Treball Fi de Grau - Curs 2022/2023

Àlgebra Universal

Autor: **ROSA PUIG VICTORIA**

Tutor: ENRIC COSME LLÓPEZ

Facultat de Matemàtiques Grau en Matemàtiques

Índex

CAPíTOL 1

Introducció

La majoria dels matemàtics es troben per primera vegada amb estructures algebraiques en els exemples clàssics de grups, anells i espais vectorials. En cadascuna d'aquestes àrees sorgeixen temes comuns, com l'existència de conjunts d'objectes que es tanquen baix una o més operacions realitzades sobre els objectes o l'interés en subconjunts que tenen la mateixa estructura (subgrups, subespais,...), en aplicacions que preserven l'estructura o en la construcció de noves estructures a partir d'antigues.

Així, l'àlgebra universal és l'àrea de les matemàtiques encarregada de generalitzar aquests casos particulars d'estructures per obtenir l'estructura d'una àlgebra: un conjunt d'objectes, amb una o més operacions definides en el conjunt [**7**].

L'àlgebra universal va nàixer a principis del segle XX amb el propòsit de desenvolupar un marc formal en el qual es pogueren considerar i analitzar estructures algebraiques de diferent natura a través d'un procés d'abstracció dels conceptes ja estudiats. Aquesta àrea d'estudi va evolucionar ràpidament i, després d'un segle des de la seua concepció, s'ha transformat en un cos de coneixement vibrant de la matemàtica contemporània.

En l'estudi de les propietats comunes a totes les estructures algebraiques, els reticles juguen un doble paper [**3**]. D'una banda, els reticles són àlgebres i per tant, compleixen les característiques d'aquests tipus d'estructures. D'altra banda, la teoria reticular aporta a l'estudi de l'àlgebra universal una noció especial d'ordre que ens conduirà a una millor comprensió de les àlgebres. Va ser Garrett Birkhoff a mitjans de la dècada de 1930 qui va iniciar el desenvolupament general de la teoria reticular. En una sèrie d'articles [**5**], va mostrar que la teoria dels reticles proporciona un marc unificador per a desenvolupaments fins ara no relacionats en moltes disciplines matemàtiques, ja que els conjunts ordenats i, en particular, els reticles, apareixen amb freqüència en multitud de contextos i poden utilitzar-se com a eines per a entendre o demostrar resultats en diverses àrees [**8**].

És per això que, abans d'introduir-nos en el món de les àlgebres, dedicarem un capítol a l'estudi de la teoria de l'ordre donada pels reticles. Encara que aquesta teoria és un camp molt ampli i podria considerar-se, per dret propi, una branca de les matemàtiques [**1**], en el capítol només ens centrarem en alguns resultats que ens resulten d'interés per a l'estudi de l'àlgebra universal.

Una volta vist aquests conceptes, ens endinsarem progressivament en l'àlgebra universal fent un recorregut des de la definició i exemples bàsics d'àlgebres ja conegudes fins a arribar als teoremes d'isomorfia i a l'àlgebra de termes, estudiant les nocions necessàries per a demostrar aquests teoremes, com els homomorfismes entre àlgebres i les congruències. Cal destacar la importància dels teoremes d'isomorfia en l'àlgebra universal, ja que es tracta d'una sèrie de resultats que ens permeten aprofundir en el coneixement de les estructures algebraiques i establir connexions significatives entre elles.

En conclusió, el treball presenta una introducció a la teoria de l'àlgebra universal, estudiant resultats ja vists al llarg de la carrera, com els homomorfismes i els teoremes d'isomorfia, però sense treballar en estructures concretes com els grups o anells, sinó de forma més general amb la noció d'àlgebra.

A continuació, resumim breument el contingut de cadascun dels següents capítols d'aquest treball. El lector pot trobar una descripció més detallada al principi de cada capítol.

En el Capítol 2, *Teoria de l'ordre*, com hem mencionat abans, ens centrarem en l'estudi dels reticles. Veurem dues definicions de reticle que són equivalents, i definirem les nocions de reticles isomorfs i subreticles. També treballarem amb dos tipus de reticles molt característics, els distributius i els modulars. Per últim, ens centrarem en els reticles complets, algebraics i en els operadors de clausura, i estudiarem un cas concret de reticle complet, el de les relacions d'equivalència d'un conjunt.

Al Capítol 3, *Elements de l'Àlgebra Universal*, començarem introduint la noció d'àlgebra i exemples d'estructures algebraiques. També introduirem el concepte d'homomorfisme entre dues àlgebres. Després ens centrarem l'estudi de les subestructures de les àlgebres, centrantnos principalment en la subàlgebra generada per un conjunt i en l'estructura de reticle que presenta el conjunt de subàlgebres d'una àlgebra. També treballarem amb les congruències, estudiant l'espai quocient associat, el conjunt de totes les congruències d'una àlgebra i la relació que existeix entre aquestes relacions i els homomorfismes. Lligat als homomorfismes, estudiarem i demostrarem els teoremes d'isomorfia,

així com explicarem les principals conseqüències d'aquests resultats. En últim lloc, treballarem amb un exemple d'àlgebra on els teoremes d'isomorfia reben especial importància, les àlgebres de termes.

Per últim, al Capítol 4 exposem les conclusions sobre els resultats més importants d'aquest treball.

En tot el contingut d'aquest treball emprarem conceptes i construccions estàndards de l'àlgebra universal clàssica [**12, 4**] i la teoria de conjunts [**6**]. Malgrat això, també hem adoptat les següents convencions.

En primer lloc, donats dos enters $a, b \in \mathbb{Z}$ escriurem el màxim comú divisor d'a i b com $\mathrm{mcd}(a, b)$ i el mínim comú múltiple com $\mathrm{mcm}(a, b)$.

A més, considerarem que un ordinal és un conjunt transitiu que està ben ordenat, de manera que si considerem $\mathbb{N}$ el conjunt dels nombres naturals, per cada n en $\mathbb{N}$, es té que $n = \{0, \ldots, n-1\}$. Siga A un conjunt, considerarem $A^0 = 1 = \{\emptyset\}$ i A^n el conjunt de n-tuples d'elements d'A. A més, denotarem per $\mathcal{P}(A)$ el conjunt de tots els conjunts X tals que $X \subseteq A$, és a dir, el conjunt de les parts d'A.

Per últim, donats A i B dos conjunts, si f és una aplicació d'A a B, aleshores l'aplicació $f[\cdot]$ de formació de la imatge directa de f, que va de $\mathcal{P}(A)$ a $\mathcal{P}(B)$, envia un conjunt X en $\mathcal{P}(A)$ a $f[X] = \{f(x) \in B \mid x \in X\}$ en $\mathcal{P}(B)$, i l'aplicació $f^{-1}[\cdot]$ de $\mathcal{P}(B)$ a $\mathcal{P}(A)$ de formació de la imatge inversa de f envia un conjunt Y en $\mathcal{P}(B)$ a $f^{-1}[Y] = \{x \in A \mid f(x) \in Y\}$ en $\mathcal{P}(A)$. També, per a una aplicació f d'A en B i un subconjunt X d'A, escriurem $\mathrm{Ker}(f)$ per al nucli de f, $\mathrm{Im}(f)$ per a expressar $f[A]$, i la restricció de f en X la denotarem per $f_{\restriction X}$. A més, si A i B són dos conjunts, denotarem per $\mathrm{Hom}(A, B)$ al conjunt de les aplicacions d'A en B.

En els diferents capítols introduirem nocions i construccions més específiques.

CAPíTOL 2

Teoria de l'ordre

> Never in the history of mathematics has a mathematical theory been the object of such vociferous vituperation as lattice theory.
>
> *Gian-Carlo Rota* [**11**]

En aquest capítol, l'objectiu és familiaritzar-se amb els conceptes i resultats de la teoria de reticles. Amb aquesta intenció, hem dividit aquest capítol en diferents seccions que, progressivament ens permetran conèixer aquestes estructures algebraiques.

En la Secció 1, titulada *Definicions de Reticles*, caracteritzarem de dues maneres diferents els reticles, per a després veure que ambdues definicions són equivalents. En la Secció 2, titulada *Reticles Isomorfs i Subreticles*, introduirem les nocions d'isomorfisme entre reticles i de subreticle. En la Secció 3, titulada *Reticles Distributius i Modulars*, després de definir aquests tipus de reticles, veurem diversos resultats que ens permetran identificar-los. En la Secció 4, titulada *Reticles Complets, Reticles Algebraics i Relacions d'Equivalència*, primer definirem la noció de reticle complet i veurem un teorema per a identificar-los. A continuació, introduirem la noció de reticle algebraic i, després de fer un recordatori de les relacions d'equivalència, demostrarem el resultat més important d'aquesta subsecció: El conjunt de relacions d'equivalència sobre un conjunt A amb la inclusió de subconjunts és un reticle complet. Finalment, la Secció 5, titulada *Operadors de Clausura*, està dedicada a l'estudi dels operadors de clausura i la seua relació amb els reticles complets i algebraics. Per últim, demostrarem que tot reticle algebraic és isomorf al reticle de subconjunts tancats d'un conjunt amb un operador de clausura algebraic.

1. Definicions de Reticles

L'origen del concepte de reticle es remunta a l'anàlisi del pensament de Boole i a l'estudi de la divisibilitat de Dedekind al segle XIX. No

obstant això, va ser en la dècada de 1930 quan va prosperar, especialment a partir de la publicació del llibre de Birkhoff *Lattice Theory* [**5**] en la dècada de 1940.

Existeixen dues maneres diferents de definir un reticle. D'una banda, el podem definir des d'un punt de vista algebraic, posant-lo al mateix nivell que els grups o els anells. D'altra banda, el podem definir basant-nos en la noció d'ordre, que ens ofereix una visió geomètrica d'aquest. Com s'ha mencionat abans, l'objectiu principal d'aquesta secció és veure que les dues definicions són equivalents.

DEFINICIÓ 2.1. *Siga L un conjunt no buit amb dues operacions binàries definides en L, $\vee$ "suprem" i $\wedge$ "ínfim". Direm que L és un* **reticle** *si satisfà les següents identitats. Per a tot $x, y, z \in L$*

Propietat commutativa

$$x \vee y = y \vee x; \qquad x \wedge y = y \wedge x. \tag{R1}$$

Propietat associativa

$$x \vee (y \vee z) = (x \vee y) \vee z; \qquad x \wedge (y \wedge z) = (x \wedge y) \wedge z. \tag{R2}$$

Lleis d'idempotència

$$x \vee x = x; \qquad x \wedge x = x. \tag{R3}$$

Lleis d'absorció

$$x = x \vee (x \wedge y); \qquad x = x \wedge (x \vee y). \tag{R4}$$

EXEMPLE 2.2. *Considerem $\mathbb{N}$ i les operacions*

$$n \vee m = \operatorname{mcm}(n, m), \ \text{ i } n \wedge m = \operatorname{mcd}(n, m).$$

Així, $(\mathbb{N}, \operatorname{mcm}, \operatorname{mcd})$ *és un reticle, ja que satisfà les condicions citades anteriorment.*

A continuació, introduirem els conceptes que ens permetran presentar la segona definició de reticle.

DEFINICIÓ 2.3. *Una relació binària $\leq$ definida en un conjunt A és un* **ordre parcial en** *A si compleix les següents propietats. Per a tot $a, b, c \in A$,*

Reflexiva

$$a \leq a. \tag{O1}$$

Antisimètrica

$$\text{Si } a \leq b \text{ i } b \leq a, \text{ aleshores } a = b. \tag{O2}$$

Transitiva

$$\text{Si } a \leq b \text{ i } b \leq c, \text{ aleshores } a \leq c. \tag{O3}$$

A més, si per a tot $a, b \in A$ es té que $a \leq b$ o $b \leq a$ es diu que $\leq$ és un **ordre total en** *A. Un conjunt no buit amb un ordre parcial és un* **conjunt parcialment ordenat**. *Anàlogament, un conjunt amb un ordre total és un* **conjunt totalment ordenat**.

Els conjunts finits parcialment o totalment ordenats tenen la característica que poden ser representats mitjançant grafs amb vèrtexs que representen els elements i línies que s'estenen cap amunt per indicar l'ordre entre elements consecutius. Aquest diagrama s'anomena *diagrama de Hasse*. Estudiem els següents exemples.

EXEMPLE 2.4. *Siga A un conjunt no buit, aleshores $(\mathcal{P}(A), \subseteq)$ és un conjunt parcialment ordenat.*

En primer lloc, és clar que compleix la propietat transitiva perquè si $B \in \mathcal{P}(A)$, es té $B \subseteq B$. A més, siguen $B_1, B_2 \in \mathcal{P}(A)$ tals que $B_1 \subseteq B_2$ i $B_2 \subseteq B_1$, aleshores $B_1 = B_2$. Per tant, es compleix la propietat antisimètrica. Per últim, siguen $B_1, B_2, B_3 \in \mathcal{P}(A)$ tals que $B_1 \subseteq B_2$ i $B_2 \subseteq B_3$ aleshores $B_1 \subseteq B_3$, complint així la propietat transitiva.

Si considerem $A = \{0, 1, 2\}$, podem estudiar aquesta relació d'orde en un cas més concret. El conjunt de les parts d'A és

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, A\}.$$

Tenint en compte que es tracta d'un conjunt parcialment ordenat, tenim el diagrama de Hasse que es mostra a la Figura 1.1.

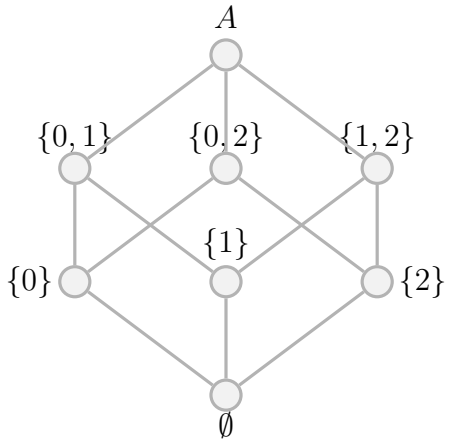

FIGURA 1.1. Diagrama de Hasse de $\big(\mathcal{P}(A), \subseteq\big)$.

EXEMPLE 2.5. *Considerem el conjunt de nombres naturals $\mathbb{N}$. La relació de ser divisible és un ordre parcial en $\mathbb{N}$.*

Notem que se satisfà la propietat reflexiva, ja que si $n \in \mathbb{N}$*, és clar que* $n|n$*.*

Així mateix es compleix la propietat antisimètrica perquè si $n, m \in \mathbb{N}$ *són tals que* $n|m$ *i* $m|n$*, aleshores* $m = k_1 n$ *i* $n = k_2 m$ *amb* $k_1, k_2 \in \mathbb{N}$*. Per tant* $m = (k_1 k_2)m$*, però, això és cert si, i només si,* $k_1 = k_2 = 1$*, és a dir, si* $n = m$*.*

Finalment, siguen $n, m, p \in A$ *tals que* $n|m$ *i* $m|p$*, aleshores* $m = k_1 n$ *i* $p = k_2 m$ *amb* $k_1, k_2 \in \mathbb{N}$*. Per tant* $p = k_2 m = k_2 k_1 n$*, i així* $n|p$*.*

Dins dels conjunts parcialment ordenats, definirem ara uns elements bàsics d'aquests.

DEFINICIÓ 2.6. *Siga* A *un subconjunt d'un conjunt parcialment ordenat* $\big(P, \leq\big)$ *i siga* $p \in P$*. Direm que* p *és* **fita superior d'***A si* $a \leq p$*, per a tot* $a \in A$*. A més, direm que* p *és* **suprem d'***A si* p *és la menor de les fites superiors, és a dir, si* p *és fita superior i per a tot* b *tal que* $a \leq b$*, per a tot* $a \in A$*, aleshores* $p \leq b$*. Anàlogament, direm que* p *és* **fita inferior d'***A si* $p \leq a$*, per a tot* $a \in A$*. A més, direm que* p *és* **ínfim d'***A si* p *és la major de les fites inferiors, és a dir, si* p *és fita inferior i per a tot* b *tal que* $b \leq a$*, per a tot* $a \in A$*, aleshores* $b \leq p$*.*

Una volta definits aquests conceptes, podem formalitzar la segona definició de reticle.

DEFINICIÓ 2.7. *Un conjunt parcialment ordenat* $(L, \leq)$ *s'anomena* **reticle** *si per a tot* $a, b \in L$ *el suprem i l'ínfim dels elements* a *i* b*, denotats respectivament com* $\sup\{a, b\}$ *i* $\inf\{a, b\}$*, existeixen en* L*.*

A continuació provarem que les dues definicions són equivalents i, per consegüent, determinen la mateixa idea des de dos punts de vista diferents, un algebraic i un altre geomètric.

PROPOSICIÓ 2.8. *Les definicions de reticle 2.1 i 2.7 són equivalents.*

DEMOSTRACIÓ. Siga L un reticle segons la Definició 2.1, és a dir, un conjunt no buit L amb dues operacions $\wedge, \vee$ definides tals que satisfan (R1), (R2), (R3) i (R4).

Siguen $x, y \in L$, definim la relació d'ordre donada per $x \leq y$ si, i només si, $x = x \wedge y$, (o equivalentment $y = x \vee y$). Vegem que $(L, \leq)$ és reticle seguint la Definició 2.7.

En primer lloc, comprovem que defineix un ordre parcial en L, o dit en altres paraules, que satisfà la propietat reflexiva, antisimètrica i transitiva

Notem que per a tot $x \in L$, per (R3), $x = x \wedge x$. Per tant, $x \leq x$.

A més, siguen $x, y \in L$ tals que $x \leq y$ i $y \leq x$, aleshores, respectivament, $x = x \wedge y$ i $y = y \wedge x$. Per tant,

$$\begin{aligned} x &= x \wedge y \\ &= y \wedge x && \text{(per (R1))} \\ &= y. \end{aligned}$$

Finalment, siguen $x, y, z \in L$ tals que $x \leq y$ i $y \leq z$, aleshores, $x = x \wedge y$ i $y = y \wedge z$. Així,

$$\begin{aligned} x \wedge z &= (x \wedge y) \wedge z \\ &= x \wedge (y \wedge z) && \text{(per (R2))} \\ &= x \wedge y \\ &= x. \end{aligned}$$

Per tant, $x \leq z$.

Anem a vore ara que, per a tot $a, b \in L$, el suprem i l'ínfim d'a i b existeixen en L.

D'una banda, per (R4) sabem que $a = a \wedge (a \vee b)$ i $b = b \wedge (b \vee a)$, i equivalentment, tenint en compte com hem definit la relació d'ordre, $a \leq a \vee b$ i $b \leq a \vee b$.

D'altra banda, siga $u \in L$ tal que $a \leq u$ i $b \leq u$.

Notem $a \vee u = (a \wedge u) \vee u = u$ i $b \vee u = (b \wedge u) \vee u = u$. Així,

$$\begin{aligned} u &= u \vee u \\ &= (a \vee u) \vee (b \vee u) \\ &= a \vee (u \vee b) \vee u && \text{(per (R2))} \\ &= a \vee (b \vee u) \vee u && \text{(per (R1))} \\ &= (a \vee b) \vee (u \vee u) && \text{(per (R2))} \\ &= (a \vee b) \vee u. && \text{(per (R3))} \end{aligned}$$

Per tant,

$$\begin{aligned} (a \vee b) \wedge u &= (a \vee b) \wedge [(a \vee b) \vee u] && \text{(per (R4))} \\ &= a \vee b. \end{aligned}$$

És a dir, $a \vee b \leq u$.

Concloem que $a \vee b$ és la menor de les fites superiors d'a i b, és a dir $a \vee b = \sup\{a, b\} \in L$. Treballant de forma anàloga amb l'ínfim, arribem al fet que $a \wedge b = \inf\{a, b\} \in L$.

Suposem ara que L és un conjunt parcialment ordenat $(L, \leq)$ tal que per a tot $a, b \in L$ el suprem i l'ínfim d'a i b existeixen en L. Dit d'una altra manera, L és un reticle segons la Definició 2.7.

Siguen $a, b \in L$, definim $a \vee b = \sup\{a, b\}$ i $a \wedge b = \inf\{a, b\}$. Anem a comprovar que satisfà les propietats de la Definició 2.1.

En primer lloc, siguen $x, y \in L$ notem que

$$x \vee y = \sup\{x, y\} = \sup\{y, x\} = y \vee x;$$
$$x \wedge y = \inf\{x, y\} = \inf\{y, x\} = y \wedge x.$$

Per tant, se satisfà la propietat commutativa.

A més, siguen $x, y, z \in L$, d'una banda

$$\begin{aligned}(x \vee y) \vee z &= \sup\{\sup\{x, y\}, z\} \\ &= \sup\{x, y, z\} \\ &= \sup\{x, \sup\{y, z\}\} \\ &= x \vee (y \vee z).\end{aligned}$$

D'altra banda,

$$\begin{aligned}(x \wedge y) \wedge z &= \inf\{\inf\{x, y\}, z\} \\ &= \inf\{x, y, z\} \\ &= \inf\{x, \inf\{y, z\}\} \\ &= x \wedge (y \wedge z).\end{aligned}$$

Concloem que les operacions $\wedge$ i $\vee$ satisfan la propietat associativa.

Així mateix, siga $x \in L$ notem que

$$x \vee x = \sup\{x, x\} = x;$$
$$x \wedge x = \inf\{x, x\} = x.$$

Per tant, es compleixen les lleis d'identitat.

Per últim, siguen $x, y \in L$, notem que se satisfan les lleis d'absorció, ja que

$$x \vee (x \wedge y) = \sup\{x, \inf\{x, y\}\} = x, \text{ perquè } \inf\{x, y\} \leq x;$$
$$x \wedge (x \vee y) = \inf\{x, \sup\{x, y\}\} = x, \text{ perquè } \sup\{x, y\} \geq x.$$

Açò conclou la demostració de la Proposició 2.8 . □

2. Reticles Isomorfs i Subreticles

La paraula isomorfisme sol usar-se per a expressar que dues estructures són iguals excepte per la natura dels seus elements. En aquest capítol veurem què vol dir que dos reticles siguen isomorfs.

Definició 2.9. *Dos reticles L_1, L_2 són* **isomorfs** *si existeix una bijecció $f : L_1 \longrightarrow L_2$ tal que per a tot $a, b \in L_1$ es cumpleix:*

$$f(a \wedge_1 b) = f(a) \wedge_2 f(b); \qquad f(a \vee_1 b) = f(a) \vee_2 f(b).$$

En aquest cas, f s'anomena **isomorfisme**.

Recordem que si f és un isomorfisme, f^{-1} també ho és. A més, la composició d'isomorfismes és un isomorfisme, i l'aplicació identitat per a un reticle també.

En conjunts parcialment ordenats, és natural abordar la idea d'aplicacions que mantenen l'ordre. Així, trobarem una caracterització dels isomorfismes entre reticles mitjançant aplicacions que preserven l'ordre o, també dites monòtones.

DEFINICIÓ 2.10. *Siguen $(P_1, \leq_1), (P_2, \leq_2)$ conjunts parcialment ordenats. L'aplicació $f : P_1 \longrightarrow P_2$ es diu* **monòtona** *si, per a tot $x, y \in P_1$ tals que $x \leq_1 y$, aleshores $f(x) \leq_2 f(y)$.*

Així, podem reformular la definició d'isomorfisme considerant les relacions d'ordre com segueix.

TEOREMA 2.11. *Siguen L_1, L_2 dos reticles. Les següents afirmacions són equivalents:*

(1) *L_1, L_2 són isomorfs.*
(2) *Existeix $f : L_1 \longrightarrow L_2$ bijectiva, monòtona i d'inversa monòtona.*

DEMOSTRACIÓ. En primer lloc, si suposem que L_1 i L_2 són isomorfs, aleshores existeix $f : L_1 \longrightarrow L_2$ bijectiva tal que

$$f(x \wedge_1 y) = f(x) \wedge_2 f(y); \qquad f(x \vee_1 y) = f(x) \vee_2 f(y).$$

Com que ja tenim que és bijectiva, vegem que és monòtona i d'inversa monòtona.

Siguen $x, y \in L_1$ tals que $x \leq_1 y$, aleshores $x = x \wedge_1 y$. Així, $f(x) = f(x \wedge_1 y) = f(x) \wedge_2 f(y)$; és a dir, $f(x) \leq_2 f(y)$ i per tant, f és monòtona.

A més, com que és isomorfisme, sabem que existeix f^{-1}, aplicació inversa de f, que també és isomorfisme i per tant satisfà

$$f^{-1}(x \wedge_1 y) = f^{-1}(x) \wedge_2 f^{-1}(y); \quad f^{-1}(x \vee_1 y) = f^{-1}(x) \vee_2 f^{-1}(y).$$

Anem a vore que l'inversa és monòtona.

Siguen $x, y \in L_2$ tals que $x \leq_2 y$, aleshores $x = x \wedge_2 y$. Per tant, $f^{-1}(x) = f^{-1}(x \wedge_2 y) = f^{-1}(x) \wedge_1 f^{-1}(y)$, és a dir $f^{-1}(x) \leq_2 f^{-1}(y)$ i així, f^{-1} és monòtona.

Suposem ara que existeix $f : L_1 \longrightarrow L_2$ bijectiva, monòtona i d'inversa monòtona. Volem demostrar que és isomorfisme.

Primer anem a provar $f(x \wedge_1 y) = f(x) \wedge_2 f(y)$.

Notem $x \wedge_1 (x \wedge_1 y) = (x \wedge_1 x) \wedge_1 y = x \wedge_1 y$. Per tant, $x \wedge_1 y \leq_1 x$ i, com que f és monòtona, $f(x \wedge_1 y) \leq_2 f(x)$.

Anàlogament, $y \wedge_1 (y \wedge_1 x) = (y \wedge_1 y) \wedge_1 x = y \wedge_1 x$, és a dir, $x \wedge_1 y \leq_1 y$ i, com f és monòtona, $f(x \wedge_1 y) \leq_2 f(y)$.

Com que l'ínfim ha de ser la major de les fites inferiors, tenim que

$$f(x \wedge_1 y) \leq_2 f(x) \wedge_2 f(y).$$

D'altra banda, siga $z \in L_2$ tal que $z \leq_2 f(x)$ i $z \leq_2 f(y)$, com que f és bijectiva, en particular és sobrejectiva i per tant, existeix $a \in L_1$ tal que $f(a) = z$. Per tant, $f(a) \leq_2 f(x)$ i $f(a) \leq_2 f(y)$. Com f^{-1} és monòtona, tenim que $a \leq_1 x$ i $a \leq_1 y$ i, per tant, $a \leq_1 x \wedge_1 y$. Així, $f(a) = z \leq_2 f(x \wedge_1 y)$. En particular, si considerem $z = f(x) \wedge_2 f(y)$, tindrem $f(x) \wedge_2 f(y) \leq_2 f(x \wedge_1 y)$. Per tant,

$$f(x) \wedge_2 f(y) = f(x \wedge_1 y).$$

De forma anàloga amb el suprem arribem a què

$$f(x) \vee_2 f(y) = f(x \vee_1 y).$$

Concloem per tant que f és un isomorfisme i, en conseqüència, L_1 i L_2 són isomorfs. □

Com és habitual quan treballem amb estructures algebraiques, anem a vore la definició de la subestructura dels reticles, els subreticles.

Definició 2.12. *Siga L un reticle i L' un subconjunt de L diferent del buit, direm L' és un* **subreticle de** *L si, per a tot $a, b \in L'$,*

$$a \wedge b \in L'; \qquad a \vee b \in L',$$

amb $\wedge$ i $\vee$ les operacions de reticle de L.

És a dir, siguen $a, b \in L'$, direm que $a \leq b$ en L' si, i només si, $a \leq b$ en L. Per tant, L' és un subreticle de L si és un reticle amb les operacions de L restringides a L'.

Definició 2.13. *Direm que un reticle L_1 està* **contingut** *en un reticle L_2 si existeix un subreticle de L_2 isomorf a L_1. En aquest cas direm que L_2 conté una còpia de L_1 com a subreticle.*

3. Reticles Distributius i Modulars

Els tipus de reticles més importants són els reticles modulars i els distributius. En aquest capítol, començarem definint aquests dos tipus de reticles.

Definició 2.14. *Un reticle L es diu* **distributiu** *si satisfà alguna de les següents condicions. Per a tot $x, y, z \in L$,*

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \tag{D1}$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z). \tag{D2}$$

PROPOSICIÓ 2.15. *Per a qualsevol reticle L sempre es té que, per a tot $x, y, z \in L$,*

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

DEMOSTRACIÓ. Com $x \wedge y \leq x$ i $x \wedge z \leq x$, aleshores

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

A més $x \wedge y \leq y \leq y \vee z$ i $x \wedge z \leq z \leq y \vee z$. Així,

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

Per tant, $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. □

Notem que, per provar que un reticle és distributiu només serà necessari demanar una de les dues condicions, ja que aquestes són equivalents.

PROPOSICIÓ 2.16. *En referència a la Definició 2.14, un reticle L satisfà (D1) si, i només si, satisfà (D2).*

DEMOSTRACIÓ. En primer lloc, suposem L satisfà (D1). Aleshores, siguen $x, y, z \in L$ tenim que

$$\begin{aligned}
x \vee (y \wedge z) &= (x \vee (x \wedge z)) \vee (y \wedge z) && \text{(per (R4))} \\
&= x \vee \big((x \wedge z) \vee (y \wedge z)\big) && \text{(per (R2))} \\
&= x \vee \big((z \wedge x) \vee (z \wedge y)\big) && \text{(per (R1))} \\
&= x \vee \big(z \wedge (x \vee y)\big) && \text{(per (D1))} \\
&= x \vee \big((x \vee y) \wedge z\big) && \text{(per (R1))} \\
&= \big(x \wedge (x \vee y)\big) \vee \big((x \vee y) \wedge z\big) && \text{(per (R4))} \\
&= \big((x \vee y) \wedge x\big) \vee \big((x \vee y) \wedge z\big) && \text{(per (R1))} \\
&= (x \vee y) \wedge (x \vee z). && \text{(per (D1))}
\end{aligned}$$

És a dir, se satisfà (D2).
Suposem ara que es compleix (D2).

Per la Proposició 2.15 sabem que $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. Notem que

$$\begin{aligned}
(x \wedge y) \vee (x \wedge z) &= \big((x \wedge y) \vee x\big) \wedge \big((x \wedge y) \vee z\big) && \text{(per (D2))}\\
&= x \wedge \big((x \wedge y) \vee z\big) && \text{(per (R4))}\\
&= x \wedge \big(z \vee (x \wedge y)\big) && \text{(per (R1))}\\
&= x \wedge \big((z \vee x) \wedge (z \vee y)\big) && \text{(per (D2))}\\
&= \big(x \wedge (z \vee z)\big) \wedge (z \vee y) && \text{(per (R2))}\\
&= x \wedge (z \vee y). && \text{(per (R4))}
\end{aligned}$$

Concloem per tant que les afirmacions (D1) i (D2) són equivalents. □

Treballem ara de forma anàloga amb els reticles modulars

Definició 2.17. *Un reticle L és* **modular** *si satisfà una de les següents condicions. Per a tot $x, y, z \in L$,*

$$\text{Si } x \leq y, \text{ aleshores } x \vee (y \wedge z) = y \wedge (x \vee z). \tag{M1}$$

$$(x \wedge y) \vee (y \wedge z) = y \wedge \big((x \wedge y) \vee z\big). \tag{M2}$$

Proposició 2.18. *En referència a la Definició 2.17, un reticle L satisfà (M1) si, i només si, satisfà (M2).*

Demostració. Suposem que es compleix la propietat (M1) de la Definició 2.17. Com $x \wedge y \leq y$, aleshores $(x \wedge y) \vee (y \wedge z) = y \wedge \big((x \wedge y) \vee z\big)$.

Suposem ara que (M2) és cert. Siguen x, y amb $x \leq y$, aleshores

$$\begin{aligned}
x \vee (y \wedge z) &= (x \wedge y) \vee (y \wedge z) && \text{(perquè } x = x \wedge y)\\
&= y \wedge \big((x \wedge y) \vee z\big) && \text{(per (M2))}\\
&= y \wedge (x \vee z). && \text{(perquè } x = x \wedge y)
\end{aligned}$$

Açò demostra la Proposició 2.18. □

Proposició 2.19. *En un reticle L, si $x, y, z \in L$ i $x \leq y$, aleshores sempre es té que $x \vee (y \wedge z) \leq y \wedge (x \vee z)$.*

Demostració. Per una part, com que $x \leq y$, tenim que $x \vee y = y$ i així

$$\begin{aligned}
\big(x \vee (y \wedge z)\big) \vee y &= x \vee \big((y \wedge z) \vee y\big) && \text{(per (R2))}\\
&= x \vee y && \text{(per (R4))}\\
&= y.
\end{aligned}$$

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

D'altra banda,

$$\begin{aligned}
\big(x \vee (y \wedge z)\big) \vee (x \vee z) &= x \vee \big((y \wedge z) \vee (x \vee z)\big) && \text{(per (R2))}\\
&= x \vee \big((y \wedge z) \vee (z \vee x)\big) && \text{(per (R1))}\\
&= x \vee \Big(\big((y \wedge z) \vee z\big) \vee x)\Big) && \text{(per (R2))}\\
&= x \vee (z \vee x) && \text{(per (R4))}\\
&= x \vee z.
\end{aligned}$$

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

Com l'ínfim ha de ser la major de les fites inferiors, es compleix que $x \vee (y \wedge z) \leq y \wedge (x \vee z)$. □

El pròxim objectiu serà mostrar una manera d'identificar els reticles distributius i modulars. Però abans de fer-ho, hem de demostrar el següent resultat.

Teorema 2.20. *Tot reticle distributiu és modular.*

Demostració. Siga L un reticle distributiu, aleshores sabem que satisfà qualsevol de les següents afirmacions equivalents

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z); \tag{D1}$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z). \tag{D2}$$

A més, per la Proposició (2.19), sabem que si $x \leq y$ aleshores

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

Així, per demostrar que L és un reticle modular basta provar l'altra desigualtat. Siguen $x, y, z \in L$ tals que $x \leq y$, aleshores

$$\begin{aligned}
y \wedge (x \vee z) &= (y \vee z) \wedge (x \vee z) && \text{(perquè } y = x \vee y)\\
&= x \vee (y \wedge z). && \text{(per (D2))}
\end{aligned}$$

Açò demostra el Teorema 2.20. □

A continuació, presentarem dos reticles, M_5 i N_5 que ens permetran arribar a una caracterització sobre reticles modulars i distributius en termes d'aquestes dues estructures ordenades.

Definició 2.21. *El reticle M_5, representat a la Figura 3.1, és un reticle modular no distributiu.*

M_5 no és distributiu perquè $a \vee (b \wedge c) = a \vee d = a$, però $(a \vee b) \wedge (a \vee c) = e \wedge e = e$.

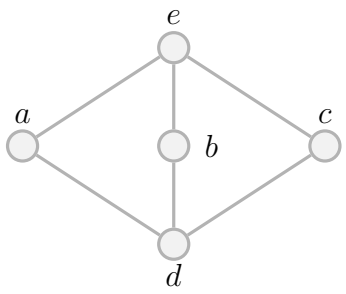

FIGURA 3.1. Reticle M_5.

No obstant això, vegem que es tracta d'un reticle modular, ja que per a tota parella d'elements x, y en M_5 tals que $x \leq y$ sempre es té que

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

En efecte, si agafem els elements a i d amb $d \leq a$, notem que

$$d \vee (a \wedge b) = d \vee d = d \text{ i } a \wedge (d \vee b) = a \wedge b = d;$$
$$d \vee (a \wedge c) = d \vee d = d \text{ i } a \wedge (d \vee c) = a \wedge c = d;$$
$$d \vee (a \wedge e) = d \vee a = a \text{ i } a \wedge (d \vee e) = a \wedge e = a.$$

La prova amb d i b o amb d i b és anàloga.

Si considerem ara els elements a i e amb $a \leq e$, notem que

$$a \vee (e \wedge b) = a \vee b = e \text{ i } e \wedge (a \vee b) = e \wedge e = e;$$
$$a \vee (e \wedge c) = a \vee c = e \text{ i } e \wedge (a \vee c) = e \wedge e = e;$$
$$a \vee (e \wedge d) = a \vee d = a \text{ i } e \wedge (a \vee d) = e \wedge a = a.$$

La prova amb e i b o amb e i b és anàloga.

Només queda comprovar amb d i e, amb $d \leq e$.

$$d \vee (e \wedge a) = d \vee a = a \text{ i } e \wedge (d \vee a) = e \wedge a = a;$$
$$d \vee (e \wedge b) = d \vee b = b \text{ i } e \wedge (d \vee b) = e \wedge b = b;$$
$$d \vee (e \wedge c) = d \vee c = c \text{ i } e \wedge (d \vee c) = e \wedge c = c.$$

DEFINICIÓ 2.22. *El reticle N_5, representat a la Figura 3.2, és un reticle no modular no distributiu.*

N_5 no és distributiu perquè $a \vee (b \wedge c) = a \vee d = a$, però $(a \vee b) \wedge (a \vee c) = b \wedge e = b$.

N_5 no és modular perquè $a \leq b$, però

$$a \vee (b \wedge c) = a \vee d = a \text{ i } b \wedge (a \vee c) = b \wedge e = b.$$

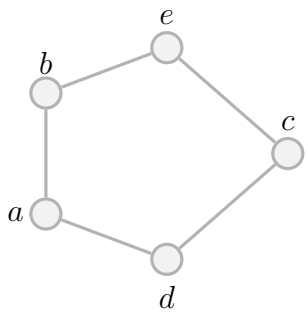

FIGURA 3.2. Reticle N_5.

En aquest punt, anem a vore dos teoremes que ens permeten identificar quan un reticle no és modular o no és distributiu.

TEOREMA 2.23 (Dedekind). *L és un reticle no modular si, i només si, N_5 està contingut en L, és a dir, si existeix una còpia de N_5 en L.*

DEMOSTRACIÓ. En primer lloc, suposem que existeix una còpia de N_5 en L. Per la definició de N_5, com que no és modular, existeixen $a, b, c \in L$, amb $a \leq b$ tals que

$$a \vee (b \wedge c) \neq b \wedge (a \vee c).$$

És a dir, L no és modular.

Suposem ara que L no és modular. Així existeixen $a, b, c \in L$ tals que $a \leq b$, però $a \vee (b \wedge c) < b \wedge (a \vee c)$; és a dir, no es compleix que

$$b \wedge (a \vee c) \leq a \vee (b \wedge c),$$

ja que l'altra desigualtat és sempre certa com hem vist a la Proposició 2.19.

Considerem $a_1 = a \vee (b \wedge c)$ i $b_1 = b \wedge (a \vee c)$. Emprant la definició de b_1 i les propietats de reticles (R1), (R2) i (R4) tenim que

$$\begin{aligned} c \wedge b_1 &= c \wedge \big(b \wedge (a \vee c)\big) && \text{(per } b_1\text{)} \\ &= c \wedge \big((a \vee c) \wedge b\big) && \text{(per (R1))} \\ &= \big(c \wedge (a \vee c)\big) \wedge b && \text{(per (R2))} \\ &= c \wedge b. && \text{(per (R4))} \end{aligned}$$

Mitjançant un raonament similar amb a_1 tenim que

$$\begin{aligned} c \vee a_1 &= c \vee \big(a \vee (b \wedge c)\big) && (\text{per } a_1) \\ &= c \vee \big((c \wedge b) \vee a\big) && (\text{per (R1)}) \\ &= \big(c \vee (c \wedge b)\big) \vee a && (\text{per (R2)}) \\ &= c \vee a. && (\text{per (R4)}) \end{aligned}$$

A més, notem que $b \wedge c \leq a \vee (b \wedge c) = a_1$ i

$$a_1 = a \vee (b \wedge c) < b \wedge (a \vee c) = b_1.$$

Per tant,

$$b \wedge c \leq a_1 < b_1. \tag{1}$$

Així, $c \wedge b \leq c \wedge a_1 \leq c \wedge b_1 = c \wedge b$. Per tant

$$c \wedge b = c \wedge a_1 = c \wedge b_1. \tag{2}$$

De forma anàloga, com que

$$a_1 < b_1 \leq c \vee a, \tag{3}$$

arribem a que

$$c \vee b_1 = c \vee a_1 = c \vee a \tag{4}$$

Tenint en compte (1), (2), (3) i (4), observem que aquestes relacions donen lloc al diagrama de la Figura 3.3. És a dir, existeix en L una còpia de N_5. □

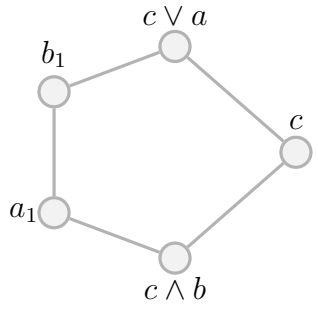

FIGURA 3.3. Còpia de N_5 en el Teorema 2.23.

Presentem ara un resultat similar per al cas dels reticles no distributius.

TEOREMA 2.24 (Birkhoff). *L és un reticle no distributiu si, i només si, L conté una còpia de N_5 o de M_5.*

DEMOSTRACIÓ. En primer lloc, suposen que L conté una còpia de N_5 o de M_5. Com que es tracta de reticles no distributius, en qualsevol cas existeixen $a, b, c \in L$ tals que

$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c).$$

Per tant, L no és distributiu.

Suposem ara que L no és distributiu i que no conté una còpia de N_5 com a subreticle. Així, pel Teorema 2.23, L serà modular. Com que L no és distributiu, tenint en compte la Proposició 2.15, existiran $a, b, c \in L$ tals que

$$(a \wedge b) \vee (a \wedge c) < a \wedge (b \vee c).$$

Definim en el reticle els següents punts.

$$\begin{array}{ll} d = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c), & a_1 = (a \wedge e) \vee d, \\ e = (a \vee b) \wedge (a \vee c) \wedge (b \vee c), & b_1 = (b \wedge e) \vee d, \\ & c_1 = (c \wedge e) \vee d. \end{array}$$

Per construcció, $d \leq a_1, b_1, c_1 \leq e$ i $d \leq e$.

Ara, notem que

$$\begin{aligned} a \wedge e &= a \wedge \big((a \vee b) \wedge (a \vee c) \wedge (b \vee c)\big) && \text{(per } e\text{)} \\ &= \Big(\big(a \wedge (a \vee b)\big) \wedge (a \vee c)\Big) \wedge (b \vee c) && \text{(per (R2))} \\ &= \big(a \wedge (a \vee c)\big) \wedge (b \vee c) && \text{(per (R4))} \\ &= a \wedge (b \vee c). && \text{(per (R4))} \end{aligned}$$

I també

$$\begin{aligned} a \wedge d &= a \wedge \big((a \wedge b) \vee (a \wedge c) \vee (b \wedge c)\big) && \text{(per } d\text{)} \\ &= \big((a \wedge b) \vee (a \wedge c)\big) \vee \big(a \wedge (b \wedge c)\big) && \text{(per la definició de } \wedge\text{)} \\ &= \big(a \wedge (b \wedge a) \vee c\big) \vee \big(a \wedge (b \wedge c)\big) && \text{(per (M2))} \\ &= a \wedge \Big(\big((b \wedge a) \vee c\big) \vee (b \wedge c)\Big) && \text{(per (R2) i (R4))} \\ &= a \wedge \big((b \wedge a) \vee c\big) && \text{(per la definició de } \vee\text{)} \\ &= (b \wedge a) \vee (a \wedge c). && \text{(per (M2))} \end{aligned}$$

Per tant, $d < e$.

Per últim, demostrarem que

$$\begin{aligned} a_1 \wedge b_1 = a_1 \wedge c_1 = b_1 \wedge c_1 = d, \\ a_1 \vee b_1 = a_1 \vee c_1 = b_1 \vee c_1 = e. \end{aligned}$$

Ho provarem només per a $a_1 \wedge b_1$, però els raonaments en la resta de casos són similars.

$$\begin{aligned}
a_1 \wedge b_1 &= \big((a \wedge e) \vee d\big) \wedge \big((b \wedge e) \vee d\big) && \text{(per } a_1 \text{ i } b_1\text{)} \\
&= \Big((a \wedge e) \wedge \big((b \wedge e) \vee d\big)\Big) \vee d && \text{(per (M2))} \\
&= \Big((a \wedge e) \wedge \big((b \vee d) \wedge e\big)\Big) \vee d && \text{(per (M2))} \\
&= \big((a \wedge e) \wedge e \wedge (b \vee d)\big) \vee d && \text{(per (R2))} \\
&= \big((a \wedge e) \wedge (b \vee d)\big) \vee d && \text{(per (R3))} \\
&= \big(a \wedge (b \vee c) \wedge (b \vee (a \wedge c))\big) \vee d && \text{(per (R4))} \\
&= \Big(a \wedge \big(b \vee ((b \vee c) \wedge (a \wedge c))\big)\Big) \vee d && \text{(per (M2))} \\
&= \Big(a \wedge \big(b \vee (a \wedge c)\big)\Big) \vee d && \text{(per (R4))} \\
&= (a \wedge c) \vee (b \wedge a) \vee d && \text{(per (M2))} \\
&= d. && \text{(per } d\text{)}
\end{aligned}$$

Així, es té que a_1, b_1, c_1, d, i e formen una còpia de M_5 com es mostra a la Figura 3.4. Açò conclou la demostració del Teorema 2.24. □

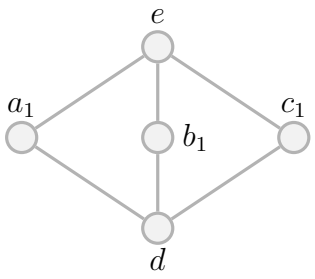

FIGURA 3.4. Còpia de M_5 en el Teorema 2.24.

4. Reticles Complets, Reticles Algebraics i Relacions d'Equivalència

En aquesta secció introduirem la noció de reticle complet, així com la noció de reticle algebraic. Després treballarem amb les relacions d'equivalència, amb l'objectiu de demostrar que es tracta d'un reticle complet. En el capítol següent veurem que algunes de les estructures més importants de les àlgebres són reticles complets i algebraics.

DEFINICIÓ 2.25. *Un conjunt parcialment ordenat $(P, \leq)$ es diu* **complet** *si per a tot subconjunt $A \subseteq P$ es té que existeixen en P tant el suprem com l'ínfim d'A. El suprem d'A es denota per $\bigvee A$ i l'ínfim per $\bigwedge A$.*

Notem que tot conjunt parcialment ordenat complet és un reticle, i un reticle que és complet com a conjunt parcialment ordenat és un reticle complet. Per tant, és natural tindre el teorema següent.

TEOREMA 2.26. *Siga $(P, \leq)$ un conjunt parcialment ordenat tal que per a tot $A \subseteq P$ existeix el suprem o l'ínfim d'A, aleshores P és un reticle complet.*

DEMOSTRACIÓ. Suposem, per hipòtesi, que els ínfims arbitraris existeixen. Així, siga $A \subseteq P$, notem que

$$\bigwedge \{z \mid \forall a \in A, (a \leq z)\} = \bigvee A.$$

De forma anàloga, si suposem que els suprems arbitraris existeixen,

$$\bigvee \{z \mid \forall a \in A, (z \leq a)\} = \bigwedge A.$$

Açò conclou la demostració del Teorema 2.26. □

NOTA 2.27. *Notem que, per la definició de reticle complet, basta demanar una de les dues condicions del Teorema 2.26.*

NOTA 2.28. *El resultat del Teorema 2.26 destaca especialment en el conjunt buit $\emptyset$. L'existència de l'ínfim de $\emptyset$ garanteix l'existència de la menor de les fites superiors, és a dir, d'un màxim global. Per tant, $\bigwedge \emptyset = 1$. Anàlogament, arribem al fet que $\bigvee \emptyset = 0$, és a dir, existeix un mínim global.*

DEFINICIÓ 2.29. *Un subreticle L' d'un reticle complet L es diu* **subreticle complet** *de L si, per a tot $A \subseteq L'$, els elements $\bigvee A$ i $\bigwedge A$, definits en L, estan en L'.*

A continuació, després de definir les nocions d'element compacte i de compactament generat, determinarem què és un reticle algebraic.

DEFINICIÓ 2.30. *Siga L un reticle, direm que un element $a \in L$ és* **compacte** *si, per a tot $A \subseteq L$ per al què $\bigvee A$ està definit, si es té que $a \leq \bigvee A$, aleshores existeix un $B \subseteq A$ amb B finit tal que $a \leq \bigvee B$. Direm que L és* **compactament generat** *si tot element en L és el suprem d'elements compactes. Un reticle L es diu* **algebraic** *si és complet i compactament generat.*

4.1. El reticle complet $\mathrm{Eqv}(A)$**.** Una volta vists aquests conceptes, l'objectiu principal serà estudiar el reticle de les relacions d'equivalència. Per a fer-ho, començaren recordant què és una relació binària i estudiarem les característiques per les quals podem considerar el conjunt de les relacions d'equivalència com un reticle.

DEFINICIÓ 2.31. *Siga A un conjunt, una* **relació binària** *R en A és un subconjunt d'$A\times A$. Siguen $a,\ b \in A$, escriurem aRb si $(a,b) \in R$.*

Notem que si $R,\ S$ són relacions binàries en A,

$$R \circ S = \{(a,c) \in A \times A \mid \exists b \in A,\ (\ (a,b) \in R\ \wedge\ (b,c) \in S)\}$$

és una relació binària. Recursivament, es pot definir

$$R_1 \circ R_2 \circ \cdots \circ R_n = (R_1 \circ R_2 \circ \cdots \circ R_{n-1}) \circ R_n.$$

A més, donada una relació binària R, es defineix la relació inversa de R com

$$R^{-1} = \{(b,a) \in A \times A \ \mid\ (a,b) \in R\}.$$

Per últim, cal destacar dues relacions binàries que es troben en qualsevol conjunt, la relació diagonal Δ_A, definida per

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

i la relació total, definida per

$$\nabla_A = A \times A.$$

DEFINICIÓ 2.32. *Una relació binària R en A és una* **relació d'equivalència** *si satisfà que, per a tot $a,b,c \in A$,*
Propietat reflexiva

$$aRa. \tag{E1}$$

Propietat simètrica

$$\textit{Si } aRb,\ \textit{aleshores } bRa. \tag{E2}$$

Propietat transitiva

$$\textit{Si } aRb \textit{ i } bRc,\ \textit{aleshores } aRc. \tag{E3}$$

Anomenem $\mathrm{Eqv}(A)$ *al conjunt de totes les relacions d'equivalència en el conjunt A.*

DEFINICIÓ 2.33. *Siga $R \in \mathrm{Eqv}(A)$, $a \in A$, la* **classe d'equivalència d'**a **respecte d'**R *és el conjunt*

$$[a]_R = \{b \in A \mid (b,a) \in R\}.$$

Així, es defineix el **conjunt quocient** *com* $A/R = \{[a]_R \mid a \in A\}$.

PROPOSICIÓ 2.34. *Siga A un conjunt, $\big(\mathrm{Eqv}(A), \subseteq\big)$ és un conjunt parcialment ordenat.*

DEMOSTRACIÓ. En primer lloc, com les relacions diagonal i total sempre existeixen, el conjunt $\mathrm{Eqv}(A)$ és no buit.

Demostrem ara que $\subseteq$ defineix una relació d'ordre en $\mathrm{Eqv}(A)$.

Trivialment, per a tot $R \in \mathrm{Eqv}(A)$ es té que $R \subseteq R$, satisfent la propietat reflexiva. A més es compleix la propietat antisimètrica, ja que per a totes les relacions $R, S \in \mathrm{Eqv}(A)$ tals que $R \subseteq S$ i $S \subseteq R$, aleshores $R = S$. Per últim, per a tot $R, S, T \in \mathrm{Eqv}(A)$ tals que $R \subseteq S$ i $S \subseteq T$, es té que $R \subseteq T$.

Açò demostra la Proposició 2.34. □

NOTA 2.35. *Notem que la relació diagonal Δ_A relaciona cada element únicament amb ell mateix. Així, per a tota relació d'equivalència R definida en A, tindrem que $\Delta_A \subseteq R$ perquè R ha de satisfer la propietat reflexiva. Per tant, Δ_A és la menor relació d'equivalència que podem trobar en un conjunt.*

D'altra banda, la relació total ∇_A, és la relació d'equivalència més gran que trobem en un conjunt, ja que per a tota relació d'equivalència R definida en A, és clar que $R \subseteq \nabla_A$.

En aquest punt, estudiarem el suprem i l'ínfim de les relacions d'equivalència sobre un conjunt A, per tal de demostrar que $\big(\mathrm{Eqv}(A), \subseteq\big)$ és un reticle complet.

PROPOSICIÓ 2.36. *Donades $R, S \in \mathrm{Eqv}(A)$, el seu suprem ve donat per*

$$\begin{aligned} R \vee S = \quad & \{(a,b) \in A \times A \mid \exists n \in \mathbb{N}^*, \exists (c_i)_{i \in n} \in A^n, \\ & (c_0 = a,\ c_n = b,\ i\ \forall i \in n,\ (c_i, c_{i+1}) \in R \cup S)\}. \end{aligned}$$

És a dir, siga (a,b) un element d'$A \times A$, direm que $(a,b) \in R \vee S$ si existeix una seqüència finita d'elements en A que comença en a i acaba en b, per a la que tots els elements consecutius estan relacionats per R o per S.

DEMOSTRACIÓ. Comprovem que és una relació d'equivalència.

En primer lloc, és trivial que la propietat reflexiva es compleix, ja que $(a,a) \in R \vee S$, per a tot $a \in A$. D'altra banda, per a tot $a, b \in A$ si $(a,b) \in R \vee S$, aleshores existeix un camí en $R \cup S$ d'a en b. Així, existeix un camí en $R \cup S$ de b en a donat per la seqüència inversa i per tant $(b,a) \in R \vee S$. Per consegüent, es compleix la propietat simètrica. Només queda comprovar la propietat transitiva. Per a tot $a, b, c \in A$, si $(a,b) \in R \vee S$ i $(b,c) \in R \vee S$, aleshores existeix un camí en $R \cup S$ d'a

en b, i un altre camí en $R \cup S$ de b en c. Unint els dos camins, tindrem que existeix un camí en $R \cup S$ d'a en c i per tant $(a, c) \in R \vee S$.

És a dir, $R \vee S$ és una relació d'equivalència, però faltaria veure que és el suprem de R i S, és a dir, que és la menor de les fites superiors.

Notem que $R \subseteq R \vee S$, $S \subseteq R \vee S$. Siga $T \in \mathrm{Eqv}(A)$ tal que $R \subseteq T$ i $S \subseteq T$, volem demostrar que $R \vee S \subseteq T$. Siga $(a, b) \in R \vee S$, aleshores existeix un cami d'n elements en $R \cup S$ que va d'a en b. Comprovarem que $(a, b) \in T$ per inducció sobre la longitud n del camí. Si $n = 1$, aleshores $(a, b) \in R \cup S$ i, com que $R \subseteq T$ i $S \subseteq T$, llavors $(a, b) \in T$. Suposem que la hipòtesi es verifica per a camins de longitud n i que $(c_i, c_{i+1})_{i \in n+1}$ és un camí en $R \cup S$ de $n + 1$ elements que va d'a en b. Així, $(c_i, c_{i+1})_{i \in n}$ és un camí en $R \cup S$ de n elements que va d'a en c_n i, per la hipòtesi d'inducció, es té que $(a, c_n) \in T$. A més, $(c_n, b) \in R \cup S \subseteq T$ i, per tant, $(a, b) \in T$ per la propietat transitiva. En conclusió, $R \vee S = \sup\{R, S\} \in \mathrm{Eqv}(A)$. □

Proposició 2.37. *Siga A un conjunt i siga $(R_i)_{i \in I}$ una família de relacions d'equivalència sobre A. Aleshores $\bigcap_{i \in I} R_i$ és una relació d'equivalència en A. A més,*

$$\bigwedge_{i \in I} R_i = \bigcap_{i \in I} R_i.$$

Demostració. En primer lloc, demostrarem que $\bigcap_{i \in I} R_i$ satisfà les propietats de la Definició 2.32. Siga $a \in A$, per ser relacions d'equivalència es té que, per a tot $i \in I$, aR_ia. Així, és clar que $(a, a) \in \bigcap_{i \in I} R_i$ i, per tant, se satisfà la propietat reflexiva. Siguen ara $a, b \in A$ tals que $(a, b) \in \bigcap_{i \in I} R_i$, aleshores $(a, b) \in R_i$ per a tot $i \in I$. Com que són relacions d'equivalència, sabem que $(b, a) \in R_i$ per a tot $i \in I$ i, per tant, es té que $(b, a) \in \bigcap_{i \in I} R_i$. Per últim, siguen $a, b, c \in A$ tals que (a, b), $(b, c) \in \bigcap_{i \in I} R_i$, aleshores (a, b), $(b, c) \in R_i$ per a tot $i \in I$. Per la propietat transitiva de les relacions d'equivalència, es té que $(a, c) \in R_i$ per a tot $i \in I$. Així, $(a, c) \in \bigcap_{i \in I} R_i$. Per tant, $\bigcap_{i \in I} R_i$ és una relació d'equivalència.

Comprovem ara que l'ínfim d'una família de relacions d'equivalència és en efecte la intersecció d'aquestes relacions. D'una banda, és clar que $\bigcap_{i \in I} R_i \subseteq R_i$ per a tot $i \in I$. D'altra banda, siga $T \in \mathrm{Eqv}(A)$ tal que $T \subseteq R_i$ per a tot $i \in I$, aleshores $T \subseteq \bigcap_{i \in I} R_i$. És a dir, $\bigcap_{i \in I} R_i$ és la major de les fites inferiors i, per tant, $\bigwedge_{i \in I} R_i = \bigcap_{i \in I} R_i$. □

En aquest punt, podem demostrar que $\mathrm{Eqv}(A)$ és un reticle complet.

Teorema 2.38. *El conjunt $\big(\mathrm{Eqv}(A), \subseteq\big)$ és un reticle complet.*

DEMOSTRACIÓ. Per la Proposició 2.34 sabem que $\big(\mathrm{Eqv}(A), \subseteq\big)$ és un conjunt parcialment ordenat. Ara, siguen R i S dues relacions d'equivalència sobre A, per demostrar que $\big(\mathrm{Eqv}(A), \subseteq\big)$ és un reticle, hem de comprovar que el suprem i l'ínfim de R i S existeixen en $\mathrm{Eqv}(A)$. Per la Proposició 2.36, sabem que $R \vee S = \sup\{R, S\} \in \mathrm{Eqv}(A)$. A més, per la Proposició 2.37, sabem que $R \cap S = R \wedge S \in \mathrm{Eqv}(A)$ i, per tant, $\big(\mathrm{Eqv}(A), \subseteq\big)$ és un reticle.

A més, siga $P \subseteq \mathrm{Eqv}(A)$, com que $\mathrm{Eqv}(A)$ és tancat per a interseccions arbitràries com hem demostrat a la Proposició 2.37, sempre existeix l'ínfim de P, $\bigvee P$. Per tant, pel Teorema 2.26 sabem que $\big(\mathrm{Eqv}(A), \subseteq\big)$ és un reticle complet. □

COROL·LARI 2.39. *Per a un conjunt A, Δ_A i ∇_A són respectivament l'element mínim i màxim del reticle complet $\big(\mathrm{Eqv}(A), \subseteq\big)$.*

COROL·LARI 2.40. *Siga A un conjunt i $(R_i)_{i\in I}$ una família de relacions d'equivalència sobre A. Aleshores $\bigvee_{i\in I} R_i$ és una relació d'equivalència sobre A.*

DEMOSTRACIÓ. Pel Teorema 2.26 i la Proposició 2.37. □

NOTA 2.41. *Siga A un conjunt, el reticle complet $\big(\mathrm{Eqv}(A), \subseteq\big)$ es pot representar pel diagrama de Hasse donat per la Figura 4.1.*

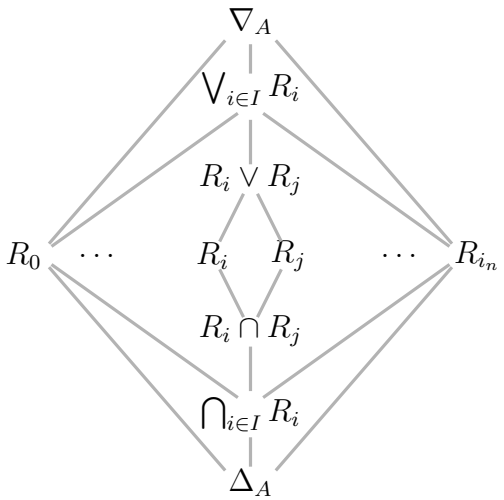

FIGURA 4.1. Reticle $\big(\mathrm{Eqv}(A), \subseteq\big)$.

5. Operadors de Clausura

Una forma de produir i reconéixer reticles complets i algebraics és a través dels operadors de clausura. En aquest capítol veurem, en primer

lloc, què és un operador de clausura i la seua relació amb els reticles complets.

DEFINICIÓ 2.42. *Siga A un conjunt i $\mathcal{P}(A)$ el conjunt de les parts d'A. Una aplicació $\mathcal{C} : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ s'anomena* **operador de clausura en** *A si, per a tot $X, Y \subseteq A$, satisfà*
Extensivitat

$$X \subseteq \mathcal{C}(X). \tag{C1}$$

Idempotència

$$\mathcal{C}^2(X) = \mathcal{C}(X). \tag{C2}$$

Monotonia

$$\text{Si } X \subseteq Y, \text{ aleshores } \mathcal{C}(X) \subseteq \mathcal{C}(Y). \tag{C3}$$

Direm que $X \subseteq A$ és **tancat** *si $\mathcal{C}(X) = X$.*

Vegem alguns exemples d'operadors de clausura.

EXEMPLE 2.43. *Siga L un reticle complet. Per a $X \subseteq L$ definim*

$$\mathcal{C}(X) = \{a \in L \mid a \leq \sup(X)\}.$$

Notem que $\mathcal{C}$ és un operador de clausura.

Per una part, siga $x \in X$, és clar que $x \leq sup(X)$ i, per la definició de $\mathcal{C}$, $x \in \mathcal{C}(X)$. Per tant,

$$X \subseteq \mathcal{C}(X),$$

és a dir, $\mathcal{C}$ és extensiu.

A més, notem que $\mathcal{C}$ és idempotent, ja que d'una banda, com $X \subseteq \mathcal{C}(X)$, aleshores $\sup(X) \leq \sup(\mathcal{C}(X))$. D'altra banda, si $a \in \mathcal{C}(X)$ aleshores $a \leq \sup(X)$. Per tant, $\sup(\mathcal{C}(X)) \leq \sup(X)$. Així,

$$\mathcal{C}^2(X) = \{a \in L \mid a \leq \sup(\mathcal{C}(X))\} = \{a \in L \mid a \leq \sup(X)\} = \mathcal{C}(X).$$

Per últim, siguen $X, Y \subseteq L$ tals que $X \subseteq Y$, aleshores $\sup(X) \leq \sup(Y)$ i, per tant,

$$\mathcal{C}(X) \subseteq \mathcal{C}(Y),$$

és a dir, $\mathcal{C}$ és monòton.

Cal assenyalar que l'Exemple 2.43 ens permet concluir que, donat un reticle complet, sempre té associat un operador de clausura. Més endavant vorem que també podem fer el procés invers.

EXEMPLE 2.44. *Siga V un $\mathbb{K}-$espai vectorial i $S \subseteq V$, recordem que $\langle S\rangle = \{\sum_{i=1}^{k} \lambda_i v_i \mid v_i \in S\}$ és el subespai generat pel subconjunt S. Per definició, l'operador $\langle * \rangle : \mathcal{P}(V) \longrightarrow \mathcal{P}(V)$ és un operador de clausura. A més, si $U = \langle S\rangle$ i $W = \langle T\rangle$, notem que*

$$U \wedge W = U \cap W \quad i \quad U \vee W = \langle U \cup W\rangle = U + W.$$

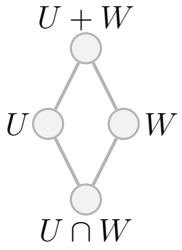

FIGURA 5.1. Figura Exemple 2.44.

A continuació demostrem que per a un operador clausura $\mathcal{C}$ definit sobre un conjunt A, el conjunt parcialment ordenat de subconjunts tancats d'A amb la inclusió $\subseteq$ com a ordre parcial és un reticle complet. El denotarem per $\big(L_{\mathcal{C}}, \subseteq\big)$, on

$$L_{\mathcal{C}} = \{X \subseteq A \mid \mathcal{C}(X) = X\}.$$

TEOREMA 2.45. *Siga $\mathcal{C}$ un operador de clausura en un conjunt A, i $(A_i)_{i\in I}$ una familia de tancats. Aleshores $L_{\mathcal{C}}$ és un reticle complet amb*

$$\bigwedge_{i\in I} \mathcal{C}(A_i) = \bigcap_{i\in I} \mathcal{C}(A_i), \tag{1}$$

$$\bigvee_{i\in I} \mathcal{C}(A_i) = \mathcal{C}\Big(\bigcup_{i\in I} A_i\Big). \tag{2}$$

DEMOSTRACIÓ. En primer lloc, anem a demostrar (1).

Notem $\bigcap_{i\in I} A_i \subseteq A_i$ per a tot $i \in I$. Per (C3), $\mathcal{C}\big(\bigcap_{i\in I} A_i\big) \subseteq \mathcal{C}(A_i)$ per a tot $i \in I$. A més, com que A_i són tancats, $\mathcal{C}(A_i) = A_i$, i així

$$\mathcal{C}\Big(\bigcap_{i\in I} A_i\Big) \subseteq \bigcap_{i\in I} \mathcal{C}(A_i) = \bigcap_{i\in I} A_i.$$

D'altra banda, per (C1), $\bigcap_{i\in I} A_i \subseteq \mathcal{C}\big(\bigcap_{i\in I} A_i\big)$.

Per tant $\bigcap_{i\in I} A_i = \mathcal{C}\big(\bigcap_{i\in I} A_i\big)$, és a dir, $\bigcap_{i\in I} A_i$ és tancat i en conseqüència

$$\bigcap_{i\in I} A_i \in L_{\mathcal{C}}.$$

Així, com que per a tot $i \in I$ es té que $\bigcap_{i\in I} A_i \subseteq A_i$, aleshores

$$\bigwedge_{i\in I} \mathcal{C}(A_i) = \bigwedge_{i\in I} A_i = \bigcap_{i\in I} A_i = \bigcap_{i\in I} \mathcal{C}(A_i).$$

A continuació demostrarem (2).

Siga Z un tancat en $L_{\mathcal{C}}$ que satisfà $A_i \subseteq Z$ per a tot $i \in I$. Aleshores $\bigcup_{i\in I} A_i \subseteq Z$, i com que $\mathcal{C}$ és monòton (C3) i Z és tancat, tenim que $\mathcal{C}\big(\bigcup_{i\in I} A_i\big) \subseteq \mathcal{C}(Z) = Z$. En particular,

$$\mathcal{C}\Big(\bigcup_{i\in I} A_i\Big) \subseteq \bigvee_{i\in I} A_i.$$

A més, com l'operador de clausura és idempotent, (C2), aleshores

$$\mathcal{C}\Big(\mathcal{C}\Big(\bigcup_{i\in I} A_i\Big)\Big) = \mathcal{C}\Big(\bigcup_{i\in I} A_i\Big)$$

i, per tant, $\mathcal{C}\big(\bigcup_{i\in I} A_i\big)$ és tancat.

Notem que, per a tot $i \in I$, $A_i \subseteq \bigcup_{i\in I} A_i$. Per (C3), per a tot $i \in I$, $A_i = \mathcal{C}(A_i) \subseteq \mathcal{C}\big(\bigcup_{i\in I} A_i\big)$. Així,

$$\bigvee_{i\in I} A_i \subseteq \mathcal{C}\Big(\bigcup_{i\in I} A_i\Big).$$

Per tant, $\bigvee_{i\in I} A_i = \mathcal{C}\Big(\bigcup_{i\in I} A_i\Big)$.

En definitiva, tenim que el conjunt parcialment ordenat $(L_{\mathcal{C}}, \subseteq)$ satisfà que per a tot subconjunt de $L_{\mathcal{C}}$ existeix el suprem i l'ínfim en $L_{\mathcal{C}}$ i, pel Teorema 2.26, tenim per tant que és un reticle complet. □

En síntesi, donat un reticle complet L es pot definir un operador de clausura seguint l'Exemple 2.43; i donat un operador de clausura $\mathcal{C}$, aleshores $L_{\mathcal{C}}$ és un reticle complet amb les condicions del Teorema 2.45.

Vegem ara què vol dir que un operador de clausura siga algebraic, així com la seua relació amb els reticles algebraics.

Definició 2.46. *Un operador de clausura $\mathcal{C}$ en un conjunt A s'anomena* **algebraic** *si per a tot $X \subseteq A$ es té que*

$$\mathcal{C}(X) = \bigcup\{\mathcal{C}(Y) \mid Y \text{ finit}, Y \subseteq X\}.$$

Teorema 2.47. *Si $\mathcal{C}$ és un operador de clausura algebraic, aleshores $L_{\mathcal{C}}$ és un reticle algebraic i els elements compactes de $L_{\mathcal{C}}$ són precisament els elements de la forma $\mathcal{C}(X)$ amb X finit.*

DEMOSTRACIÓ. El teorema es demostra comprovant que $\mathcal{C}(X)$ és compacte si, i només si, X és finit.

Suposem en primer lloc que X és finit. Com $\mathcal{C}$ és un operador de clausura, per la idempotència (C2), es té que

$$\mathcal{C}\big(\mathcal{C}(X)\big) = \mathcal{C}^2(X) = \mathcal{C}(X),$$

és a dir, $\mathcal{C}(X)$ és tancat.

Per veure que $\mathcal{C}(X)$ és compacte basta provar que és fitat.

Siga $A \subseteq L_{\mathcal{C}}$, com $L_{\mathcal{C}}$ és un reticle complet, $\bigvee A$ existeix. Si suposem que $\mathcal{C}(X) \subseteq \bigvee A$, com X finit, $X = \{x_i \mid i \in n\}$, podem suposar $A = \{A_i \mid i \in n\}$. Així,

$$\mathcal{C}(X) \subseteq \bigvee A = \bigvee_{i\in n} A_i = \mathcal{C}\Big(\bigcup_{i\in n} A_i\Big) \qquad \text{(pel Teorema 2.45)}$$

Com $\mathcal{C}$ és algebraic,

$$\mathcal{C}\Big(\bigcup_{i\in n} A_i\Big) = \bigcup\{\mathcal{C}(Y) \mid Y \subseteq \bigcup_{i\in n} A_i,\ Y \text{ finit}\}.$$

És a dir, $\mathcal{C}(X)$ està contingut en la unió finita de clausures de subconjunts finits i, per tant, està fitat.

Suposem ara que $\mathcal{C}(X)$ és compacte i, per reducció a l'absurd, suposem que $\mathcal{C}(Y)$ és un compacte tal que

$$\mathcal{C}(Y) \subset \bigcup\{\mathcal{C}(X) \mid X\text{finit},\ X \subseteq Y\},$$

amb la inclusió estricta. Si $\mathcal{C}(Y)$ estiguera inclòs en una unió finita de $\mathcal{C}(X)$, és a dir,

$$\mathcal{C}(Y) \subseteq \mathcal{C}(X_1) \cup \cdots \cup \mathcal{C}(X_k) \subseteq \mathcal{C}(X_1 \cup \cdots \cup X_k)$$

amb $X_1, \ldots X_k \subseteq Y$, tindríem que

$$X_1 \cup \cdots \cup X_k \subseteq Y$$

i aleshores

$$\mathcal{C}(X_1 \cup \cdots \cup X_k) \subseteq \mathcal{C}(Y).$$

Per tant, $\mathcal{C}(X_1 \cup \cdots \cup X_k) = \mathcal{C}(Y)$. Açò és una contradicció amb el que hem suposat.

Aleshores, $\mathcal{C}(Y)$ no és compacte, que també seria una contradicció. Per tant, $\mathcal{C}(Y) = \mathcal{C}(X)$ per a algun X finit.

Així, en efecte, els elements compactes de $L_{\mathcal{C}}$ són els elements de la forma $\mathcal{C}(X)$ amb X finit i, per tant, $L_{\mathcal{C}}$ és compactament generat. Per definició, $L_{\mathcal{C}}$ és complet i podem concloure així que $L_{\mathcal{C}}$ és un reticle algebraic. □

En conclusió, mentre que els operadors de clausura creen reticles $L_{\mathcal{C}}$ complets, els operadors de clausura algebraics generen reticles algebraics.

A partir d'un operador de clausura, definirem ara els conceptes de ser generador d'un conjunt, finitament generat i generador minimal.

DEFINICIÓ 2.48. *Siga $\mathcal{C}$ un operador de clausura en A i Y un subconjunt tancat d'A. Direm que X és un* **generador d'Y** *si $\mathcal{C}(X) = Y$. Direm que Y és* **finitament generat** *si existeix un generador d'Y finit. Direm que X és* **generador minimal d'Y** *si X és generador d'Y i cap subconjunt estricte de X genera Y.*

Aquestes definicions ens permetran trobar una relació entre els elements compactes i un operador de clausura algebraic, amb ajuda del següent corol·lari.

COROL·LARI 2.49. *Siga $\mathcal{C}$ un operador de clausura algebraic en A. Aleshores els subconjunts d'A finitament generats són els elements compactes de $L_{\mathcal{C}}$.*

DEMOSTRACIÓ. Siga Y un subconjunt d'A finitament generat, aleshores per definició existeix X un subconjunt finit d'A generador d'Y, és a dir, tal que

$$\mathcal{C}(X) = Y.$$

Pel Teorema 2.47, sabem que els conjunts $\mathcal{C}(X)$ amb X finit són conjunts compactes de $L_{\mathcal{C}}$. Açò demostra el Corol·lari 2.49. □

Com hem vist abans, un operador de clausura algebraic genera un reticle algebraic. En realitat, la relació entre ells va més enllà, ja que qualsevol reticle algebraic és isomorf a un reticle amb un operador de clausura algebraic, com demostrarem en el següent Teorema.

TEOREMA 2.50. *Tot reticle algebraic és isomorf al reticle dels subconjunts tancats d'un conjunt amb un operador de clausura algebraic.*

DEMOSTRACIÓ. Siga L un reticle algebraic, considerem $A \subseteq L$ el conjunt format per tots els elements compactes de L.

Ara, definim un operador de clausura $\mathcal{C}$ sobre L de la següent manera:

$$\begin{array}{rccc} \mathcal{C}: & \mathcal{P}(A) & \longrightarrow & \mathcal{P}(A) \\ & X & \longmapsto & \{a \in A \mid a \leq \bigvee X\}. \end{array}$$

És a dir, per a qualsevol subconjunt X de L, definim $\mathcal{C}(X)$ com el conjunt de tots els elements compactes que són menors o iguals al suprem de X.

Vegem que $\mathcal{C}$ és un reticle algebraic. Siga $a \in A$, com que a és compacte, existirà $B_a \subseteq A$ amb B_a finit tal que $a \leq \bigvee B_a$. Notem $\mathcal{C}(B_a) = \{a \in A \mid a \leq \bigvee B_a\}$. Per tant, per a tot $X \subseteq A$, podem escriure $\mathcal{C}(X)$ com la unió dels $\mathcal{C}(B_a)$, amb B_a finit i $a \in A$ tals que $a \leq \bigvee X$. Així, pel Teorema 2.47, sabem que $L_{\mathcal{C}}$ és un reticle algebraic i els elements compactes de $L_{\mathcal{C}}$ són precisament els elements de la forma $\mathcal{C}(X)$ amb X finit.

En aquest punt, podem definir una funció que assigne a cada element z en L el conjunt de tots els elements compactes de $L_{\mathcal{C}}$ que són menors o iguals que z, és a dir, una funció definida de la següent manera:

$$\begin{array}{rccl} \phi: & L & \longrightarrow & L_{\mathcal{C}} \\ & z & \longmapsto & \{a \in A \mid a \leq z\}. \end{array}$$

Demostrarem que ϕ és un isomorfisme entre els reticles L i $L_{\mathcal{C}}$.

En primer lloc, comprovarem la injectivitat. Siguen $x, y \in L$ tals que $\phi(x) = \phi(y)$. Això significa que

$$\{a \in A \mid a \leq x\} = \{a \in A \mid a \leq y\}.$$

Per tant, x i y han de ser iguals, ja que els conjunts d'elements compactes que són menors o iguals són els mateixos.

Vegem ara que ϕ és sobrejectiva. Siga $Y \subseteq L_{\mathcal{C}}$, volem demostrar que existeix un element x en L tal que $\phi(x) = Y$. Considerem el suprem de tots els elements compactes en Y, és a dir,

$$x = \bigvee \{a \in A \mid a \leq y, y \in Y\}.$$

Llavors, $\phi(x) = \{a \in A \mid a \leq x\} = Y$, ja que Y conté tots els elements compactes que són menors o iguals que x.

Per últim, ϕ preserva les operacions. Siguen $x, y \in L$, d'una banda,

$$\begin{aligned} \phi(x \vee y) &= \{a \in A \mid a \leq x \vee y\} \\ &= \{a \in A \mid a \leq \bigvee \{x, y\}\} \\ &= \{a \in A \mid a \leq x\} \vee \{a \in A \mid a \leq y\} \\ &= \phi(x) \vee \phi(y). \end{aligned}$$

D'altra banda, notem que

$$\begin{aligned} \phi(x \wedge y) &= \{a \in A \mid a \leq x \wedge y\} \\ &= \{a \in A \mid a \leq \bigwedge \{x, y\}\} \\ &= \{a \in A \mid a \leq x, a \leq y\} \\ &= \phi(x) \wedge \phi(y). \end{aligned}$$

Per tant, ϕ és un isomorfisme entre els reticles L i $L_{\mathcal{C}}$. Açò conclou la demostració del Teorema 2.50. $\square$

CAPíTOL 3

Elements de l'Àlgebra Universal

> El álgebra es generosa; a menudo da más de lo que se le pide.
>
> *Jean Le Rond d'Alembert*[**9**]

Com hem mencionat abans, un dels objectius de l'àlgebra universal és extraure trets comuns d'estuctures algebraiques aparentment diferents. Així, obtenim conceptes generals i resultats que no només generalitzen i unifiquen estructures conegudes, sinò que, degut al nivell superior d'abstracció, també es poden aplicar a situacions noves.

En aquest capítol recopilem els conceptes i resultats bàsics que ens permeten introduir-nos en el món de l'àlgebra universal. En la Secció 1, titulada *Definicions i Exemples*, començarem definint el concepte d'àlgebra i estudiarem diferents exemples d'aquest tipus d'estructures, com els grups o els reticles. També introduirem la noció d'homomorfisme entre dos àlgebres. En la Secció 2, titulada *Subàlgebres*, després de definir la noció de subàlgebra, treballarem el concepte de subàlgebra generada. També demostrarem que la imatge d'un homomorfisme entre dues àlgebres és un conjunt tancat de l'àlgebra imatge per a les operacions d'aquesta. La Secció 3, titulada *Congruències i Àlgebra Quocient*, té com a finalitat establir els fonaments teòrics necessaris per a abordar els conceptes de congruència, àlgebra quocient i homomorfisme. A més, es proporcionarà una visió general dels conjunts de congruències en àlgebres, posant èmfasi en la seua estructura de reticle algebraic. En la Secció 4, titulada *Teoremes d'Isomorfia*, després de presentar diferents resultats sobre els $\Sigma-$homomorfismes i estudiar aquesta noció, treballarem amb els Teoremes d'Isomorfia. Dedicarem a cada teorema una subsecció en la qual introduirem els conceptes i els resultats necessaris per a presentar i demostrar el respectiu teorema. Per últim, en la Secció 5 titulada *Àlgebra de Termes*, definirem què és una àlgebra de termes i demostrarem la seua Propietat Universal. Per concloure, demostrarem que tota àlgebra és isomorfa a un quocient d'una àlgebra de termes.

1. Definicions i Exemples

Començarem la secció definint els conceptes d'operació $n-$ària i de signatura. Després, emprarem aquestes definicions per a presentar la noció d'àlgebra i estudiar exemples concrets d'àlgebres, alguns dels quals ens resultaran familiars, com els grups o els anells. Per últim, introduirem el concepte d'homomorfisme entre àlgebres de la mateixa signatura.

DEFINICIÓ 3.1. *Siga A un conjunt no buit i $n \in \mathbb{N}$ un natural. Definim $A^n = \mathrm{Hom}(n, A) = \{a : n \longrightarrow A \mid a \text{ aplicació}\}$, on*

$$\begin{array}{rccc} a: & n & \longrightarrow & A \\ & 0 & \longmapsto & a_0 \\ & 1 & \longmapsto & a_1 \\ & & \vdots & \\ & n-1 & \longmapsto & a_{n-1} \end{array}$$

Podem escriure a com la n-tupla en forma compacta

$$(a_0, a_1, \ldots, a_{n-1}) = (a_i)_{i \in n}.$$

Una **operació n-ària** *és qualsevol aplicació en* $\mathrm{Hom}(A^n, A)$.

Per exemple, una constant és una aplicació 0-ària, és a dir, un element qualsevol d'$\mathrm{Hom}(A^0, A) = \mathrm{Hom}(1, A)$. Aquestes constants estan completament determinades pel valor de l'aplicació en 0, de forma que

$$\begin{array}{rccc} \sigma: & 1 & \longrightarrow & A \\ & 0 & \longmapsto & a_0 \end{array},$$

és a dir $\sigma = (a_0)$.

DEFINICIÓ 3.2. *Una* **signatura** *és un parell (Σ, ar) on Σ és un conjunt, els elements del qual s'anomenen* **símbols d'operacions** *i* ar *és una aplicació* $\mathrm{ar} : \Sigma \longrightarrow \mathbb{N}$ *que assigna a cada símbol d'operació la seua aritat. El subconjunt de símbols d'operacions n-àries es denota per $\Sigma_n = \mathrm{ar}^{-1}[\{n\}]$. A més, si les aritats estan clares, escriurem Σ en compte de (Σ, ar).*

EXEMPLE 3.3. *Podem considerar $\Sigma = \{+, \cdot\, , 1, 0\}$ i les aritats*

$$\begin{array}{rccc} \mathrm{ar}: & \Sigma & \longrightarrow & \mathbb{N} \\ & + & \longmapsto & 2 \\ & \cdot & \longmapsto & 2 \\ & 1 & \longmapsto & 0 \\ & 0 & \longmapsto & 0 \end{array}$$

de manera que Σ és una signatura amb dos operacions binàries i dos operacions constants. Aixi, $\Sigma_2 = \{+, \cdot\}$, $\Sigma_0 = \{1, 0\}$ i $\Sigma_n = \emptyset$ per a $n \notin \{0, 2\}$.

A continuació, com es va anunciar prèviament, tenint en compte la Definició 3.2 de signatura, formalitzarem la definició d'àlgebra.

DEFINICIÓ 3.4. *Siga Σ una signatura, una* **$\Sigma-$àlgebra** *és un parell $\mathbf{A} = (A, F)$ on A és un conjunt i F és una aplicació que ens dóna l'interpretació dels símbols d'operació en l'àlgebra $\mathbf{A}$.*

$$\begin{array}{rccl} F: & \Sigma & \longrightarrow & \bigcup_{n\in\mathbb{N}} \mathrm{Hom}(A^n, A) \\ & \sigma & \longmapsto & F(\sigma) \in \mathrm{Hom}(A^{\mathrm{ar}(\sigma)}, A) \end{array}$$

En llenguatge comú, en una àlgebra dotem un conjunt A d'operacions que sempre donen com a resultats elements d'eixe conjunt en aplicar-les sobre famílies de les respectives aritats.

EXEMPLE 3.5. *Si considerem Σ definida com abans amb $\Sigma = \{+, \cdot, 1, 0\}$, un exemple de Σ-àlgebra és $\mathbb{R}$ amb la suma i el producte habitual, i l'elecció del 0 i l'1 com a constants.*

EXEMPLE 3.6. *Seguint amb la signatura $\Sigma = \{+, \cdot, 1, 0\}$, el conjunt S dels cercles en $\mathbb{R}^2$,*

$$S = \{B(0, r) \mid r \in \mathbb{R}\}$$

és un altre exemple de Σ-àlgebra amb les operacions definides com seguеix.

$$\begin{array}{rccl} +: & S \times S & \longrightarrow & S \\ & \big(B(0,r), B(0,s)\big) & \longmapsto & B(0, r+s), \end{array}$$

És a dir, l'operació $+$ dona com a resultat el cercle de radi $r + s$, amb la suma habitual.

$$\begin{array}{rccl} \cdot: & S \times S & \longrightarrow & S \\ & \big(B(0,r), B(0,s)\big) & \longmapsto & B(0, r\cdot s) \end{array}$$

És a dir, l'operació $\cdot$ dona com a resultat el cercle de radi $r \cdot s$, amb el producte habitual.

Per últim

$$\begin{array}{rccl} 1: & 1 & \longrightarrow & S \\ & 1 & \longmapsto & B(0,1) \end{array} \qquad \begin{array}{rccl} 0: & 0 & \longrightarrow & S \\ & 0 & \longmapsto & B(0,0) \end{array}$$

donen respectivament els cercles de radis 1 i 0, amb l'elecció del 0 i l'1 com a constants.

NOTA 3.7. *Normalment treballarem amb una única estructura de $\Sigma-$àlgebra sobre una àlgebra $\mathbf{A} = (A, F)$, i si $\sigma \in \Sigma$, escriurem $\sigma^{\mathbf{A}}$ en compte de $F(\sigma)$, o fins i tot identificarem els símbols d'operació amb les seues interpretacions.*

Per exemple, $\mathbb{R} = (\mathbb{R}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, 0^{\mathbb{R}}, 1^{\mathbb{R}}) = (\mathbb{R}, +, \cdot, 0, 1)$.

Anem a vore exemples més concrets de Σ-àlgebres.

EXEMPLE 3.8 (Grups). *Un grup $\mathbf{G} = (G, \cdot, (\cdot)^{-1}, 1)$ és una àlgebra per a les operacions d'aritat*

$$\mathrm{ar}(\cdot) = 2; \qquad \mathrm{ar}\big((\cdot)^{-1}\big) = 1; \qquad \mathrm{ar}(1) = 0,$$

que satisfà que, per a tot $x, y, z \in G$,
Associativitat

$$(x \cdot y) \cdot z = x \cdot (y \cdot z). \tag{G1}$$

Neutre

$$x \cdot 1 = 1 \cdot x = x. \tag{G2}$$

Invers

$$x \cdot x^{-1} = x^{-1} \cdot x = 1. \tag{G3}$$

A més, un grup és abelià si es verifica que, per a tot $x, y \in G$,
Commutativitat

$$x \cdot y = y \cdot x. \tag{G4}$$

EXEMPLE 3.9 (Semigrups i monoids). *Un semigrup és una àlgebra $(G, \cdot)$ que satisfà (G1). Un monoide és una àlgebra $(G, \cdot, 1)$ que satisfà (G1) i (G2).*

EXEMPLE 3.10 (Quasigrups i loops). *Un quasigrup és una àlgebra $\mathbf{Q} = (Q, /, \setminus, \cdot)$ amb tres operacions binàries que per a tot $x, y \in Q$ satisfan*

$$x \setminus (x \cdot y) = y \ i \ (x \cdot y)/y = x. \tag{Q1}$$

$$x \cdot (x \setminus y) = y \ i \ (x \setminus y) \cdot y = x. \tag{Q2}$$

Un loop és un quasigrup amb identitat, és a dir una àlgebra $(Q, /, \setminus, \cdot, 1)$ que satisfà (G2), (Q1) i (Q2).

EXEMPLE 3.11 (Anells). *Un anell és una àlgebra $\mathbf{A} = (A, +, \cdot, (\cdot)^{-1}, 0)$ amb*

$$\mathrm{ar}(+) = 2; \qquad \mathrm{ar}(\cdot) = 2; \qquad \mathrm{ar}\big((\cdot)^{-1}\big) = 1; \qquad \mathrm{ar}(0) = 0$$

que satisfà

Grup abelià

$$(A, +, (\cdot)^{-1}, 0) \text{ és un grup abelià i per tant satisfà les} \tag{A1}$$

propietats (G1,) (G2), (G3) i (G4).

Semigrup

$$(A, \cdot) \text{ és un semigrup, és a dir, satisfà (G1).} \tag{A2}$$

Distributiu *Per a tot $x, y, z \in A$ es té que*

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad i \quad (x + y) \cdot z = (x \cdot z) + (y \cdot z). \tag{A3}$$

Un anell amb identitat és una àlgebra $(A, +, \cdot, (\cdot)^{-1}, 0, 1)$ que satisfà (A1), (A2), (A3) i (G2).

EXEMPLE 3.12 (Espais vectorials). *Siga $\mathbb{K}$ un cos, un $\mathbb{K}$-espai vectorial $\mathbf{V} = (V, +, (\cdot_\lambda)_{\lambda\in\mathbb{K}}, 0)$, és una àlgebra amb*

$$+ : \ V \times V \ \longrightarrow \ V$$

i on $\cdot_\lambda$ és una operació unària per a cada $\lambda \in \mathbb{K}$, de la forma

$$\begin{array}{rccc} \cdot_\lambda : & V & \longrightarrow & V \\ & v & \longmapsto & \lambda v. \end{array}$$

EXEMPLE 3.13 (Reticles). *Un reticle és una àlgebra $(L, \wedge, \vee)$ amb dues operacions binàries que satisfan les lleis (R1), (R2), (R3) i (R4) vistes a la Definició 2.1.*

A continuació, introduïm els homomorfismes d'àlgebres.

DEFINICIÓ 3.14. *Siga Σ una signatura i $\mathbf{A} = (A, F)$, $\mathbf{B} = (B, G)$ dos $\Sigma-$àlgebres, un* **$\Sigma-$homomorfisme d'A en B** *és una aplicació $f : A \longrightarrow B$ que satisfà que, per a tot $\sigma \in \Sigma$ amb $\mathrm{ar}(\sigma) = n$ i tota familia $(a_i)_{i\in n} \in A^n$, es compleix*

$$f\Big(\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big)\Big) = \sigma^{\mathbf{B}}\Big(\big(f(a_i)\big)_{i\in n}\Big).$$

Ho escriurem com $f : \mathbf{A} \longrightarrow \mathbf{B}$.

EXEMPLE 3.15. *Considerem una signatura $\Sigma = \{+, 0\}$ amb $+$, una operació binària, i 0, una constant. Siguen $\mathbf{A}$ i $\mathbf{B}$ dues subàlgebres per a Σ. Aleshores es compleix que*

$$f(a +^{\mathbf{A}} b) = f(a) +^{\mathbf{B}} f(b).$$

En altres paraules, la imatge per f de l'element $a +^{\mathbf{A}} b$ amb la suma definida en l'àlgebra $\mathbf{A}$ és el resultat de realitzar la suma definida en l'àlgebra $\mathbf{B}$ dels elements $f(a)$ i $f(b)$, que per la definició de l'homomorfisme, es troben en B.

Anàlogament, si considerem l'operació constant 0 *en* $\mathbf{A}$ *i* $\mathbf{B}$*, tenim que*

$$f(0^{\mathbf{A}}) = 0^{\mathbf{B}}.$$

És a dir, la imatge per f *de la constant definida per* 0 *en* $\mathbf{A}$ *ha de ser la constant definida per* 0 *en* $\mathbf{B}$*.*

Notem que per definir la noció de $\Sigma-$*homomorfisme entre les àlgebres* $\mathbf{A}$ *i* $\mathbf{B}$ *no és necessari que ambdues siguen d'una classe en especial, basta només amb què estiguen definides sobre la mateixa signatura.*

DEFINICIÓ 3.16. *Siguen* $\mathbf{A}$ *i* $\mathbf{B}$ *dues* $\Sigma-$*àlgebres i siga* $f : \mathbf{A} \longrightarrow \mathbf{B}$ *un homomorfisme. Direm que* f *és imbibició o* **monomorfisme** *si* f *és injectiu. Direm que* f *és* **epimorfisme** *si* f *és sobrejectiu. Per últim, direm que* f *és* **isomorfisme** *si* f *és un homomorfisme bijectiu. En aquest cas direm que les àlgebres* $\mathbf{A}$ *i* $\mathbf{B}$ *són isomorfes, i ho denotarem per* $\mathbf{A} \cong \mathbf{B}$*.*

2. Subàlgebres

En les àlgebres, destaca l'existència de subconjunts que són tancats per a les operacions de la signatura, nomenats subàlgebres. En la construcció de subàlgebres destaca la subàlgebra generada per un conjunt , però també podem trobar subconjunts tancats per a les operacions d'una signatura mitjançant la formació d'imatges homomòrfiques. A més, continuarem estudiant la relació que existeix entre els reticles i les àlgebres demostrant un dels resultats més importants d'aquesta secció: el conjunt de totes les subàlgebres d'una àlgebra és un reticle algebraic.

Comencem definint la noció de subàlgebra.

DEFINICIÓ 3.17. *Siga* $\mathbf{A}$ *una* Σ*-àlgebra i* $B \subseteq A$ *un subconjunt. Direm que* B *està tancat per a* Σ *si, per a tot* $n \in \mathbb{N}$*, per a tot* $\sigma \in \Sigma_n$ *i* $(b_i)_{i\in n} \in B^n$ *es té que* $\sigma^{\mathbf{A}}\big((b_i)_{i\in n}\big) \in B$*. En cas afirmatiu,* B *admet estructura de* $\Sigma-$*àlgebra amb la mateixa interpretació que en* $\mathbf{A}$*. Denotarem aquest fet per* $\mathbf{B} \leq \mathbf{A}$ *i direm que* $\mathbf{B}$ *és una subàlgebra d'*$\mathbf{A}$*. El conjunt de totes les subàlgebres d'*$\mathbf{A}$ *es defineix com*

$$\mathrm{Sub}(\mathbf{A}) = \{B \subseteq A \mid \mathbf{B} \leq \mathbf{A}\} \subseteq \mathcal{P}(A).$$

Siga $\mathbf{A}$ una àlgebra i siga X un subconjunt arbitrari d'A. En principi, és poc probable que X siga una subàlgebra d'A, ja que molt possiblement existeix una operació bàsica que, quan s'aplica a uns certs elements de X, produeix un valor fora de X. Com a primer pas cap a l'extensió de X a una subàlgebra, es podria reunir en un conjunt Y tots aquells elements que resulten d'aplicar les operacions als elements de X. Llavors $X \cup Y$ ja no és deficient com ho era X. Els nous elements

d'Y, no obstant això, ara es poden prendre com a arguments per a les operacions bàsiques, i $X \cup Y$ pot no estar tancat baix totes aquestes operacions. Però en repetir aquest procés, una quantitat numerable de voltes, X pot extendre's a una subàlgebra d'$\mathbf{A}$. Respecte a la relació de subconjunt, aquesta subàlgebra serà l'àlgebra més xicoteta d'$\mathbf{A}$ que inclou a X, ja que només s'introdueixen en ella aquells elements requerits pel tancament de les operacions. A més, la subàlgebra així obtinguda ha d'estar inclosa en tota subàlgebra que continga el subconjunt X. Per tant, pot obtenir-se com la intersecció de totes aquestes subàlgebres. Notem que el caràcter finit de les operacions fonamentals de l'àlgebra assegura que aquest procés iteratiu tinga èxit [**10**].

Formalitzem ara aquesta idea a través del concepte de subàlgebra generada.

DEFINICIÓ 3.18. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra, per a cada* $X \subseteq A$ *definim la* **subàlgebra generada per** X *com*

$$\mathrm{Sg}(X) = \bigcap \{B \subseteq A \mid X \subseteq B \ i \ \mathbf{B} \leq \mathbf{A}\} \subseteq \mathcal{P}(A),$$

és a dir, com la intersecció de totes les subàlgebres d'$\mathbf{A}$ *que contenen a* X*.*

PROPOSICIÓ 3.19. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra, per a cada* $X \subseteq A$*,* $\mathrm{Sg}(X)$ *és la menor subàlgebra d'*$\mathbf{A}$ *que conté a* X*.*

DEMOSTRACIÓ. En primer lloc, per la definició de subàlgebra generada, tenim que $X \subseteq \mathrm{Sg}(X) = \bigcap \{B \subseteq A \mid X \subseteq B \text{ i } \mathbf{B} \leq \mathbf{A}\} \subseteq A$.

D'altra banda, siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$, $(z_i)_{i\in n} \in \big(\mathrm{Sg}(X)\big)^n$, per a cada $B \subseteq A$ que satisfà $X \subseteq B$ i $\mathbf{B} \leq \mathbf{A}$ es té que $(z_i)_{i\in n} \in B^n$. Per tant, com $\mathbf{B}$ és una subalgebra de $\mathbf{A}$, es té que $\sigma^{\mathbf{A}}\big((z_i)_{i\in n}\big) \in B$, i com que açò passa per a tot B amb aquestes condicions, $\sigma^{\mathbf{A}}\big((z_i)_{i\in n}\big) \in \mathrm{Sg}(X)$. Així, $\mathrm{Sg}(X)$ és un subconjunt d'A tancat per a Σ, és a dir, $\mathbf{Sg}(\mathbf{X}) \leq \mathbf{A}$.

Per tant, només queda demostrar la minimalitat. Siga $\mathbf{C}$ una subàlgebra d'$\mathbf{A}$ que conté a X, és a dir, C un subconjunt d'A, $C \subseteq A$, tal que $X \subseteq C$ i $\mathbf{C} \leq \mathbf{A}$, aleshores

$$C \in \{B \subseteq A \mid X \subseteq C \text{ i } \mathbf{C} \leq \mathbf{A}\}.$$

Així, $\mathrm{Sg}(X) \subseteq C$.

Concloem per tant que $\mathrm{Sg}(X)$ és la menor subàlgebra d'$\mathbf{A}$ que conté a X. □

Demostrem ara que aquest operador que emprem per a construir subàlgebres és en realitat un operador de clausura.

PROPOSICIÓ 3.20. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra. L'aplicació*

$$\begin{array}{rccc} \mathrm{Sg}: & \mathcal{P}(\mathbf{A}) & \longrightarrow & \mathcal{P}(\mathbf{A}) \\ & X & \longmapsto & \mathrm{Sg}(X) \end{array}$$

és un operador de clausura.

DEMOSTRACIÓ. Recordant la Definició 2.42 d'operador de clausura del Capítol 2, hem de provar que se satisfan les propietats d'extensivitat, idempotència i monotonia.

En primer lloc, $X \subseteq \mathrm{Sg}(X)$ per la pròpia definició de subàlgebra generada, pel que se satisfà (C1).

Demostrarem ara (C2), és a dir que Sg satisfà

$$\mathrm{Sg}^2(X) = \mathrm{Sg}(X).$$

D'una banda, per (C1), $\mathrm{Sg}(X) \subseteq \mathrm{Sg}\big(\mathrm{Sg}(X)\big) = \mathrm{Sg}^2(X)$.

D'altra banda, siga $\mathbf{C}$ una subàlgebra d'$\mathbf{A}$ que conté a X. Per la minimalitat de la subàlgebra generada per X, sabem que $\mathrm{Sg}(X) \subseteq C$. Si considerem com a subconjunt d'$\mathbf{A}$ la subàlgebra generada $\mathrm{Sg}(X)$, notem que $\mathrm{Sg}(X)$ és una subàlgebra d'$\mathbf{A}$ que conté a $\mathrm{Sg}(X)$, i per la minimalitat de la subàlgebra generada per un conjunt, sabem que $\mathrm{Sg}\big(\mathrm{Sg}(X)\big) \subseteq \mathrm{Sg}(X)$.

Per últim, siga $X \subseteq Y$, notem

$$\{B \subseteq A \mid X \subseteq B \ i \ \mathbf{B} \leq \mathbf{A}\} \subseteq \{B \subseteq A \mid Y \subseteq B \ i \ \mathbf{B} \leq \mathbf{A}\}.$$

Per tant,

$$\bigcap\{B \subseteq A \mid X \subseteq B \ i \ \mathbf{B} \leq \mathbf{A}\} \subseteq \bigcap\{B \subseteq A \mid Y \subseteq B \ i \ \mathbf{B} \leq \mathbf{A}\}.$$

És a dir,$\mathrm{Sg}(X) \subseteq \mathrm{Sg}(Y)$ i es compleix així (C3).

Açò demostra que, en efecte, Sg és un operador de clausura. □

Vegem ara una presentació més constructiva de la subàlgebra generada per un conjunt relacionada amb l'argument d'afegir elements amb què havíem iniciat la secció.

PROPOSICIÓ 3.21. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra. Definim l'operador*

$$\begin{array}{rccc} E: & \mathcal{P}(A) & \longrightarrow & \mathcal{P}(A) \\ & X & \longmapsto & X \cup \{\sigma^{\mathbf{A}}\big((x_i)_{i\in n}\big) \in A \mid n \in \mathbb{N},\ \sigma \in \Sigma_n,\ (x_i)_{i\in n} \in X^n\}. \end{array}$$

És a dir, E estén un subconjunt X d'A amb el resultat de totes les operacions de Σ sobre elements d'X.

Definim recursivament les iteracions com segueix.

$$E^0(X) = X,$$
$$E^{n+1}(X) = E\big(E^n(X)\big).$$

Finalment definim $\mathrm{Sg}'(X) = \bigcup_{n\in\mathbb{N}} E^n(X)$. *Així,* $\mathrm{Sg} = \mathrm{Sg}'$, *és a dir, aquesta construcció de la subàlgebra generada és igual a la que hem vist en la Definició 3.18.*

Demostració. D'una banda, per construcció, $\mathrm{Sg}'(X)$ és un subconjunt d'A tancat per a les operacions de Σ. A més, $X \subseteq \mathrm{Sg}'(X)$. Per la minimalitat de la subàlgebra generada, es té que

$$\mathrm{Sg}(X) \subseteq \mathrm{Sg}'(X).$$

D'altra banda, notem que si $m \geq n$, aleshores $E^n(X) \subseteq E^m(X)$. Així, podem demostrar per inducció, que $E^n(X) \subseteq \mathrm{Sg}(X)$, per a tot $n \in \mathbb{N}$.

Per a $n = 0$, $E^0(X) = X \subseteq \mathrm{Sg}(X)$.

Siga $n \geq 1$, suposem $E^m(X) \subseteq \mathrm{Sg}(X)$ per a tot $m \in n$. Així,

$$\begin{aligned} E^n(X) &= E\big(E^{n-1}(X)\big) \\ &= E^{n-1}(X) \cup \{\sigma^{\mathbf{A}}\big((x_i)_{i\in m}\big) \in A \mid m \in \mathbb{N},\ \sigma \in \Sigma_m, \\ &\quad (x_i)_{i\in m} \in \big(E^{n-1}(X)\big)^m\} \\ &\subseteq \mathrm{Sg}(X). \end{aligned}$$

Per tant, $E^n(X) \subseteq \mathrm{Sg}(X)$ per a tot $n \in \mathbb{N}$ i aleshores,

$$\mathrm{Sg}'(X) = \bigcup_{n\in\mathbb{N}} E^n(X) \subseteq \mathrm{Sg}(X).$$

En conclusió, $\mathrm{Sg}(X) = \mathrm{Sg}'(X)$. Per tant, $\mathrm{Sg} = \mathrm{Sg}'$. □

Aquesta construcció de l'operador de clausura Sg ens permet demostrar la següent proposició.

Proposició 3.22. *Donada* $\mathbf{A}$ *una* $\Sigma-$*àlgebra, aleshores el conjunt* $\mathrm{Sub}(\mathbf{A})$ *és un reticle algebraic per a l'ordre donat per la inclusió de subconjunts. El denotem per* $\mathbf{Sub}(\mathbf{A}) = \big(\mathrm{Sub}(\mathbf{A}), \subseteq\big)$.

Demostració. Començarem demostrant que es tracta d'un reticle complet. Pel Teorema 2.26, és suficient demostrar que existeix l'ínfim d'una família arbitrària de subàlgebres $\{\mathbf{B}_i \mid i \in I\} \subseteq \mathrm{Sub}(\mathbf{A})$.

Demostrarem en primer lloc que el conjunt $\bigcap_{i\in I} B_i$ està tancat per a les operacions de Σ. Siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $(b_j)_{j\in n} \in \big(\bigcap_{i\in I} B_i\big)^n$, aleshores per a cada $i \in I$, $(b_j)_{j\in n} \in (B_j)^n$. Com, per a cada $i \in I$, $\mathbf{B}_i$ és subàlgebra d'$\mathbf{A}$, es té que $\sigma^{\mathbf{A}}\big((b_j)_{j\in n}\big) \in B_i$. Així,

$$\sigma^{\mathbf{A}}\big((b_j)_{j\in n}\big) \in \bigcap_{i\in I} B_i,$$

és a dir, $\bigcap_{i\in I} B_i$ està tancat per a les operacions de Σ.

Així, $\bigcap_{i\in I}\mathbf{B}_i$ és una subàlgebra d'$\mathbf{A}$. A més, notem que per a cada $i\in I$, es té que $\bigcap_{i\in I}B_i\subseteq B_i$, és a dir, $\bigcap_{i\in I}B_i$ és una fita inferior de la família $\{\mathbf{B}_i\mid i\in I\}$. Anem a vore que $\bigcap_{i\in I}\mathbf{B}_i$ és la major de les fites inferiors.

Siga $\mathbf{Z}$ una subàlgebra d'$\mathbf{A}$ tal que, per a cada $i\in I$, $Z\subseteq B_i$. Aleshores $Z\subseteq\bigcap_{i\in I}B_i$. Concloem per tant que

$$\bigwedge_{i\in I}\mathbf{B}_i=\bigcap_{i\in I}\mathbf{B}_i.$$

Així, $\mathrm{Sub}(\mathbf{A})$ és un reticle complet.

A continuació demostrarem que les subàlgebres de la forma $\mathrm{Sg}(X)$ amb X finit són elements compactes. Suposem que $\mathrm{Sg}(X)\subseteq\bigvee\mathscr{A}$, amb $\mathscr{A}\subseteq\mathrm{Sub}(\mathbf{A})$. Com que X és finit, podem considerar $X=\{x_k\mid k\in m\}$. A més, com $X\subseteq\mathrm{Sg}(X)$, aleshores $\{x_k\mid k\in m\}\subseteq\bigvee\mathscr{A}$.

Així, per a cada $k\in m$, existeix un $\mathbf{B}_k\in\mathscr{A}$ de forma que $x_k\in\mathbf{B}_k$. Considerem

$$\mathscr{B}=\{\mathbf{B}_k\mid k\in m\}.$$

Notem que $\mathscr{B}\subseteq\mathscr{A}$ finit. Anem a comprovar que $\mathrm{Sg}(X)\subseteq\bigvee\mathscr{B}$.

Per a fer-ho, demostrarem que, si z és un element en $\mathrm{Sg}(X)$, aleshores $z\in\bigvee\mathscr{B}$. Per la Nota 3.21, sabem que $\mathrm{Sg}(X)=\bigcup_{r\in\mathbb{N}}E^r(X)$. Així, farem la demostració per inducció sobre r.

Estudiem primer el cas base, és a dir, suposem $z\in E^0(X)=X$. Així, existeix un $k\in m$ de forma que $z=x_k\in\mathbf{B}_k$. Com que $B\subseteq\bigvee\mathscr{B}$, es té que $z\in\mathscr{B}$.

Com a hipòtesi inductiva, suposem ara que l'enunciat és cert per a $z\in E^r(X)$ i anem a demostrar-ho per a $z\in E^{r+1}(X)$. Recordem que

$$E^{r+1}(X)=E\big(E^r(X)\big).$$

Així, si $z\in E^{r+1}(X)$, aleshores $z\in E^r(X)$ o $z=\sigma^{\mathbf{A}}\big((x_j)_{j\in n}\big)$ amb $n\in\mathbb{N}$, $\sigma\in\Sigma_n$ i $(x_j)_{j\in n}\in\big(E^r(X)\big)^n$.

Si $z\in E^r(X)$, aleshores per hipòtesi inductiva, $z\in\bigvee\mathscr{B}$.

Si $z=\sigma^{\mathbf{A}}\big((x_j)_{j\in n}\big)$, com per a cada $j\in n$, $x_j\in E^r(X)$, per hipòtesi inductiva es té que, per a cada $j\in n$, $x_j\in\bigvee\mathscr{B}$. Com $\bigvee\mathscr{B}$ és una subàlgebra d'$\mathbf{A}$, es té que $\bigvee\mathscr{B}$ és tancat per a les operacions de Σ. Així, $z=\sigma^{\mathbf{A}}\big((x_j)_{j\in n}\big)\in\bigvee\mathscr{B}$.

En qualsevol cas, $z\in\bigvee\mathscr{B}$ i per tant, $\mathrm{Sg}(X)$ amb X finit és un element compacte.

Per últim, hem de demostrar que $\mathrm{Sub}(\mathbf{A})$ és compactament generat. Per a fer-ho, demostrarem que, si $\mathbf{X}$ és una subàlgebra d'$\mathbf{A}$, aleshores

$$X=\bigvee\{\mathrm{Sg}(Y)\mid Y\subseteq X\text{ amb }Y\text{ finit}\}.$$

Pel resultat anterior, com que Y és finit, sabem que $\mathrm{Sg}(Y)$ és un element compacte.

D'una banda, com $\mathbf{X}$ és una subàlgebra d'$\mathbf{A}$, $\mathrm{Sg}(X) = X$. A més, com l'operador de clausura Sg és extensiu, si $Y \subseteq X$ amb Y finit, aleshores $\mathrm{Sg}(Y) \subseteq \mathrm{Sg}(X) = X$. Per tant,

$$\bigvee\{\mathrm{Sg}(Y) \mid Y \subseteq X \text{ amb } Y \text{ finit}\} \subseteq X.$$

D'altra banda, siga $z \in X$, notem que $\{z\}$ és finit i $z \in \mathrm{Sg}(\{z\})$. Així, $z \in \mathrm{Sg}(\{z\}) \subseteq \bigvee\{\mathrm{Sg}(Y) \mid Y \subseteq X \text{ amb } Y \text{ finit}\}$. Per tant,

$$X \subseteq \bigvee\{\mathrm{Sg}(Y) \mid Y \subseteq X \text{ amb } Y \text{ finit}\}.$$

Així, hem demostrat que tot element $\mathbf{X} \in \mathrm{Sub}(\mathbf{A})$ és el suprem d'elements compactes, és a dir, que $\mathrm{Sub}(\mathbf{A})$ és compactament generat. Com que $\mathrm{Sub}(\mathbf{A})$ és a més un reticle complet, hem demostrat que es tracta d'un reticle algebraic. □

NOTA 3.23. *Siguen $\mathbf{A}$ i $\mathbf{B}$ dues $\Sigma-$àlgebres. Notem que si $\mathbf{B} \leq \mathbf{A}$, aleshores l'aplicació inclusió*

$$\begin{array}{rccc} \mathrm{in}^{\mathbf{B},\mathbf{A}}: & \mathbf{B} & \longrightarrow & \mathbf{A} \\ & b & \longmapsto & b \end{array}$$

és un homomorfisme de $\Sigma-$àlgebres injectiu, ja que si $n \in \mathbb{N}, \sigma \in \Sigma_n$, $(b_i)_{i\in n} \in B^n$, es compleix

$$\mathrm{in}^{\mathbf{B},\mathbf{A}}\Big(\sigma^{\mathbf{B}}\big((b_i)_{i\in n}\big)\Big) = \sigma^{\mathbf{B}}\big((b_i)_{i\in n}\big) = \sigma^{\mathbf{A}}\big((b_i)_{i\in n}\big) = \sigma^{\mathbf{A}}\Big(\mathrm{in}^{\mathbf{B},\mathbf{A}}\big((b_i)\big)_{i\in n}\Big),$$

és a dir, $\mathrm{in}^{\mathbf{B},\mathbf{A}}$ és un homomorfisme, i és injectiva per la pròpia definició de l'aplicació.

Com que els $\Sigma-$homomorfismes es "porten bé" per a les operacions en àlgebres, és natural que siguen una ferramenta per a construir subàlgebres.

TEOREMA 3.24. *Siguen $\mathbf{A}$ i $\mathbf{B}$ dues $\mathbf{\Sigma}-$àlgebres i siga $f : \mathbf{A} \longrightarrow \mathbf{B}$ un homomorfisme. Aleshores $f[A]$ és un subconjunt de B tancat per a Σ, on $f[A] = \{f(a) \in B \mid a \in A\}$. Denotarem per $f[\mathbf{A}]$ a l'estructura de subàlgebra de $f[A]$ en $\mathbf{B}$.*

DEMOSTRACIÓ. Anem a veure que es compleixen les condicions de la Definició 3.17. En primer lloc, és clar que

$$f[A] = \{f(a) \in B \ \mid \ a \in A\} \subseteq B.$$

A més, si $n \in \mathbb{N}, \sigma \in \Sigma_n$, $(z_i)_{i\in n} \in f[A]^n$ aleshores existeix una família $(a_i)_{i\in n} \in A^n$ tal que $(z_i)_{i\in n} = \big(f(a_i)\big)_{i\in n}$. Així, tenint en compte que f

és un $\Sigma-$homomorfisme, tenim que

$$\sigma^{\mathbf{B}}\big((z_i)_{i\in n}\big) = \sigma^{\mathbf{B}}\Big(\big(f(a_i)\big)_{i\in n}\Big) = f\Big(\sigma^{\mathbf{A}}\big((a_i)\big)_{i\in n}\Big) \in f[A].$$

Per tant, $f[A]$ és un subconjunt tancat de $\mathbf{B}$. □

3. Congruències i Àlgebra Quocient

Com ja sabem, els subgrups normals juguen un paper fonamental en la definició de grups quocients i en els anomenats teoremes d'isomorfia de grups. Els ideals, introduïts en la segona meitat del segle passat per Dedekind, juguen un paper anàleg en la definició d'anells quocients, i en els corresponents teoremes d'isomorfia en la teoria d'anells. Donada una situació tan paral·lela, era inevitable que els matemàtics buscaren una formulació comuna general. En aquestes dues seccions, s'observarà que les congruències formen el concepte unificador i, alhora, proporcionen un altre punt d'encontre per a la teoria dels reticles i l'àlgebra universal [**10**].

Els conceptes de congruència, àlgebra quocient i homomorfisme estan estretament relacionats i tenen una rellevància fonamental en l'àmbit de les matemàtiques. En aquesta secció, primer introduirem les nocions de congruència i àlgebra quocient. A més, estudiarem l'-homomorfisme de projecció al quocient. Posteriorment, analitzarem detalladament el conjunt de congruències d'una àlgebra $\mathbf{A}$, amb l'objectiu de demostrar que aquest conjunt, denotat com a $\mathrm{Con}(\mathbf{A})$, és un reticle algebraic per a l'ordre dotat per la inclusió. Aquesta propietat és de particular interès i esdevé un aspecte clau en l'estudi de les congruències en àlgebres.

Definició 3.25. *Siga $\mathbf{A}$ una $\Sigma-$àlgebra, una relació $\theta \subseteq A \times A$ es diu* **congruència** *si θ és una relació d'equivalència i a més, per a tot $n \in \mathbb{N} - \{0\}$, i per a tot símbol d'operació $\sigma \in \Sigma_n$, si $(a_i)_{i\in n}$, $(b_i)_{i\in n} \in A^n$ són famílies tals que, per a tot $i \in n$, $(a_i, b_i) \in \theta$ aleshores*

$$\big(\sigma^{\mathbf{A}}((a_i)_{i\in n}), \sigma^{\mathbf{A}}((b_i)_{i\in n})\big) \in \theta.$$

Denotem per $\mathrm{Con}(\mathbf{A})$ *al conjunt de totes les congruències sobre $\mathbf{A}$. Notem que* $\mathrm{Con}(\mathbf{A}) \subseteq \mathrm{Eqv}(\mathbf{A})$.

Introduïm un exemple de congruència en $\mathbb{Z}$ que és àmpliament utilitzada en diverses àrees de les matemàtiques: la congruència mòdul n en la que dos nombres enters estan relacionats quan la seua diferència és divisible per n.

EXEMPLE 3.26. *Per a l'anell d'enters* $\big(\mathbb{Z}, +, \cdot, 0, 1\big)$ *i per a* $n \in \mathbb{N}$, *estudiem la congruència mòdul* n *en* $\mathbb{Z}$, *donada per*

$$a \equiv b \text{ mòd } n \text{ si, i només si, } n|(a-b).$$

En primer lloc, demostrarem que es tracta d'una relació d'equivalència, és a dir, que satisfà les propietats reflexiva, simètrica i transitiva enunciades a la Definició 2.32.

Siga $a \in \mathbb{Z}$, *es compleix la propietat reflexiva*

$$a \equiv a \text{ mòd } n,$$

ja que $n|(a-a) = 0$.

A més, siguen $a, b \in \mathbb{Z}$ *tals que* $a \equiv b$ *mòd* n, *aleshores* $n|(a-b)$, *és a dir, existeix* $k \in \mathbb{Z}$ *tal que* $a - b = kn$. *Així,* $b - a = -kn$ *amb* $-k \in \mathbb{Z}$ *i per tant,* $n|(b-a)$, *és a dir,*

$$b \equiv a \text{ mòd } n.$$

Açò demostra que se satisfà la propietat simètrica.

Per últim, siguen $a, b, c \in \mathbb{Z}$, *tals que* $a \equiv b$ *mòd* n *i* $b \equiv c$ *mòd* n. *Aleshores existeixen respectivament* $k_1, k_2 \in \mathbb{Z}$ *tals que* $a - b = k_1 n$ *i* $b - c = k_2 n$. *Així,* $a - c = (a-b) + (b-c) = k_1 n + k_2 n = (k_1 + k_2)n$, *i per tant*

$$a \equiv c \text{ mòd } n,$$

és a dir, es compleix la propietat transitiva.

En segon lloc, veurem la compatibilitat de la relació amb la suma i el producte. Siguen $a, b, c, d \in \mathbb{Z}$ *tals que* $a \equiv b$ *mòd* n *i* $c \equiv d$ *mòd* n, *aleshores existeixen* $k_1, k_2 \in \mathbb{Z}$ *tals que* $a - b = k_1 n$ *i* $b - c = k_2 n$.

Si considerem l'operació suma, notem que

$$(a+c) - (b+d) = (a-b) + (c-d) = k_1 n + k_2 n = (k_1 + k_2)n.$$

Per tant $(a+c) \equiv (b+d)$ *mòd* n.

Si considerem ara l'operació producte, com que $a = k_1 n + b$ *i* $c = k_2 n + d$, *tenim que*

$$ac = (k_1 n + b)(k_2 n + d) = (k_1 k_2 n + d k_1 + b k_2)n + bd.$$

Per tant, $ac - bd = (k_1 k_2 n + d k_1 + b k_2)n$, *és a dir,* $(ac) \equiv (bd)$ *mòd* n. *Concloem per tant que es tracta d'una congruència. A més, notem que aquesta relació de congruència forma una partició de l'anell* $\mathbb{Z}$ *en classes d'equivalència, on cada classe conté tots els elements de* $\mathbb{Z}$ *que són congruents entre si mòdul* n.

Per tant, el conjunt quocient estarà format per totes les classes d'equivalència, és a dir, pels conjunts de nombres enters que són congruents entre si mòdul n.

Com que les congruències són compatibles per a les operacions de les àlgebres, aquesta condició ens permet introduir una estructura algebraica en el conjunt de les classes d'equivalència heretada de l'àlgebra de partida.

DEFINICIÓ 3.27. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* $\theta \in \mathrm{Con}(\mathbf{A})$*, el conjunt quocient*

$$\mathbf{A}/\theta = \{[a]_\theta \mid a \in A\}$$

té estructura de $\Sigma-$*àlgebra, amb la interpretació de les operacions següent; si* $n \in \mathbb{N}$*,* $\sigma \in \Sigma_n$ *i* $([a_i]_\theta)_{i\in n}$ *una família de classes en* $(A/\theta)^n$*, definim el resultat de fer l'operació* σ *sobre la família com*

$$\sigma^{\mathbf{A}/\theta}\big(([a_i]_\theta)_{i\in n}\big) = \big[\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big)\big]_\theta.$$

Anomenem $\mathbf{A}/\theta$ *a l'***estructura quocient d'A per** θ**.**

Presentem a continuació un exemple que ens permeteix comprendre la relació entre subgrups normals i congruències en un grup.

EXEMPLE 3.28. *Siga* $\mathbf{G}$ *un grup i* N *un subgrup normal de* G*, és a dir, un subgrup tal que per a tot* $g \in G$ *es té que* $gN = Ng$*. Aleshores, per a tot* $x, y \in G$ *la relació binària*

$$(x, y) \in \theta \text{ si, i només si, } xy^{-1} \in N$$

és una congruència en G*. A més notem que* $[1]_\theta = N$*.*

Recíprocament, siga θ *una congruència sobre* $\mathbf{G}$ *i siguen* $x, y \in G$*, notem que*

$$(x, y) \in \theta \text{ si, i només si, } xy^{-1} \in [1]_\theta.$$

Així, $[1]_\theta$ *és una subàlgebra que forma un subgrup normal de* $\mathbf{G}$

Aquesta correspondència entre subgrups normals i congruències en un grup posa de manifest que la noció de congruència representa una generalització de la noció de subgrup normal. A més, a través d'aquesta relació, s'evidencia la importància de les congruències com a eines per a comprendre les propietats i les estructures dels grups.

Siga $\mathbf{A}$ una $\Sigma-$àlgebra i $\theta \in \mathrm{Con}(\mathbf{A})$, vegem ara un homomorfisme que sempre trobem entre $\mathbf{A}$ i l'algebra quocient $\mathbf{A}/\theta$.

PROPOSICIÓ 3.29. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* $\theta \in \mathrm{Con}(\mathbf{A})$*, aleshores l'aplicació projecció al quocient, que envia cada element d'A a la seua classe respecte* θ*,*

$$\begin{array}{rccc} \mathrm{pr}^\theta : & \mathbf{A} & \longrightarrow & \mathbf{A}/\theta \\ & a & \longmapsto & [a]_\theta \end{array}$$

és un epimorfisme de $\Sigma-$*àlgebres.*

DEMOSTRACIÓ. Siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $([a_i]_\theta)_{i\in n}$ una família en $(A/\theta)^n$, aleshores

$$\begin{aligned} \mathrm{pr}^\theta\big(\sigma^{\mathbf{A}}((a_i)_{i\in n})\big) &= \big[\sigma^{\mathbf{A}}\big((a_i)\big)_{i\in n}\big]_\theta && \text{(Def. } \mathrm{pr}^\theta) \\ &= \sigma^{\mathbf{A}/\theta}\big(([a_i]_\theta)_{i\in n}\big) && \text{(Def. } A/\theta) \\ &= \sigma^{\mathbf{A}/\theta}\big((\mathrm{pr}^\theta(a_i))_{i\in n}\big). && \text{(Def. } \mathrm{pr}^\theta) \end{aligned}$$

Així, pr^θ és un $\Sigma-$homomorfisme.

A més, siga $[a]_\theta \in A/\theta$, és clar que $a \in A$ i $\mathrm{pr}^\theta(a) = [a]_\theta$. És a dir, pr^θ és sobrejectiva i, per tant, es tracta d'un epimorfisme. □

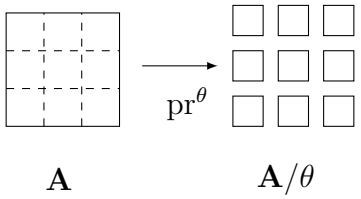

FIGURA 3.1. Projecció al quocient.

A la Figura 3.1 observem com funciona l'aplicació pr^θ*. A la dreta tenim l'àlgebra* $\mathbf{A}$*, dividida en diferents seccions mitjançant línies discontínues. Aquestes seccions representen els elements d'*A *que estan relacionats entre ells a través de la congruència* θ*, obtenint així una partició d'*A*. L'aplicació* pr^θ *envia cada element a la seua classe d'equivalència, obtenint com a imatge de l'aplicació el conjunt quocient* $\mathbf{A}/\theta$*.*

Estudiarem ara l'estructura de reticle de $\mathrm{Con}(\mathbf{A})$.

PROPOSICIÓ 3.30. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra,* $\big(\mathrm{Con}(\mathbf{A}), \subseteq\big)$ *és un subreticle complet de* $\big(\mathrm{Eqv}(\mathbf{A}), \subseteq\big)$*.*

DEMOSTRACIÓ. Pel Teorema 2.38 sabem que $\big(\mathrm{Eqv}(\mathbf{A}), \subseteq\big)$ és un reticle complet, amb el suprem i l'ínfim de dues relacions d'equivalència R i S definits per, $R \vee S$ i $R \cap S$ respectivament.

Tenint en compte la Definició 2.29, per demostrar que $\mathrm{Con}(\mathbf{A})$ és un subreticle complet hem de comprovar que aquest és tancat per a la intersecció i la unió arbitraria de congruències.

Siga $(\theta_i)_{i\in I}$ una família de congruències en $\mathrm{Con}(\mathbf{A})$ i siguen $n \in \mathbb{N} - \{0\}$, $\sigma \in \Sigma_n$ i $(a_j)_{j\in n}$, $(b_j)_{j\in n} \in A^n$.

Començarem treballant amb la intersecció arbitrària. Si suposem que per a tot $j \in n$ es té que

$$(a_j, b_j) \in \bigcap_{i \in I} \theta_i,$$

aleshores se satisfà que per a tot $j \in n$ i, per a tot $i \in I$, $(a_j, b_j) \in \theta_i$. Com que, per a tot $i \in I$, θ_i és una congruència, aleshores,

$$\Big(\sigma^{\mathbf{A}}\big((a_j)_{j\in n}\big), \sigma^{\mathbf{A}}\big((b_j)_{j\in n}\big)\Big) \in \theta_i.$$

Per tant,

$$\Big(\sigma^{\mathbf{A}}\big((a_j)_{j\in n}\big), \sigma^{\mathbf{A}}\big((b_j)_{j\in n}\big)\Big) \in \bigcap_{i \in I} \theta_i.$$

Suposem ara que per a tot $j \in n$ es té que

$$(a_j, b_j) \in \bigvee_{i \in I} \theta_i,$$

amb $\bigvee$ definit com en la Nota 2.36. Aleshores per a cada $j \in n$ existeix un camí en $\bigcup_{i\in I} \theta_i$ que va de a_j a b_j. És a dir, per a cada $j \in n$ existeixen $j_0, \ldots, j_k \in I$ tals que

$$(a_j, b_j) \in \theta_{j_0} \circ \theta_{j_1} \circ \cdots \circ \theta_{j_k}.$$

Com que θ_i són congruències, llavors per a tot $i \in I$

$$\Big(\sigma^{\mathbf{A}}\big((a_j)_{j\in n}\big), \sigma^{\mathbf{A}}\big((b_j)_{j\in n}\big)\Big) \in \theta_i.$$

Per tant, en particular

$$\Big(\sigma^{\mathbf{A}}\big((a_j)_{j\in n}\big), \sigma^{\mathbf{A}}\big((b_j)_{j\in n}\big)\Big) \in \theta_{j_0} \circ \theta_{j_1} \circ \cdots \circ \theta_{j_k}.$$

Per tant, $\bigvee_{i\in I} \theta_i$ és una relació de congruència en $\mathbf{A}$.

Concloem així que $\big(\mathrm{Con}(\mathbf{A}), \subseteq\big)$ és un subreticle complet. □

Una volta demostrat que és complet, anem a demostrar que es tracta d'un reticle algebraic. Per a fer-ho, definirem en $A \times A$ un operador clausura que ens permetrà treballar millor amb els elements compactes de $\mathrm{Con}(\mathbf{A})$, basant-nos en [**12**].

TEOREMA 3.31. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra, aleshores existeix un operador de clausura algebraic* Cg *en* $A \times A$ *tal que els subconjunts tancats d'*$A \times A$ *són les congruències en* $\mathbf{A}$.

DEMOSTRACIÓ. En primer lloc, establirem una estructura algebraica apropiada en $A \times A$.

Siga $n \in \mathbb{N}$, $(a_i)_{i\in n}, (b_i)_{i\in n} \in A^n$, per a cada símbol d'operació $n-$àri $\sigma \in \Sigma_n$ definit en $\mathbf{A}$, definim la corresponent operació en $A \times A$ com

$$\sigma^{\mathbf{A}\times\mathbf{A}}\Big((a_i, b_i)_{i\in n}\Big) = \Big(\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big), \sigma^{\mathbf{A}}\big((b_i)_{i\in n}\big)\Big). \tag{5}$$

A més, afegim l'operació constant (a, a) per a cada $a \in A$, l'operació $1-$ària S definida per

$$S\big(a, b\big) = (b, a),$$

i l'operació $2-$ària T definida per

$$T\big((a, b), (c, d)\big) = \begin{cases} (a, d) & \text{si } b = c; \\ (a, b) & \text{si } b \neq c. \end{cases}$$

Així, si considerem Σ' la nova signatura amb les operacions que hem afegit, $\mathbf{A} \times \mathbf{A}$ és una $\Sigma'-$àlgebra.

En segon lloc, anem a demostrar que $\mathbf{B}$ és una subàlgebra de l'algebra $\mathbf{A} \times \mathbf{A}$ si, i només si, $\mathbf{B}$ és una congruència en $\mathbf{A}$.

D'una banda, si suposem que $\mathbf{B}$ és una subàlgebra d'$\mathbf{A} \times \mathbf{A}$, aleshores $B \subseteq A \times A$ i per a tot $n \in \mathbb{N}$ i per a tot $\sigma \in \Sigma_n^{'}$ si $\big(b_i, b_i^{'}\big)_{i\in n} \in B^n$, llavors

$$\sigma^{\mathbf{A}\times\mathbf{A}}\Big(\big(b_i, b_i^{'}\big)_{i\in n}\Big) \in B. \tag{6}$$

Per com hem definit la $\mathbf{\Sigma'}$-àlgebra, notem que per a tot $b \in A$, $(b, b) \in B$, satisfent així la propietat reflexiva. A més, siguen $a, b \in A$ tals que $(a, b) \in B$, aleshores $S\big(a, b\big) = (b, a) \in B$, demostrant que se satisfà la propietat simètrica. Per últim, siguen $a, b, c \in A$ tals que $(a, b), (b, c) \in B$, aleshores $T\big((a, b), (b, c)\big) = (a, c) \in B$.

És a dir, B és una relació d'equivalència sobre A. Falta demostrar que és una congruència.

Siga $n \in \mathbb{N} - \{0\}$ i siga $\sigma \in \Sigma_n$, si $(a_i)_{i\in n}, (b_i)_{i\in n} \in A^n$ són famílies tals que per a tot $i \in n$ $(a_i, b_i) \in B$, aleshores

$$\begin{aligned} \big(\sigma^{\mathbf{A}}((a_i)_{i\in n}), \sigma^{\mathbf{A}}((b_i)_{i\in n})\big) &= \sigma^{\mathbf{A}\times\mathbf{A}}\Big(\big(a_i, b_i\big)_{i\in n}\Big) && \text{(per (5))} \\ &= \sigma^{\mathbf{B}}\Big(\big(a_i, b_i\big)_{i\in n}\Big) \in B. && \text{(per (6))} \end{aligned}$$

Per tant, tota subàlgebra d'$\mathbf{A} \times \mathbf{A}$ és una congruència en $\mathbf{A}$.

D'altra banda, suposem ara que $\mathbf{B}$ és una congruència en $\mathbf{A}$. Aleshores B és una relació d'equivalència, $B \subseteq A \times A$ i a més, per a tot $n \in \mathbb{N}-\{0\}$ i per a tot símbol d'operació $\sigma \in \Sigma_n$, si $(a_i)_{i\in n}$, $(b_i)_{i\in n} \in A^n$ són famílies tals que per a tot $i \in n$, $(a_i, b_i) \in B$ aleshores

$$\big(\sigma^{\mathbf{A}}((a_i)_{i\in n}), \sigma^{\mathbf{A}}((b_i)_{i\in n})\big) \in B.$$

Per tant, siga $n \in \mathbb{N} - \{0\}$, per als $\sigma \in \Sigma_n \cap \Sigma'_n$, si $\big(a_i, b_i\big)_{i\in n} \in B^n$, aleshores

$$\begin{aligned}\big(\sigma^{\mathbf{A}}((a_i)_{i\in n}), \sigma^{\mathbf{A}}((b_i)_{i\in n})\big) &= \sigma^{\mathbf{A}\times\mathbf{A}}\Big(\big(a_i, b_i\big)_{i\in n}\Big) \\ &= \sigma^{\mathbf{B}}\Big(\big(a_i, b_i\big)_{i\in n}\Big).\end{aligned}$$

A més, com que B satisfà les propietats reflexiva, simètrica i transitiva per ser relació d'equivalència, és clar que siguen que $a, b, c \in A$ tals que $(a, b), (b, c) \in B$, aleshores

$$(a, a) \in B,\ S\big(a, b\big) = (b, a) \in B,\ \text{i } \mathrm{T}\big((\mathrm{a}, \mathrm{b}), (\mathrm{b}, \mathrm{c})\big) = (\mathrm{a}, \mathrm{c}) \in \mathrm{B}.$$

És a dir, B està tancat per a les operacions de Σ' i per tant és una subàlgebra d'$\mathbf{A} \times \mathbf{A}$.

Per últim, si considerem $\mathrm{Cg} = \mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}$, aleshores Cg és un operador de clausura algebraic en $\mathbf{A} \times \mathbf{A}$. Així, els subconjunts tancats d'$A \times A$, que són de la forma $B = \mathrm{Cg}(B)$ son subàlgebres d'$\mathbf{A} \times \mathbf{A}$ i per tant, són congruències en $\mathbf{A}$. □

Corol·lari 3.32. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra, aleshores el conjunt* $\mathrm{Con}(\mathbf{A})$ *és un reticle algebraic per a l'ordre donat per la inclusió de subconjunts. El denotem per* $\mathrm{Con}(\mathbf{A}) = \big(\mathrm{Con}(\mathbf{A}), \subseteq\big)$.

Demostració. Per la Proposició 3.22 i el Teorema 3.31. □

4. Teoremes d'Isomorfia

Els teoremes d'isomorfia són resultats fonamentals en l'àmbit de les àlgebres, que ens permeten identificar unes certes propietats i estructures d'una àlgebra mitjançant la construcció d'isomorfismes amb altres àlgebres conegudes. Això proporciona una manera de relacionar i comparar les propietats de les àlgebres, permetent-nos establir connexions significatives entre elles.

Dividirem la secció en quatre subapartats. Els tres primers els dedicarem cadascun a un teorema d'isomorfia, enunciant i demostrant els resultats previs necessaris. L'últim apartat el dedicarem al Teorema de Correspondència.

4.1. Primer Teorema d'Isomorfia.

Teorema 3.33. *Siguen* $\mathbf{A}, \mathbf{B}$ *dues* $\Sigma-$*àlgebres i* $f : \mathbf{A} \longrightarrow \mathbf{B}$ *un homomorfisme.*

(1) *La imatge de* f *és una subàlgebra de* $\mathbf{B}$*, on*

$$\mathrm{Im}(f) = \{f(a) \in B \mid a \in A\}.$$

(2) *El nucli de f és una congruència en $\mathbf{A}$, on*

$$\mathrm{Ker}(f) = \{(a, a') \in A \times A \mid f(a) = f(a')\}.$$

(3) $\mathrm{in}^{\mathrm{Im}(f)} : \mathrm{Im}(f) \longrightarrow \mathbf{B}$ *és un homomorfisme injectiu.*
(4) $\mathrm{pr}^{\mathrm{Ker}(f)} : \mathbf{A} \longrightarrow \mathbf{A}/\mathrm{Ker}(f)$ *és un homomorfisme sobrejectiu.*

Demostració. En primer lloc, anem a demostrar (1). D'una banda, és clar que

$$\mathrm{Im}(f) \subseteq B.$$

D'altra banda, siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $\big(f(a_i)\big)_{i\in n}$ una família d'n elements en $\mathrm{Im}(f)^n$. Aleshores, per la Definició 3.14 sabem que

$$\sigma^{\mathbf{B}}\big((f(a_i))_{i\in n}\big) = f\big(\sigma^{\mathbf{A}}((a_i)_{i\in n})\big) \in \mathrm{Im}(f).$$

Per tant, $\mathrm{Im}(f)$ és un subconjunt tancat de $\mathbf{B}$.

Demostrem ara (2). Per a fer-ho, primer hem de comprovar que $\mathrm{Ker}(f)$ és una relació d'equivalència.

Siga $a \in A$, és clar que $f(a) = f(a)$ i per tant, $(a, a) \in \mathrm{Ker}(f)$. És a dir, se satisfà la propietat reflexiva.

Anem a treballar ara amb la propietat simètrica. Siguen $a, a' \in A$ tals que $(a, a') \in \mathrm{Ker}(f)$, aleshores $f(a) = f(a')$. Així, $f(a') = f(a)$ i llavors $(a', a) \in \mathrm{Ker}(f)$.

Per últim, demostrem la transitivitat. Siguen $a, b, c \in A$ tals que $(a, b), (b, c) \in \mathrm{Ker}(f)$, aleshores $f(a) = f(b)$ i $f(b) = f(c)$. Per tant, $f(a) = f(c)$, i així $(a, c) \in \mathrm{Ker}(f)$.

Açò demostra que $\mathrm{Ker}(f)$ és una relació d'equivalència.

Ara, siga $n \in \mathbb{N}-\{0\}$, $\sigma \in \Sigma_n$ i $\big((a_i, a_i')\big)_{i\in n}$ una família de n parelles en $\mathrm{Ker}(f)^n$. Notem que, per a cada $i \in n$, es té que $f(a_i) = f(a_i')$. Així, tenint en compte la Definició 3.14, notem:

$$\begin{aligned} f\Big(\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big)\Big) &= \sigma^{\mathbf{B}}\Big(\big(f(a_i)\big)_{i\in n}\Big) \\ &= \sigma^{\mathbf{B}}\Big(\big(f(a_i')\big)_{i\in n}\Big) \\ &= f\Big(\sigma^{\mathbf{A}}\big((a_i')_{i\in n}\big)\Big). \end{aligned}$$

Concloem doncs que

$$\Big(\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big), \sigma^{\mathbf{A}}\big((a_i')_{i\in n}\big)\Big) \in \mathrm{Ker}(f),$$

i per tant $\mathrm{Ker}(f)$ és una congruència.

L'apartat (3) està demostrat en la Proposició 3.23. Denotarem per $\mathbf{Im}(f)$ a l'estructura de subàlgebra associada a $\mathrm{Im}(f)$.

L'apartat (4) està demostrat en la Proposició 3.29. Denotarem per $\mathbf{A}/\mathrm{Ker}(f)$ a l'estructura d'àlgebra quocient associada a $\mathrm{Ker}(f)$.

Açò demostra el Teorema 3.33. □

En aquest punt, anem a enunciar i demostrar el primer teorema d'isomorfia.

TEOREMA 3.34 (Primer Teorema d'Isomorfia). *Siguen* $\mathbf{A}, \mathbf{B}$ *dos* $\Sigma-$*àlgebres i* $f : \mathbf{A} \longrightarrow \mathbf{B}$ *un* $\Sigma-$*homomorfisme. Aleshores*

$$\mathbf{A}/\mathrm{Ker}(f) \cong \mathbf{Im}(f).$$

DEMOSTRACIÓ. En primer lloc, considerem l'aplicació

$$\begin{array}{rccc} f^b: & A/\mathrm{Ker}(f) & \longrightarrow & \mathrm{Im}(f) \\ & [a]_{\mathrm{Ker}(f)} & \longmapsto & f(a). \end{array}$$

Notem que, per com hem definit l'aplicació, $[a]_{\mathrm{Ker}(f)} = [a']_{\mathrm{Ker}(f)}$ si, i només si, $f(a) = f(a')$. Per tant, f^b està ben definida i és injectiva.

A més, siga $b \in \mathrm{Im}(f) = \{f(a) \in B \mid a \in A\}$, és clar que existeix $a \in A$ tal que $f(a) = b$. Així, si considerem la seua classe d'equivalència respecte a la congruència $\mathrm{Ker}(f)$,

$$[a]_{\mathrm{Ker}(f)} = \{a' \in A \mid f(a) = f(a')\},$$

tenim que

$$f^b([a]_{\mathrm{Ker}(f)}) = f(a).$$

Així, f^b és sobrejectiva i, per tant, bijectiva.

Només queda demostrar que es tracta d'un $\Sigma-$homomorfisme. Siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $\left([a_i]_{\mathrm{Ker}(f)}\right)_{i\in n}$ una família de n tuples en $\left(A/\mathrm{Ker}(f)\right)^n$. Tenint en compte que f és un homomorfisme per hipòtesi, la Definició 3.27 i com hem definit l'aplicació f^b, notem que

$$\begin{aligned} f^b\Big(\sigma^{\mathbf{A}/\mathrm{Ker}(f)}\big(([a_i]_{\mathrm{Ker}(f)})_{i\in n}\big)\Big) &= f^b\Big(\big[\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big)\big]_{\mathrm{Ker}(f)}\Big) \\ &= f\Big(\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big)\Big) \\ &= \sigma^{\mathbf{B}}\Big(\big(f(a_i)\big)_{i\in n}\Big) \\ &= \sigma^{\mathbf{Im}(f)}\Big(\big(f(a_i)\big)_{i\in n}\Big) \\ &= \sigma^{\mathbf{Im}(f)}\Big(\big(f^b([a_i]_{\mathrm{Ker}(f)})\big)_{i\in n}\Big). \end{aligned}$$

Per tant, f^b és un isomorfisme i $\mathbf{A}/\mathrm{Ker}(f) \cong \mathbf{Im}(f)$. □

Com podem veure a la Figura 4.1, l'aplicació f *crea una partició d'*$\mathbf{A}$ *amb els elements que van a la mateixa imatge, és a dir, ens dòna la congruència* $\mathrm{Ker}(f)$. *Així, podem considerar l'aplicació projecció al*

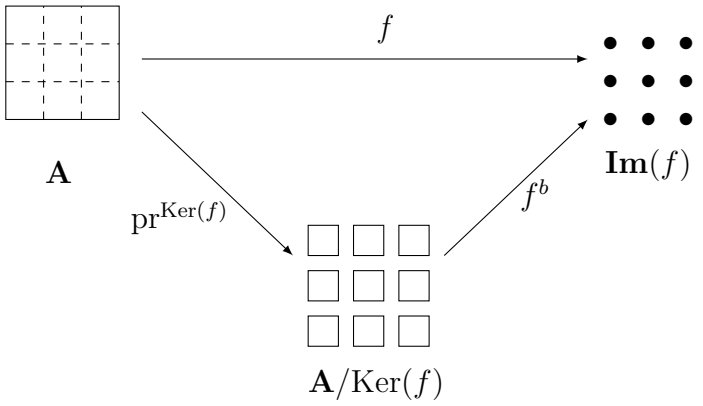

FIGURA 4.1. El Primer Teorema d'Isomorfia.

quocient, explicada la Figura 3.1, per treballar amb l'estructura quocient $\mathbf{A}/\mathrm{Ker}(f)$. *Per tant, és clar que podem trobar un isomorfisme* f^b *que porta cada classe d'equivalència en l'estructura quocient a la seua imatge per* f.

La importància d'aquest teorema és que ens permet comprendre l'estructura del quocient d'una àlgebra pel seu nucli a través de l'estudi de la imatge d'un homomorfisme. Així, es tracta d'una eina poderosa per a analitzar i simplificar estructures algebraiques.

Observem que com f pot no ser sobrejectiva, l'isomorfisme va només a $\mathrm{Im}(f)$. No obstant això, treballant amb l'aplicació $\mathrm{in}^{\mathrm{Im}(f)}$, tenim el següent resultat.

COROL·LARI 3.35. *En les condicions del Teorema 3.34, el diagrama de conjunts de la Figura 4.2 commuta*

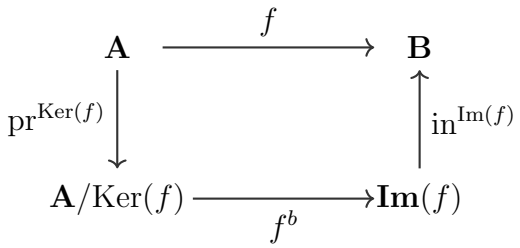

FIGURA 4.2. Corol·lari 3.35.

4.2. Segon Teorema d'Isomorfia. El segon teorema d'isomorfia estableix que, donades dues congruències sobre un àlgebra, una menor

que l'altra, el quocient de l'àlgebra per la congruència menor entre el quocient de les congruències és isomorf al quocient de l'àlgebra per la congruència major. Per demostrar-ho, començarem introduint els següents conceptes previs.

PROPOSICIÓ 3.36. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* θ, ϕ *dues congruències en* $\mathbf{A}$ *tals que* $\theta \subseteq \phi$. *Aleshores l'aplicació*

$$\begin{array}{rccc} \varphi: & \mathbf{A}/\theta & \longrightarrow & \mathbf{A}/\phi \\ & [a]_\theta & \longmapsto & [a]_\phi \end{array}$$

és un $\Sigma-$*homomorfisme sobrejectiu.*

DEMOSTRACIÓ. En primer lloc, notem que l'aplicació φ està ben definida perquè, com $\theta \subseteq \phi$, si $a, b \in A$ són tals que $(a, b) \in \theta$, aleshores $(a, b) \in \phi$.

Vegem que φ és un $\Sigma-$homomorfisme. Siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $\big([a_i]_\theta\big)_{i\in n} \in \big(A/\theta\big)^n$. Tenint en compte com hem definit l'aplicació φ i la Definició 3.27 d'estructura quocient, aleshores

$$\begin{aligned} \varphi\Big(\sigma^{\mathbf{A}/\theta}\big(([a_i]_\theta)_{i\in n}\big)\Big) &= \varphi\Big(\big[\sigma^{\mathbf{A}}\big((a_i)_{i\in n}\big)\big]_\theta\Big) \\ &= \Big[\sigma^{\mathbf{A}}\Big((a_i)_{i\in n}\Big)\Big]_\phi \\ &= \sigma^{\mathbf{A}/\phi}\Big(\big([a_i]_\phi\big)_{i\in n}\Big) \\ &= \sigma^{\mathbf{A}/\phi}\Big(\big(\varphi([a_i]_\theta)\big)_{i\in n}\Big). \end{aligned}$$

Per últim, vegem que és sobrejectiva.

Si $[a]_\phi$ és un element de A/ϕ, aleshores per a la classe $[a]_\theta$ es té que $\varphi\big([a]_\theta\big) = [a]_\phi$. En particular, φ és un epimorfisme i $\mathbf{Im}(\varphi) = \mathbf{A}/\phi$. □

DEFINICIÓ 3.37. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* θ, ϕ *dues congruències en* $\mathbf{A}$ *tals que* $\theta \subseteq \phi$. *Si considerem el* $\Sigma-$*homomorfisme de la Proposició 3.36*

$$\begin{array}{rccc} \varphi: & \mathbf{A}/\theta & \longrightarrow & \mathbf{A}/\phi \\ & [a]_\theta & \longmapsto & [a]_\phi \end{array}$$

aleshores denotem per ϕ/θ *al nucli de* φ. *Notem que*

$$\begin{aligned} \phi/\theta &= \mathrm{Ker}(\varphi) \\ &= \{\big([a]_\theta, [a']_\theta\big) \in A/\theta \times A/\theta \mid \varphi([a]_\theta) = \varphi([a']_\theta)\} \\ &= \{\big([a]_\theta, [a']_\theta\big) \in A/\theta \times A/\theta \mid (a, a') \in \phi\}. \end{aligned}$$

En aquest punt, anem a enunciar i demostrar el Segon Teorema d'Isomorfia.

TEOREMA 3.38 (Segon Teorema d'Isomorfia). *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* θ, ϕ *dues congruències en* $\mathbf{A}$ *tals que* $\theta \subseteq \phi$. *Aleshores*

$$\big(\mathbf{A}/\theta\big)/\big(\phi/\theta\big) \cong \mathbf{A}/\phi.$$

DEMOSTRACIÓ. Per la Proposició 3.36, sabem que φ és un epimorfisme i per tant,

$$\mathbf{Im}(\varphi) = \mathbf{A}/\phi.$$

Pel Primer Teorema d'Isomorfia, Teorema 3.34, sabem que

$$\big(\mathbf{A}/\theta\big)/\mathrm{Ker}(\varphi) \cong \mathbf{Im}(\varphi).$$

Tenint en compte que φ és sobrejectiva i la Definició 3.37, en efecte obtenim que

$$\big(\mathbf{A}/\theta\big)/\big(\phi/\theta\big) \cong \mathbf{A}/\phi.$$

Açò conclou la demostració del Segon Teorema d'Isomorfia. □

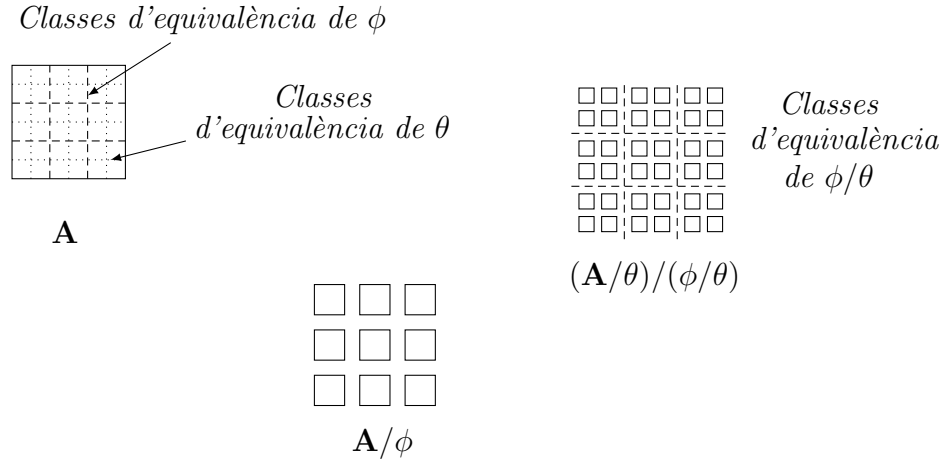

FIGURA 4.3. El Segon Teorema d'Isomorfia

Com podem veure a la Figura 4.3, en primer lloc tenim a l'esquerra l'àlgebra $\mathbf{A}$ *amb les particions degudes a la congruència* ϕ *assenyalades amb una línia discontinua i les degudes a la congruència* θ *marcades amb una línia de punts. Després, en mig tenim el conjunt quocient* $\mathbf{A}/\phi$, *format per les classes d'equivalència que genera la congruència* ϕ *sobre* $\mathbf{A}$. *Per últim, a la dreta tenim el conjunt quocient* $(\mathbf{A}/\theta)/(\phi/\theta)$ *que agrupa les classes degudes a la congruència* θ *que es troben dins de la mateixa classe respecte a la congruència* ϕ.

El Segon Teorema d'Isomorfia demostra que els quocients $\mathbf{A}/\phi$ *i* $(\mathbf{A}/\theta)/(\phi/\theta)$ *són isomorfs.*

4.3. Tercer Teorema d'Isomorfia. En primer lloc treballarem amb la noció de saturació d'un conjunt.

DEFINICIÓ 3.39. *Siga A un conjunt i θ una relació d'equivalència en A. Siga $B \subseteq A$, definim la* **saturació de B respecte de θ**, *denotat com B^θ, al conjunt*

$$B^\theta = \bigcup_{b \in B} [b]_\theta.$$

Direm que $B \subseteq A$ és **saturat per θ** *si $B = B^\theta$.*

NOTA 3.40. *Cal destacar que, com que $B \subseteq B^\theta$ sempre és cert, per demostrar que un subconjunt és saturat per θ, només cal comprovar la inclusió $B^\theta \subseteq B$.*

PROPOSICIÓ 3.41. *Siga A un conjunt i $\theta \in \mathrm{Eqv}(A)$, l'operador*

$$\begin{array}{rccc} (\cdot)^\theta : & \mathcal{P}(A) & \longrightarrow & \mathcal{P}(A) \\ & B & \longmapsto & B^\theta \end{array}$$

és un operador de clausura.

DEMOSTRACIÓ. Per la Definició 2.42, per demostrar que es tracta d'un operador de clausura hem de comprovar que l'operador $(\cdot)^\theta$ satisfà les propietats d'extensivitat, idempotència i monotonia.

En primer lloc, com sempre tenim $B \subseteq B^\theta$, aleshores l'operador és extensiu.

Ara, d'una banda, notem que $B^\theta \subseteq (B^\theta)^\theta$. D'altra banda,

$$(B^\theta)^\theta = \bigcup_{[b]_\theta \in B/\theta} \big[[b]_\theta\big]_\theta \subseteq \bigcup_{b \in B} [b]_\theta = B^\theta.$$

Per tant, es compleix la idempotència.

Per últim, siguen $X, Y \in \mathcal{P}(A)$ tals que $X \subseteq Y$. Aleshores

$$X^\theta = \bigcup_{x \in X} [x]_\theta \subseteq \bigcup_{y \in Y} [y]_\theta = Y^\theta.$$

Açò demostra la Proposició 3.41. □

NOTA 3.42. *Siga A un conjunt, θ una relació d'equivalència en A i $B \subseteq A$, aleshores la saturació de B respecte de θ, B^θ, és la col·lecció de classes d'equivalència respecte de θ que intersecten B, com es mostra a la Figura 4.4.*

De la Proposició 3.41 i la Nota 3.42, s'obté que B^θ és el menor subconjunt d'A que conté a B i que està saturat per a la relació d'equivalència θ en B. És a dir, per a tot $b \in B$, tindrem que $[b]_\theta \subseteq B^\theta$. En el cas que $\mathbf{A}$ siga una $\Sigma-$àlgebra i θ una congruència en $\mathbf{A}$ i B un

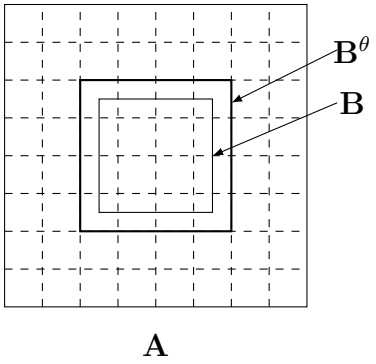

FIGURA 4.4. Saturació de B respecte de θ.

subconjunt tancat d'$\mathbf{A}$, demostrarem a continuació que la saturació de B per θ també és un subconjunt tancat d'$\mathbf{A}$.

PROPOSICIÓ 3.43. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra,* $\mathbf{B}$ *una subàlgebra d'*$\mathbf{A}$ *i* θ *una congruència en* $\mathbf{A}$*. Aleshores* $B^\theta \subseteq A$ *és un subconjunt tancat d'A. Denotem per* $\mathbf{B}^\theta$ *la respectiva subàlgebra. A més, la relació*

$$\theta_{\restriction_{B^\theta}} = \theta \cap (B^\theta \times B^\theta)$$

és una congruència en $\mathbf{B}^\theta$*.*

DEMOSTRACIÓ. Primer, demostrem que B^θ és un subconjunt tancat d'A. Siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $(z_i)_{i\in n}$ una família d'elements en B^θ, volem veure que $\sigma^{\mathbf{A}}\big((z_i)_{i\in n}\big) \in B^\theta$. Com per a cada $i \in n$, $z_i \in B^\theta = \bigcup_{b\in B}[b]_\theta$, llavors existeix $b_i \in B$ tal que $(z_i, b_i) \in \theta$. A més, com $\mathbf{B}$ és subàlgebra, $\sigma^{\mathbf{A}}\big((b_i)_{i\in n}\big) \in B$.

Donat que θ és una congruència,

$$\Big(\sigma^{\mathbf{A}}\big((z_i)_{i\in n}\big), \sigma^{\mathbf{A}}\big((b_i)_{i\in n}\big)\Big) \in \theta.$$

Així,

$$\sigma^{\mathbf{A}}\big((z_i)_{i\in n}\big) \in \big[\sigma^{\mathbf{A}}\big((b_i)_{i\in n}\big)\big]_\theta \subseteq \bigcup_{b\in B}[b]_\theta = B^\theta.$$

És a dir, B^θ és un subconjunt tancat d'$\mathbf{A}$.

Vegem ara que $\theta_{\restriction_{B^\theta}}$ és una relació de congruència en B^θ. És clar que $B_{\restriction_{B^\theta}}$ és d'equivalència, així que només comprovarem la compatibilitat amb les operacions.

Siga $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $\big((u_i, v_i)\big)_{i\in n} \in (\theta_{\restriction_{B^\theta}})^n$. Volem veure que

$$\Big(\sigma^{\mathbf{A}}\big((u_i)_{i\in n}\big), \sigma^{\mathbf{A}}\big((v_i)_{i\in n}\big)\Big) \in \theta_{\restriction_{B^\theta}}.$$

D'una banda, notem que per a cada $i \in n,\ u_i, v_i \in B^\theta$, donat que B^θ és una subàlgebra, es té que $\sigma^{\mathbf{A}}\big((u_i)_{i\in n}\big) \in B^\theta$ i $\sigma^{\mathbf{A}}\big((v_i)_{i\in n}\big) \in B^\theta$. Així,

$$\Big(\sigma^{\mathbf{A}}\big((u_i)_{i\in n}\big), \sigma^{\mathbf{A}}\big((v_i)_{i\in n}\big)\Big) \in (B^\theta \times B^\theta).$$

D'altra banda, per a cada $i \in n$, $(u_i, v_i) \in \theta$. Com θ és congruència, es té que

$$\Big(\sigma^{\mathbf{A}}\big((u_i)_{i\in n}\big), \sigma^{\mathbf{A}}\big((v_i)_{i\in n}\big)\Big) \in \theta.$$

Per tant, $\Big(\sigma^{\mathbf{A}}\big((u_i)_{i\in n}\big), \sigma^{\mathbf{A}}\big((v_i)_{i\in n}\big)\Big) \in \theta_{\restriction_{B^\theta}}$.

Açò conclou la demostració de la Proposició 3.43. □

A conseqüència d'aquest teorema, tenim el següent resultat.

COROLLARI 3.44. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra,* $\mathbf{B}$ *una subàlgebra d'*$\mathbf{A}$ *i* θ *una congruència en* $\mathbf{A}$*. Aleshores* $\mathbf{B}^\theta/\theta_{\restriction_{B^\theta}}$ *és una* $\Sigma-$*àlgebra.*

Introduirem i estudiarem a continuació una aplicació que emprarem per a demostrar el Tercer Teorema d'Isomorfia.

PROPOSICIÓ 3.45. *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra,* $\mathbf{B}$ *una subàlgebra d'*$\mathbf{A}$ *i* θ *una congruència en* $\mathbf{A}$*. Llavors l'aplicació* ξ *donada per*

$$\begin{array}{rccc} \xi: & \mathbf{B} & \longrightarrow & \mathbf{B}^\theta/\theta_{\restriction_{B^\theta}} \\ & b & \longmapsto & [b]_{\theta_{\restriction_{B^\theta}}} \end{array}$$

és un $\Sigma-$*homomorfisme sobrejectiu amb nucli* $\mathrm{Ker}(\xi) = \theta_{\restriction_B}$.

DEMOSTRACIÓ. En primer lloc, demostrarem que es tracta d'un $\Sigma-$homomorfisme. Siguen $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $(b_i)_{i\in n} \in B^n$, aleshores

$$\begin{aligned} \xi\Big(\sigma^{\mathbf{B}}\big((b_i)_{i\in n}\big)\Big) &= \big[\sigma^{\mathbf{B}}\big((b_i)_{i\in n}\big)\big]_{\theta_{\restriction_{B^\theta}}} && \text{(Def. } \xi) \\ &= \big[\sigma^{\mathbf{A}}\big((b_i)_{i\in n}\big)\big]_{\theta_{\restriction_{B^\theta}}} && (\mathbf{B} \leq \mathbf{A}) \\ &= \big[\sigma^{\mathbf{B}^\theta}\big((b_i)_{i\in n}\big)\big]_{\theta_{\restriction_{B^\theta}}} && (\mathbf{B}^\theta \leq \mathbf{A}) \\ &= \sigma^{\mathbf{B}^\theta/\theta_{\restriction_{B^\theta}}}\Big(\big([b_i]_{\theta_{\restriction_{B^\theta}}}\big)_{i\in n}\Big) && (\mathbf{B}^\theta/\theta_{\restriction_{B^\theta}}) \\ &= \sigma^{\mathbf{B}^\theta/\theta_{\restriction_{B^\theta}}}\Big(\big(\xi(b_i)\big)_{i\in n}\Big). && \text{(Def. } \xi) \end{aligned}$$

Així, ξ és un $\Sigma-$homomorfisme.

Vegem ara que és una aplicació sobrejectiva. Notem que un element arbitrari de $B^\theta/\theta_{\restriction_{B^\theta}}$ té la forma $[z]_{\theta_{\restriction_{B^\theta}}}$ amb $z \in B^\theta$. Per tant, existeix un $b \in B$ de forma que $(b, z) \in \theta$.

Però, com $b \in B \subseteq B^\theta$ i $z \in B^\theta$ i $(b, z) \in \theta$, aleshores $(b, z) \in \theta_{\restriction_{B^\theta}}$.

Així,

$$\xi(b) = [b]_{\theta_{\restriction_{B^\theta}}} = [z]_{\theta_{\restriction_{B^\theta}}}.$$

És a dir, ξ és sobrejectiva.

Per últim, abans d'estudiar el nucli de ξ, demostrarem que si $b, b' \in B$, aleshores $[b]_{\theta_{\restriction_{B^\theta}}} = [b']_{\theta_{\restriction_{B^\theta}}}$ si, i només si, $(b, b') \in \theta$.

D'una banda, si $[b]_{\theta_{\restriction_{B^\theta}}} = [b']_{\theta_{\restriction_{B^\theta}}}$, aleshores

$$(b, b') \in \theta_{\restriction_{B^\theta}} = \theta \cap (B^\theta \times B^\theta).$$

En particular $(b, b') \in \theta$.

D'altra banda, si suposem que $(b, b') \in \theta$, com $b, b' \in B \subseteq B^\theta$, es té que

$$(b, b') \in \theta \cap (B^\theta \times B^\theta) = \theta_{\restriction_{B^\theta}}.$$

Per tant, $[b]_{\theta_{\restriction_{B^\theta}}} = [b']_{\theta_{\restriction_{B^\theta}}}$.

Així, tenint en compte aquesta afirmació, el nucli de ξ és per definició $\theta_{\restriction_{B^\theta}}$, ja que

$$\begin{aligned}
\mathrm{Ker}(\xi) &= \{(b, b') \in B \times B \mid \xi(b) = \xi(b')\} \\
&= \{(b, b') \in B \times B \mid [b]_{\theta_{\restriction_{B^\theta}}} = [b']_{\theta_{\restriction_{B^\theta}}}\} \\
&= \{(b, b') \in B \times B \mid (b, b') \in \theta\} \\
&= \theta_{\restriction_B}.
\end{aligned}$$

Amb açò queda demostrada la Proposició 3.45. □

Una volta vist els resultats previs necessaris, donem pas al Tercer Teorema d'Isomorfia, que estableix que el quocient d'una subàlgebra respecte a la restricció d'una congruència és isomorf al quocient de la saturació entre la restricció de la congruència.

Teorema 3.46 (Tercer Teorema d'Isomorfia). *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* θ *una congruència en* $\mathbf{A}$. *Siga* $\mathbf{B} \leq \mathbf{A}$ *una subàlgebra. Aleshores*

$$\mathbf{B}/\theta_{\restriction_B} \cong B^\theta/\theta_{\restriction_{B^\theta}}.$$

Demostració. Per la Proposició 3.45 sabem que ξ és un homomorfisme. Pel Primer Teorema d'Isomorfia, Teorema 3.34, sabem que

$$\mathbf{B}/\mathrm{Ker}(\xi) \cong \mathbf{Im}(\xi).$$

D'una banda, com ξ és una aplicació sobrejectiva, $\mathbf{Im}(\xi) = \mathbf{B}^\theta/\theta_{\restriction_{B^\theta}}$.

D'altra banda, per la Proposició 3.45, $\mathrm{Ker}(\xi) = \theta_{\restriction_B}$. Per tant,

$$\mathbf{B}/\theta_{\restriction_B} \cong \mathbf{B}^\theta/\theta_{\restriction_{B^\theta}}.$$

Açò conclou la demostració del Tercer Teorema d'Isomorfia. □

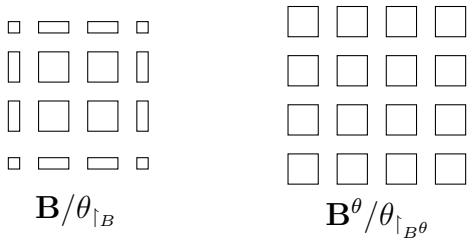

FIGURA 4.5. El Tercer Teorema d'Isomorfia.

Com podem veure a la Figura 4.5, existeix un isomorfisme entre el quocient de la subàlgebra $\mathbf{B}$ *per la congruència* $\theta_{\restriction_B}$ *i el quocient de la saturació* $\mathbf{B}^\theta$ *per* $\theta_{\restriction_{B^\theta}}$*, que completa les classes d'equivalència. Aquest resultat ens mostra que els quocients de* $\mathbf{B}$ *i* $\mathbf{B}^\theta$ *tenen estructures similars a pesar de les diferències inicials.*

4.4. Teorema de correspondència. Primer, hem de definir la noció d'interval entre dos elements d'un reticle, ja que aquest està dotat d'una relació d'ordre.

DEFINICIÓ 3.47. *Siga* L *un reticle i* $a, b \in L$*, amb* $a \leq b$*, definim l'interval entre* a *i* b*, denotat per* $[a, b]$*, al subreticle associat al conjunt*

$$[a, b] = \{z \in L \mid a \leq z \leq b\}.$$

Recordem que, com varem demostrar al Teorema 3.32, l'estructura $\big(\mathrm{Con}(\mathbf{A}), \subseteq\big)$ és un reticle algebraic. Llavors, donada una congruència θ, podem considerar un interval dins d'aquest reticle de θ a ∇_A. El següent teorema ens mostra la relació que existeix entre l'interval mencionat i l'espai de congruències del quocient d'$\mathbf{A}$ per θ.

TEOREMA 3.48 (Teorema de correspondència). *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* $\theta \in \mathrm{Con}(\mathbf{A})$*, llavors existeix un isomorfisme de reticles entre l'interval* $[\theta, \nabla_A]$ *i* $\mathrm{Con}(\mathbf{A}/\theta)$*.*

DEMOSTRACIÓ. Considerem l'aplicació

$$\begin{array}{rccc} \alpha: & [\theta, \nabla_A] & \longrightarrow & \mathrm{Con}(\mathbf{A}/\theta) \\ & \phi & \longmapsto & \phi/\theta. \end{array}$$

Com que $\theta \subseteq \phi$, ja vam veure al Segon Teorema d'Isomorfia, Teorema 3.36, que ϕ/θ és una congruència. Per tant, α està ben definida. Llavors hem de comprovar que α és un homomorfisme bijectiu.

En primer lloc, per demostrar que es tracta d'un homomorfisme anem a veure que, per a tot parell de congruències ϕ, ψ en $[\theta, \nabla_A]$ es té que $\phi \subseteq \psi$ si, i només si, $\alpha(\phi) \subseteq \alpha(\psi)$.

Notem que, per la definició de l'aplicació α, açò és equivalent a comprovar que $\phi \subseteq \psi$ si, i només si, $\phi/\theta \subseteq \psi/\theta$.

Suposem que $\phi \subseteq \psi$. Siga $\big([a]_\theta, [b]_\theta\big) \in \phi/\theta$, aleshores $(a,b) \in \phi$. A més, com $\phi \subseteq \psi$, aleshores $(a,b) \in \psi$. Així, $\big([a]_\theta, [b]_\theta\big) \in \psi/\theta$ i per tant, $\phi/\theta \subseteq \psi/\theta$.

Suposem ara que $\phi/\theta \subseteq \psi/\theta$. Siga $(a,b) \in \phi$, aleshores $\big([a]_\theta, [b]_\theta\big) \in \phi/\theta$. Com $\phi/\theta \subseteq \psi/\theta$, aleshores $\big([a]_\theta, [b]_\theta\big) \in \psi/\theta$. Així, $(a,b) \in \psi$ i, per tant, $\phi \subseteq \psi$.

Anem a provar ara la injectivitat. Siguen $\psi, \phi \in [\theta, \nabla_A]$ diferents, sense pèrdua de generalitat podem trobar $(a,b) \in \phi - \psi$. Així $\big([a]_\theta, [b]_\theta\big) \in \phi/\theta - \psi/\theta$, és a dir, $\phi/\theta \neq \psi/\theta$.

Per acabar, demostrem que és sobrejectiva. Siga ψ una congruència en $\mathrm{Con}\big(\mathbf{A}/\theta\big)$, aleshores podem considerar les projeccions

$$\mathrm{pr}^\psi : \ A/\theta \ \longrightarrow \ \big(A/\theta\big)/\psi; \qquad \mathrm{pr}^\theta : \ A \longrightarrow \ A/\theta.$$

Considerem $\phi = \mathrm{Ker}(\mathrm{pr}^\psi \circ \mathrm{pr}^\theta)$. Com les projeccions són homomorfismes, ϕ és una congruència en $\mathbf{A}$. A més,

$$\begin{aligned}
\alpha(\phi) &= \phi/\theta \\
&= \{\big([a]_\theta, [b]_\theta\big) \in A/\theta \times A/\theta \mid (a,b) \in \phi\} \\
&= \{\big([a]_\theta, [b]_\theta\big) \in A/\theta \times A/\theta \mid (a,b) \in \mathrm{Ker}(\mathrm{pr}^\psi \circ \mathrm{pr}^\theta)\} \\
&= \{\big([a]_\theta, [b]_\theta\big) \in A/\theta \times A/\theta \mid \mathrm{pr}^\psi \circ \mathrm{pr}^\theta(a) = \mathrm{pr}^\psi \circ \mathrm{pr}^\theta(b)\} \\
&= \{\big([a]_\theta, [b]_\theta\big) \in A/\theta \times A/\theta \mid \mathrm{pr}^\psi([a]_\theta) = \mathrm{pr}^\psi([b]_\theta)\} \\
&= \{\big([a]_\theta, [b]_\theta\big) \in \ A/\theta \times A/\theta \mid \big([a]_\theta, [b]_\theta\big) \in \psi\} \\
&= \psi.
\end{aligned}$$

Aixi, α és sobrejectiva.

Per tant, l'aplicació α és un isomorfisme. □

Com podem veure a la Figura 4.6, l'interval entre les congruències θ i ∇_A és isomorf a l'espai de congruències del quocient $\mathbf{A}/\theta$.

En resum, el Teorema de Correspondència estableix una relació entre les congruències de l'interval $[\theta, \nabla_A]$ i les congruències d'$\mathbf{A}/\theta$, la qual cosa ens permet entendre l'estructura i les propietats dels dos conjunts.

5. Àlgebra de Termes

En la següent secció vorem un exemple d'aplicació dels teoremes d'isomorfia.

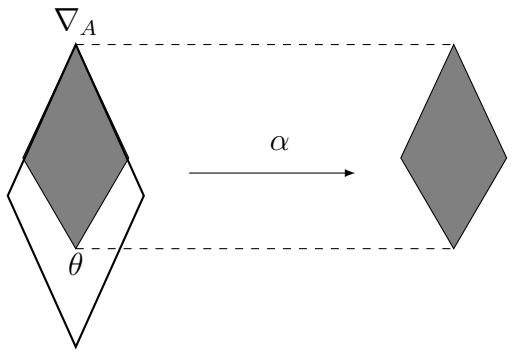

FIGURA 4.6. El Teorema de correspondència.

DEFINICIÓ 3.49. *Siga X un conjunt de variables i Σ una signatura, el* **conjunt $\mathrm{T}_\Sigma(X)$ de $\Sigma-$termes sobre** *X es defineix com el menor conjunt que satisfà que $X \subseteq \mathrm{T}_\Sigma(X)$, i que si $n \in \mathbb{N}$, $\sigma \in \Sigma_n$ i $(P_i)_{i\in n}$ una família en $\mathrm{T}_\Sigma(X)$, aleshores*

$$\sigma\big((P_i)_{i\in n}\big) \in \mathrm{T}_\Sigma(X).$$

EXEMPLE 3.50. *Siga $\Sigma = \{+, \square, 0\}$, amb aritat $2, 3$ i 0 respectivament i $X = \{x, y, z\}$.*

Notem $x + y \in \mathrm{T}_\Sigma(X)$ i $\square(x + y, y, x) \in \mathrm{T}_\Sigma(X)$.

NOTA 3.51. *L'àlgebra de termes no s'ha de confondre amb els polinomis, ja que l'àlgebra de termes diferencia els següents termes.*

$$x + (y + z) \neq (x + y) + z.$$

NOTA 3.52. *Siga X un conjunt de variables i Σ una signatura, el conjunt $\mathrm{T}_\Sigma(X)$ admet estructura de $\Sigma-$àlgebra.*

Siga $n \in \mathbb{N}, \sigma \in \Sigma_n$ i $(P_i)_{i\in n}$ una família en $\mathrm{T}_\Sigma(X)$, aleshores

$$\sigma^{\mathrm{T}_\Sigma(X)}\big((P_i)_{i\in n}\big) = \sigma\big((P_i)_{i\in n}\big) \in \mathrm{T}_\Sigma(X).$$

Així, σ s'interpreta de forma sintàctica, com una paraula. Denotarem per $\mathbf{T}_\Sigma(X)$ l'estructura de $\Sigma-$àlgebra en $\mathrm{T}_\Sigma(X)$. A més, tenim l'aplicació inclusió

$$\begin{array}{rccc} \mathrm{in}^X: & X & \longrightarrow & \mathrm{T}_\Sigma(X) \\ & x & \longmapsto & x. \end{array}$$

Vegem ara el resultat més important d'aquesta secció, que ens permet obtindre $\Sigma-$homomorfismes a partir d'aplicacions que tenen com a imatge una $\Sigma-$àlgebra.

TEOREMA 3.53 (Propietat Universal). *Siga* $\mathbf{A}$ *una* $\Sigma-$*àlgebra i* $h: \ X \longrightarrow A$ *una aplicació, aleshores existeix un únic* $\Sigma-$*homomorfisme*

$$h^{\#}: \ \mathbf{T}_{\Sigma}(X) \longrightarrow \mathbf{A}$$

tal que $h^{\#} \circ \mathrm{in}^X = h$.

DEMOSTRACIÓ. Notem que tot terme P de $\mathrm{T}_{\Sigma}(X)$ és de la forma $P = x$ amb $x \in X$ o $P = \sigma\big((P_i)_{i\in n}\big)$ amb $\sigma \in \Sigma_n$ i $(P_i)_{i\in n}$ termes. Aleshores definim $h^{\#}$ sobre les variables com $h^{\#}(x) = h(x)$ i, si suposem definit $h^{\#}(P_i)$ per a $i \in n$, aleshores

$$h^{\#}\Big(\sigma\big((P_i)_{i\in n}\big)\Big) = \sigma^{\mathbf{A}}\Big(\big(h^{\#}(P_i)\big)_{i\in n}\Big).$$

A més, $h^{\#}$ és un $\Sigma-$homomorfisme, ja que, si $n \in \mathbb{N}, \sigma \in \Sigma_n$ i $(P_i)_{i\in n}$ és una família en $\mathrm{T}_{\Sigma}(X)$, aleshores

$$h^{\#}\Big(\sigma^{\mathbf{T}_{\Sigma}(X)}\big((P_i)_{i\in n}\big)\Big) = \sigma^{\mathbf{A}}\Big(\big(h^{\#}(P_i)\big)_{i\in n}\Big).$$

En efecte, $(h^{\#} \circ \mathrm{in}^X)(x) = h^{\#}(x) = h(x)$ i, per tant, $h^{\#} \circ \mathrm{in}^X = h$, és a dir, $h^{\#}$ és el $\Sigma-$homomorfisme desitjat.

Vegem ara la unicitat. Suposem que existeix

$$g: \ \mathrm{T}_{\Sigma}(X) \longrightarrow A$$

un $\Sigma-$homomorfisme que satisfà $g \circ \mathrm{in}^X = h$. Així, si $P \in \mathrm{T}_{\Sigma}(X)$, distingim els dos casos.

D'una banda, si $P = x$,

$$\begin{aligned} g(P) &= g \circ \mathrm{in}^X(x) \\ &= h(x) \\ &= h^{\#}(x) \\ &= h^{\#}(P). \end{aligned}$$

D'altra banda, si $P = \sigma\big((P_i)_{i\in n}\big)$, llavors

$$\begin{aligned} g(P) &= \sigma^{\mathbf{A}}\Big(\big(g(P_i)\big)_{i\in n}\Big) \\ &= \sigma^{\mathbf{A}}\Big(\big(h^{\#}(P_i)\big)_{i\in n}\Big) \\ &= h^{\#}(P). \end{aligned}$$

Així, $g = h^{\#}$.

Açò demostra el Teorema 3.53. □

EXEMPLE 3.54. *En grups, considerem* $\Sigma = \{\cdot, ()^{-1}, 1\}$ *i* $X = \{x, y, z\}$. *Siga* $P = (x \cdot y) \cdot z^{-1} \cdot (x) \in \mathrm{T}_\Sigma(X)$.

Siga $\mathbf{G}$ *un grup, considerem l'aplicació*

$$\begin{array}{rccc} h: & X & \longrightarrow & G \\ & x & \longmapsto & 1 \\ & y & \longmapsto & g \\ & z & \longmapsto & g^2. \end{array}$$

Per la Propietat Universal, Teorema 3.53, existeix un únic homomorfisme $h^\# : \mathbf{T}_\Sigma(X) \longrightarrow \mathbf{G}$ *tal que* $h^\# \circ \mathrm{in}^X = h$.

Així, la interpretació del terme P *d'acord amb la valoració* h *és*

$$h^\#(P) = (1 \cdot g)(g^2)^{-1} \cdot (1) = g^2 \in G.$$

Així, el Teorema 3.53 ens assegura l'existència de $\Sigma-$homomorfismes entre un àlgebra de termes i una $\Sigma-$àlgebra a partir d'aplicacions sobre el conjunt de variables i l'àlgebra del codomini. Amb ajuda dels teoremes d'isomorfia vists a la secció anterior, podem demostrar que existeix una relació d'isomorfia entre un quocient de l'àlgebra de termes i una $\Sigma-$àlgebra qualsevol.

COROL·LARI 3.55. *Tota àlgebra és isomorfa a un quocient d'una àlgebra de termes.*

DEMOSTRACIÓ. Siga $\mathbf{A}$ una $\Sigma-$àlgebra. Considerem l'àlgebra de termes $\mathbf{T}_\Sigma(A)$ i l'aplicació identitat

$$\begin{array}{rccc} \mathrm{id}^A: & A & \longrightarrow & A \\ & a & \longmapsto & a. \end{array}$$

Per la Propietat Universal, Teorema 3.53, existeix un únic homomorfisme

$$\big(\mathrm{id}^A\big)^\# : \mathbf{T}_\Sigma(A) \longrightarrow \mathbf{A}$$

tal que $\big(\mathrm{id}^A\big)^\# \circ \mathrm{in}^A = \mathrm{id}^A$.

A més, $\big(\mathrm{id}^A\big)^\#$ és sobrejectiva, ja que, si $a \in A$, aleshores

$$\begin{aligned} (\mathrm{id}^A)^\#(a) &= (\mathrm{id}^A)^\#\big(\mathrm{in}^A(a)\big) \\ &= \mathrm{id}^A(a) \\ &= a. \end{aligned}$$

Així, $\mathbf{Im}\big((\mathrm{id}^A)^\#\big) = \mathbf{A}$.

Per tant, pel Primer Teorema d'Isomorfia, Teorema 3.34 sabem que

$$\mathbf{T}_\Sigma(A)/\mathrm{Ker}\big((\mathrm{id}^A)^\#\big) \cong \mathbf{Im}\big((\mathrm{id}^A)^\#\big) = \mathbf{A}.$$

Açò demostra el Corol·lari 3.55. □

CAPíTOL 4

Conclusions

> La matemàtica pura es, a su manera, la poesía de las ideas lógicas
>
> *A. Einstein* [**2**]

Com hem dit abans, l'àlgebra universal és l'àrea de les matemàtiques que se centra en l'estudi abstracte de les propietats generals i les estructures comunes a diferents sistemes algebraics, independentment de la natura d'aquests.

En aquest estudi, els reticles juguen un paper important, ja que aporten una noció especial d'ordre que ens permet una millor comprensió de les àlgebres. Entre els diferents tipus de reticles, destaquen els complets i els algebraics.

Un reticle complet satisfà que sempre existeixen en ell el suprem i l'ínfim de qualsevol subconjunt, així sempre podem trobar una fita superior i inferior al reticle. Un reticle algebraic és aquell que és complet i compactament generat, és a dir, que a més de ser complet, satisfà que tot element del reticle és el suprem d'un conjunt d'elements compactes.

També cal destacar la figura dels operadors de clausura i la seua relació amb aquest tipus de reticles. En general, un operador de clausura és una funció que pren un conjunt com a entrada i l'extén incloent tots els elements necessaris per a complir amb unes certes condicions o propietats. Llavors, podem caracteritzar els conjunts tancats com aquells que són invariants per un operador de clausura. En relació amb els reticles complets, donat un operador de clausura podem definir un reticle complet i, recíprocament, donat un reticle d'aquest tipus sempre podem definir un operador de clausura. Si afegim la característica que siga finitament generat, llavors es pot provar que el reticle algebraic és isomorf al reticle dels subconjunts tancats d'un conjunt amb un operador de clausura algebraic.

Recordem que una àlgebra és un conjunt dotat d'operacions que sempre donen com a resultat elements d'eixe conjunt en aplicar-les sobre famílies de les respectives aritats o, equivalentment, el conjunt és

tancat per a aquestes operacions. Aquesta definició ens permet tractar estructures de diferent natura com les mateixes estructures i obtindre resultats que es verifiquen per a totes les estructures algebraiques.

Donada una àlgebra, podem trobar en ella subconjunts que són tancats per a totes les operacions d'aquesta, denotats com subàlgebres. En la creació de subàlgebres, destaquen les subàlgebres generades per un conjunt, noció en la qual apareix un operador de clausura. A més, cal destacar que el conjunt de subàlgebres d'una àlgebra és un reticle algebraic. Aquest resultat ens permet ordenar totes les possibles subàlgebres d'una àlgebra, de forma que, per a qualsevol subconjunt de subàlgbres, existeixen sempre subàlgebres que són suprem i ínfim.

En les àlgebres també destaca la noció de congruència, una relació d'equivalència que és compatible amb les operacions definides sobre l'àlgebra. A més, donada una àlgebra i una congruència sobre l'àlgebra, podem definir el conjunt quocient, que per la compatibilitat amb les operacions, també tindrà estructura d'àlgebra. El conjunt de les congruències sobre una àlgebra és també un reticle algebraic per a l'ordre donat per la inclusió de conjunts. Conéixer l'estructura del reticle de congruències definides sobre una àlgebra també ens pot aportar informació la mateixa àlgebra.

En aquest context, un isomorfisme d'àlgebres és una aplicació bijectiva que preserva certes propietats importants entre les àlgebres. Quan aquesta situació es dona, es diu que les àlgebres són isomorfes. L'existència d'un isomorfisme entre dues àlgebres permet establir una correspondència entre els seus elements i les seues operacions. Això proporciona una manera de relacionar i comparar les propietats de les àlgebres, permetent-nos entendre millor les seues estructures. Així, els teoremes d'isomorfia són un conjunt de resultats fonamentals en l'àlgebra universal que ens permeten establir relacions i correspondències entre àlgebres, identificant estructures similars i preservant propietats essencials.

Siguen $\mathbf{A}$ i $\mathbf{B}$ dues àlgebres i $f : \mathbf{A} \longrightarrow \mathbf{B}$ un $\Sigma-$homomorfisme, hem comprovat que la imatge de f és una subàlgebra de $\mathbf{B}$ i que el nucli de l'homomorfisme és una congruència sobre $\mathbf{A}$. Així, el Primer Teorema d'Isomorfia estableix l'existència d'un isomorfisme entre l'espai quocient d'$\mathbf{A}$ pel nucli de f i la imatge de f. Aquest resultat ens facilita la comprensió de l'estructura del quocient d'una àlgebra pel seu nucli a través de l'estudi de la imatge d'un homomorfisme.

En segon lloc, donades dues congruències θ i ϕ sobre una $\Sigma-$àlgebra $\mathbf{A}$, amb $\theta \subseteq \phi$, el Segon Teorema d'Isomorfia demostra la relació d'isomorfia que existeix entre el quocient de l'àlgebra per la congruència

menor entre el quocient de les congruències i el quocient de l'àlgebra per la congruència major.

En tercer lloc, per treballar amb el Tercer Teorema d'Isomorfia hem degut treballar amb la saturació d'un conjunt. Recordem que, donada una relació d'equivalència θ sobre un conjunt A, es defineix la saturació d'un subconjunt $B \subseteq A$ respecte de θ com la unió de les classes d'equivalència dels elements de B respecte a la relació θ. És a dir, es completa el conjunt B amb tots els elements que estan relacionats a través de θ amb algun element de B. Quan treballem amb àlgebres, la saturació d'una subàlgebra $\mathbf{B}$ és una estructura tancada per a les operacions de l'àlgebra, i la restricció de θ al conjunt saturat és una congruència en la subàlgebra del saturat. Així, el quocient del saturat per la congruència restringida al saturat té estructura de $\Sigma-$àlgebra i, a més, és isomorfa al quocient de $\mathbf{B}$ per la congruència restringida a B. Aquest resultat ens permet establir una correspondència entre els quocients de $\mathbf{B}$ i $\mathbf{B}^\theta$, mostrant que tenen estructures similars malgrat les diferències inicials.

Per últim, siga $\mathbf{A}$ una $\Sigma-$àlgebra i θ una congruència sobre $\mathbf{A}$, llavors el teorema de correspondència mostra l'isomorfisme existent entre l'interval que trobem de θ a ∇_A i l'espai de congruències del quocient d'$\mathbf{A}$ per θ.

Tots aquests resultats suposen eines de gran rellevància per a l'estudi en profunditat de qualsevol àlgebra. A través d'aquesta comprensió, podem establir analogies i transferir coneixements d'una àlgebra a una altra, obrint també la porta a noves investigacions.

Bibliografia

[1] L. Acosta. *Temas de teoría de retículos*. Universidad Nacional de Colombia, 2015.

[2] M.R. Àlvarez. Àlgebra y algoritmos. un breve paseo por la historia.

[3] C. Bergman. *Universal algebra: Fundamentals and selected topics*. CRC Press, 2011.

[4] G.M. Bergman. *An invitation to general algebra and universal constructions*, volume 558. Springer, 2015.

[5] G. Birkhoff. *Lattice theory*, volume 25. American Mathematical Soc., 1940.

[6] N. Bourbaki. *Théorie des ensembles*. Springer, 2006.

[7] K. Denecke and S.L. Wismath. *Universal algebra and coalgebra*. World Scientific, 2009.

[8] J.C. Gibbings. *Lattice Theory: Foundation*. Springer Basel, Basel, 2011.

[9] J. Estevan and L. Chaves. Teorema fundamental del álgebra: visualizaciones, intuiciones y demostraciones formales.

[10] R.N. McKenzie, G.F. McNulty, and W.F. Taylor. *Algebras, lattices, varieties*, volume 383. American Mathematical Soc., 2018.

[11] G.C. Rota. The many lives of lattice theory. *Notices of the AMS*, 44(11):1440–1445, 1997.

[12] H.P. Sankappanavar and S. Burris. A course in universal algebra. *Graduate Texts Math*, 78:56, 1981.