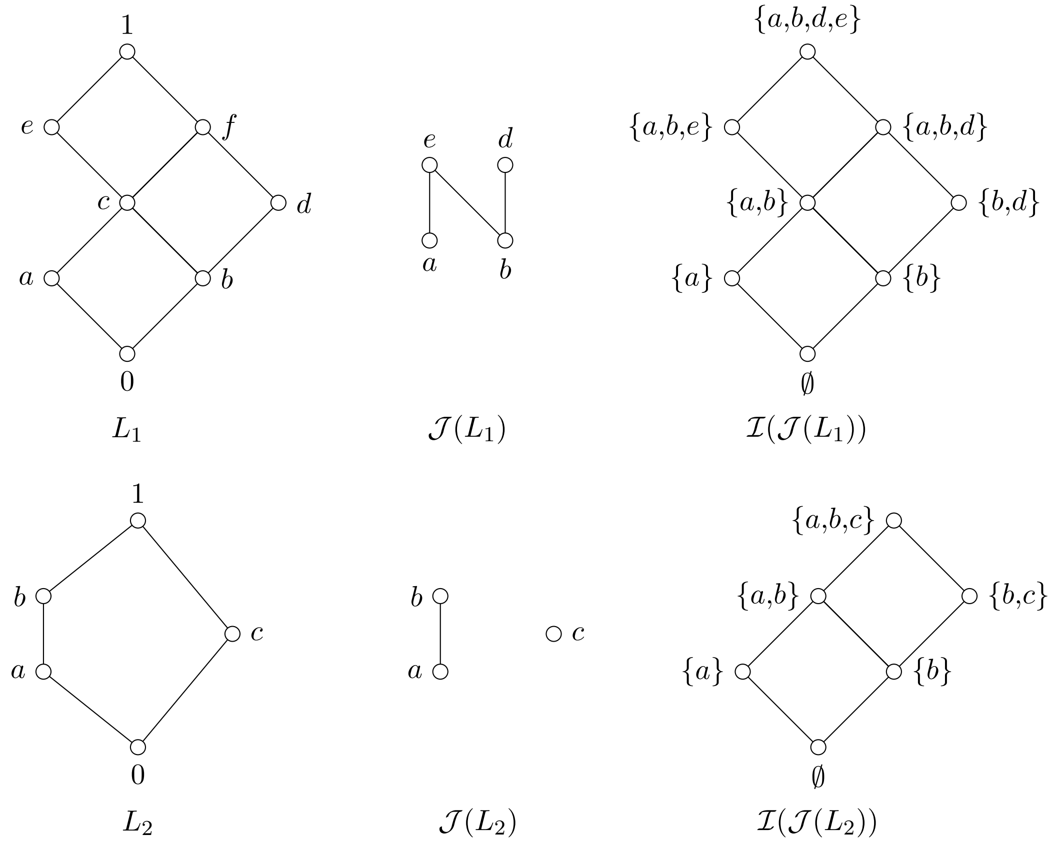
La proposició 6.1 ens garanteix que serà suficient demostrar que η és un isomorfisme d'ordre, és a dir, que $a \leq b$ a $L \Longleftrightarrow \eta(a) \subseteq \eta(b)$ a $\mathcal{I}(\mathcal{J}(L))$. Per veure la implicació cap a la dreta, utilitzem que $x \in \eta(a) \Longrightarrow x \leq a \Longrightarrow x \leq b \Longrightarrow x \in \eta(b)$. Per veure la implicació cap a l'esquerra, utilitzem la proposició 6.2 i el fet que, donats dos conjunts S, T amb $S \subseteq T$, aleshores $\bigvee S \leq \bigvee T$. Així, tenim que $a = \bigvee \eta(a) \leq \bigvee \eta(b) = b$

Per acabar, ens falta veure que si $U \in \mathcal{I}(\mathcal{J}(L))$, aleshores $U = \eta(a)$ per algun $a \in L$. Com que $\eta(0) = \emptyset$, podem prendre $\emptyset \neq U \in \mathcal{I}(\mathcal{J}(L))$ i escriure'l com $U = \{a_1, \ldots, a_k\}$. Definint $a = a_1 \vee \cdots \vee a_k$ veurem que $U = \eta(a)$. Per veure la inclusió cap a la dreta, és a dir, $U \subseteq \eta(a)$, prenem $x \in U$ qualsevol. Així, $x = a_i$ per algun i i tenim que x és irreductible respecte la unió i $x \leq a$, per tant $x \in \eta(a)$. Per veure la inclusió cap a l'esquerra, prenem $x \in \eta(a)$. Aleshores, $x \leq a = a_1 \vee \cdots \vee a_k$ i, per la proposició 6.3, $x \leq a_i$ per algun i. Com que U és un ideal i $a_i \in U$, tenim $x \in U$.

Corol·lari 5.5: Sigui L un reticle finit, L és distributiu $\Longleftrightarrow L \cong \mathcal{I}(\mathcal{J}(L))$.

Exemple 5.6:

i) Començarem amb un exemple senzill que ens permetrà comprovar que el Corol·lari 6.5 ens presenta un resultat alternatiu al Teorema 3.10. A la figura 6.1, podem veure els diagrames de Hasse de L, $\mathcal{J}(L)$ i $\mathcal{I}(\mathcal{J}(L))$ de dos reticles.



El primer d'ells, L_1 es tracta d'un reticle distributiu al ser isomorf a $\mathcal{I}(\mathcal{J}(L_1))$ i al no contenir cap subreticle isomorf al pentagon o al diamant. Per altra banda, L_2 no es isomorf a $\mathcal{I}(\mathcal{J}(L_2))$ i es confirma que no es distributiu.

Abans de veure un segon exemple una mica més sofisticat, estudiarem detalladament una família d'objectes anomenats clutters.

Sigui $\Omega \neq 0$ un conjunt finit, un **clutter** sobre Ω és una família $C = \{A_1, \ldots, A_r\}$ amb $A_i \subseteq \Omega$ no comparables, és a dir, $A_i \subseteq A_j \Longrightarrow A_i = A_j$ per a tot i, j. Definim $Clut(\Omega) \subseteq \mathcal{P}(\mathcal{P}(\Omega))$ com el conjunt de tots els clutters sobre Ω.

Proposició 5.7: Siguin $C_1, C_2 \in Clut(\Omega)$ i $\leq$ l'operació definida per

$$C_1 \leq C_2 \Longleftrightarrow \forall A \in C_1, \text{ existeix } B \in C_2 \text{ tal que } A \subseteq B,$$

aleshores $(Clut(\Omega), \leq)$ és un reticle distributiu.

Prova: Definim les operacions $\vee$ i $\wedge$ com

$$C_1 \vee C_2 = \bigcup_{i,j \in \{1,2\}} \{A \in C_i \mid \text{ existeix } B \in C_j \text{ amb } B \subseteq A\},$$

$$C_1 \wedge C_2 = \bigcup_{i,j \in \{1,2\}} \{A \in C_i \mid \text{ existeix } B \in C_j \text{ amb } A \subseteq B\}.$$

D'aquesta manera es satisfà $C_1 \wedge C_2 \leq C_1, C_2 \leq C_1 \vee C_2$ i hem de veure que $C_1 \wedge (C_2 \vee C_3) = (C_1 \wedge C_2) \vee (C_1 \wedge C_3)$ per a tot $C_1, C_2, C_3 \in Clut(\Omega)$.

i) Sigui $A \in C_1 \wedge (C_2 \vee C_3)$, volem veure que $A \in (C_1 \wedge C_2) \vee (C_1 \wedge C_3)$.

Si $A \in C_2 \vee C_3$ amb $A \subseteq B \in C_1$, suposem que $A \in C_2$ i existeix $D \in C_3$ tal que $D \subseteq A$. D'aquesta manera, tenim que $A \in C_1 \wedge C_2$ ja que $A \subseteq B \in C_1$ i només falta veure que existeix $E \in C_1 \wedge C_3$ tal que $E \subseteq A$. Com que $D \subseteq A \subseteq B \in C_1$, podem prendre $E = D$ que també pertany a $C_1 \wedge C_3$ i ja ho tenim. Si $A \in C_1$ es demostra de manera similar.

ii) Sigui $A \in (C_1 \wedge C_2) \vee (C_1 \wedge C_3)$, volem veure que $A \in C_1 \wedge (C_2 \vee C_3)$.

Si $A \in C_1 \wedge C_2$ amb $B \subseteq A, B \in C_1 \wedge C_3$ (la demostració és completament anàloga si ho considerem al revés), suposem que $A \in C_2$ i existeix $D \in C_1$ tal que $A \subseteq D$. Si $B \in C_1$ amb $B \subseteq E \in C_3$, tenim $B \subseteq A \subseteq D$, la qual cosa implica $B = A = D$ per ser C_1 un clutter i no té sentit. Per tant, $B \in C_3$ amb $B \subseteq E \in C_1$ i tenim que $A \in C_2 \vee C_3$ ja que $A \in C_2$ i $B \subseteq A, B \in C_3$. Així, com que $A \subseteq D \in C_1$, tenim que $A \in C_1 \wedge (C_2 \vee C_3)$.

Per altra banda, si $A \in C_1$ amb $A \subseteq D \in C_2$, suposem $B \in C_3$ (ara B no pot pertànyer també a C_1 al ser un clutter) amb $B \subseteq E \in C_1$ i tenim que $B \subseteq A \subseteq D$. Per tant, $D \in C_2 \vee C_3$ i, com que $A \in C_1, A \subseteq D$, tenim que $A \in C_1 \wedge (C_2 \vee C_3)$.

Així doncs, hem vist que $C_1 \wedge (C_2 \vee C_3) = (C_1 \wedge C_2) \vee (C_1 \wedge C_3)$ per a tot $C_1, C_2, C_3 \in Clut(\Omega)$ i que, per tant, $(Clut(\Omega), \leq)$ és un reticle distributiu.

Un cop estudiades aquestes definicions i propietats, ja podem tornar al segon exemple que volíem veure.

ii) Sigui $Clut(\Omega)$ el conjunt de tots els clutters sobre $\Omega \neq 0$ conjunt finit, $C = \{A_1, \ldots, A_r\} \in Clut(\Omega)$, definim $\downarrow C = \{H \in Clut(\Omega) \mid H \leq C\}$, és a dir, $H = \{H_1, \ldots, H_n\}$ i per a tot H_i, existeix A_j tal que $H_i \subseteq A_j$. D'aquesta manera, podem descriure $\mathcal{I}(\mathcal{J}(Clut(\Omega)))$ com les famílies Γ de subconjunts de Ω "decreixents", és a dir, famílies tals que

$$B \in \Gamma, B' \subseteq B \Longrightarrow B' \in \Gamma.$$

Per tant, podem construir l'isomorfisme

$$\begin{array}{ccc} Clut(\Omega) & \longleftrightarrow & Decr(\Omega) \\ C & \longleftrightarrow & \Gamma \end{array}$$

que envia cada clutter $\{C_1, \ldots, C_r\}$ a la família decreixent que té per elements maximals $C_1, \ldots, C_r$.

Corol·lari 5.8 (Teorema de representació de Stone): Sigui B una àlgebra de Boole finita, $A = \mathrm{At}(B)$, aleshores és isomorfa a $\mathcal{P}(A)$, és a dir

$$(B, \wedge, \vee) \cong_b (\mathcal{P}(A), \cap, \cup).$$

Prova: Sabem que, per la pròpia definició, tota àlgebra de Boole és, en particular, un reticle distributiu. D'aquesta manera, només hem de veure que podem identificar $\mathcal{J}(B)$ amb $\mathrm{At}(B)$ per demostrar el corol·lari.

Sabem pel lema 2.23 que cada àtom d'un reticle L amb element minimal (és el cas de les àlgebres de Boole) és irreductible respecte la unió. Per altra banda, pel lema 2.25 sabem també que cada element irreductible respecte la unió d'un reticle L distributiu i complementat (també és el cas de les àlgebres de Boole) és un àtom. Per tant, ja hem vist $\mathcal{J}(B) = \mathrm{At}(B)$ i demostrat el corol·lari.

Bibliografia

[1] R. Lidl, G.Plitz: Applied Abstract Algebra, 2a edició, Springer, 1997.

[2] Bernd S. W. Schröder: Ordered Sets - An Introduction, Birkhäuser, 2003.

[3] B. A. Davey, H. A. Priestley: Introduction to Lattices and Order, 2a edició, Cambridge University Press, 2002.

[4] George Grätzer: General Lattice Theory, 2a edició, Birkhäuser, 1998.

[5] Yilong Yang: Notes for Introduction to Lattice theory, https://www.math.ucla.edu/ yy26/works/Lattice%20Talk.pdf, 2013.

[6] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, Elena Yudovina : Introduction to representation theory, http://math.mit.edu/ etingof/replect.pdf, 2011.

[7] P. Halmos: Lectures on Boolean Algebras, Van Nostrand, New York, 1963.

[8] R. Balbes, Ph. Dwinger: Distributive Lattices, University of Missouri Press, Missouri, 1974.

[9] D. Monk: Handbook of Boolean Algebras, North Holland, Volume 1,2 and 3, 1989.

[10] Clara María Corbalán Mirete: Álgebras de Boole y la dualidad de Stone, https://temat.es/wp-content/uploads/2019/05/2019-p75.pdf, 2018.