

Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

El Teorema de Birkhoff

Autor: Marc Alexis Ortega Aguasca

Director: Dr. Joan Gispert Braso

Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 28 de juny de 2017

Abstract

Birkhoff's Theorem states that let K be a class of algebras, then K is an equational class if, and only if, K is a variety. To reach this result, it is necessary to understand some basic concepts of universal algebra. Varieties, free algebras and identities will be essential to understand the proof of Birkhoff's Theorem. We study that statement and how to achieve the proof of it. We also study some of the immediate consequences of Birkhoff's Theorem in equational logic. Moreover, there is a final section as appendix where we study some properties of lattices.

Resum

El Teorema de Birkhoff afirma que donada K una classe d'àlgebres, direm que aquesta és equacional si, i només si, és variacional. Per tal d'arribar a aquest resultat és necessari comprendre una sèrie de conceptes bàsics propis de l'àlgebra universal. Entre aquests conceptes destaquen les varietats, les àlgebres lliures i les identitats que seran essencials per tal d'assolir la demostració del teorema de Birkhoff. En aquest treball s'estudia l'enunciat esmentat i com arribar a la seva demostració, així com algunes de les seves conseqüències més immediates com les que es poden observar en lògica equacional. Tanmateix, s'inclou un apartat en forma d'annex on s'estudien algunes propietats dels reticles, que representen una de les àlgebres més presents al llarg del treball.

Agraïments

Vull agrair al Dr. Joan Gispert per totes les hores que ha dedicat a tutelar aquest treball. En primer lloc per descobrir-me el Teorema de Birkhoff arran de la seva proposta del tema, per assessorar-me sempre que ha estat necessari i per totes les indicacions que m'ha fet al llarg de la preparació i escriptura de la memòria.

Índex

1	Introducció	1
2	Àlgebres	3
3	Homomorfismes	7
4	Congruències	9
5	Teoremes de Isomorfia	15
6	Producte Directe i Productes Subdirectes	21
7	Varietats	27
8	Àlgebres Lliures	31
9	Identitats i Teorema de Birkhoff	35
10	Les condicions de Mal'cev	41
11	Lògica Equacional	45
12	Annex: Reticles	49
13	Conclusions	59

1 Introducció

El 1935, Garreth Birkhoff va presentar per primera vegada el resultat que s'estudia en aquest treball dins de l'article *On the structure of abstract algebras*. Aquest resultat se'l coneix com el Teorema de Birkhoff i afirma que donada una classe d'àlgebres, aquesta és equacional si, i només si, és variacional.

La motivació principal d'aquest treball sorgeix arran de la proposta del Dr. Joan Gispert davant la possibilitat d'estudiar un resultat que permet relacionar conceptes propis de l'àlgebra amb els de la lògica.

L'estudi d'aquest teorema s'engloba dins de l'àlgebra universal, per tant, abans d'entrar en aquest, és necessari estudiar prèviament els conceptes bàsics més importants d'aquest camp de la matemàtica. L'àlgebra universal ens permet l'estudi dels resultats comuns de les estructures algebraiques de forma abstracte, sense entrar en cap model concret.

La primera part del treball consisteix en estudiar els conceptes que ens permetran construir la demostració del Teorema de Birkhoff. Podrem veure més àmpliament alguns dels resultats vistos en assignatures al llarg del grau propis d'algunes estructures algebraiques com poden ser els grups i els anells, però des d'una nova perspectiva.

En primer lloc es presenta el concepte d'àlgebra amb alguns exemples de les més conegudes i de les més importants pel treball, com seria l'àlgebra de termes. Posteriorment, també es treballa en profunditat altres conceptes coneguts com podrien ser les funcions homomorfes o les congruències, juntament amb algunes de les seves principals propietats.

La segona part del treball introdueix més resultats de l'àlgebra universal que no s'han vist prèviament en cap assignatura anterior i per tant han requerit d'una feina de preparació. Dins d'aquest espai s'hi trobarien les varietats, les àlgebres lliures i les identitats, totes elles necessàries per construir la demostració del Teorema de Birkhoff.

D'altra banda, aquesta part conclou amb la demostració del Teorema de Birkhoff. Per tal d'arribar a la demostració s'ha seguit principalment la proposta que es presenta en l'obra de S. Burris i H. P. Snakappanavar, [4], tant pels conceptes previs com per la demostració en si mateix. Tanmateix, s'inclou l'enunciat del teorema tal com el va presentar Birkhoff per primera vegada en [2].

Per últim, s'afegeixen dos capítols més on s'incideix en algunes de les conseqüències directes del Teorema de Birkhoff. Aquests resultats consisteixen en les

condicions de Mal'cev i una apartat sobre lògica equacional.

Tanmateix, davant la importància que tenen els reticles al llarg d'aquest estudi s'ha optat per afegir un annex al final de la memòria amb alguns dels resultats més importants propis d'aquesta estructura algebraica, a més d'un exemple on es pot observar alguns del resultats estudiats. En aquest apartat ha estat útil i sovint s'ha consultat l'obra de Birkhoff sobre reticles [3].

Al llarg de la memòria s'han consultat algunes obres que no es citen explícitament, això és degut a que la seva funció ha estat complementaria, amb l'objectiu de clarificar o veure presentacions diferents d'un resultat. En aquesta situació s'hi troben [7] i [8].

2 Àlgebres

En aquesta secció l'objectiu és presentar els elements bàsics que giren al voltant del concepte d'àlgebra.

Definició 2.1. *Un llenguatge algebraic (o tipus) és una parella $\tau = (\mathfrak{F}, \sigma)$. On $\mathfrak{F}$ és un conjunt de símbols funcionals i σ és una aplicació de $\mathfrak{F}$ a $\mathbb{N}$, diem que $\sigma(f)$ és l'arietat.*

S'expressarà τ per referir-se a un llenguatge algebraic $(\mathfrak{F}, \sigma)$.

Donat un llenguatge algebraic τ , direm que un símbol funcional $f \in \mathfrak{F}$ és n -àri quan $\sigma(f) = n$.

Sigui τ un llenguatge algebraic, una àlgebra $\mathbf{A}$ és una parella $\mathbf{A} = \langle A, \{f^{\mathbf{A}} : f \in \mathfrak{F}\} \rangle$, on A és un conjunt no buit.

Per cada $f \in \mathfrak{F}$, $f^{\mathbf{A}}$ és una aplicació d'ordre $\sigma(f)$ en A , és a dir, $f^{\mathbf{A}} : A^{\sigma(f)} \rightarrow A$.

En el cas en que $\sigma(f) = 0$, aleshores direm que la funció és nul·lària i tindrem que $f^{\mathbf{A}} \in A$. El conjunt d'operacions fonamentals nul·làries d'una àlgebra l'expressarem com $\mathfrak{F}_0$.

Anomenem A univers de $\mathbf{A}$ i $\{f^{\mathbf{A}}, f \in \mathfrak{F}\}$ el conjunt d'operacions fonamentals de $\mathbf{A}$.

Exemple 1. Observem dos exemples d'àlgebres:

Sigui $\mathbf{G}_1 = \langle \mathbb{R}, \{f_1^{\mathbf{G}_1} := +, f_2^{\mathbf{G}_1} := -, f_3^{\mathbf{G}_1} := 0\} \rangle$, o per simplificar $\mathbf{G}_1 = \langle \mathbb{R}, +, -, 0 \rangle$, on els símbols funcionals són de tipus $\langle 2, 1, 0 \rangle$ respectivament i corresponen a la suma, símbol negatiu i el zero usals. Per definició d'àlgebra és evident que $\mathbf{G}_1$ és una àlgebra.

Sigui $\mathbf{G}_2 = \langle \mathbb{R}^+, f_1^{\mathbf{G}_2} := \cdot, f_2^{\mathbf{G}_2} := ^{-1}, f_3^{\mathbf{G}_2} := 1 \rangle$, on els símbols funcionals són de tipus $\langle 2, 1, 0 \rangle$ respectivament i corresponen al producte, invers i 1 usals. Aleshores, $\mathbf{G}_2 = \langle \mathbb{R}, \cdot, ^{-1}, 1 \rangle$ també és una àlgebra.

Observem que hem obtingut dues àlgebres diferents, però del mateix tipus $\langle 2, 1, 0 \rangle$.

Definició 2.2. *Un grup és una àlgebra $\langle G, \{f_1^{\mathbf{G}} := \cdot, f_2^{\mathbf{G}} := ^{-1}, f_3^{\mathbf{G}} := 1\} \rangle$ de tipus $\langle 2, 1, 0 \rangle$, on G és un conjunt. $\langle G, \cdot, ^{-1}, 1 \rangle$ compleix:*

(i) *Per tot $x, y, z \in G$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$*

(ii) *Per tot $x \in G$, $x \cdot 1 = 1 \cdot x = x$*

(iii) *Per tot $x \in G$, $x \cdot x^{-1} = x^{-1} \cdot x = 1$.*

Si a més compleix:

(iii) Per tot $x, y \in G$, $x \cdot y = y \cdot x$.

Aleshores direm que el grup és abelià.

Observem que les àlgebres $\mathbf{G}_1$ i $\mathbf{G}_2$ de l'exemple 1 són grups.

Definició 2.3. *Un semigrup $\langle S, \cdot \rangle$ és una àlgebra amb una sola operació fonamental binària i que compleix la primera condició per ser grup.*

Exemple 2. Agafant $\mathbf{G} = \langle \mathbb{R}, \cdot \rangle$ amb el mateix símbol funcional que l'exemple anterior podem veure que l'àlgebra compleix les condicions per tal de ser un semigrup.

Exemple 3. Definim l'àlgebra: $\mathcal{R} = \langle \mathbb{R}, +, \cdot, -, 0 \rangle$, on els símbols funcionals són d'ordre $\langle 2, 2, 1, 0 \rangle$ respectivament i corresponen a la suma, producte, símbol negatiu i 0.

(i) $\langle \mathbb{R}, +, -, 0 \rangle$ és un grup per el que ja hem vist en l'exemple de grups i abelià per la commutativa de la suma.

(ii) $\langle \mathbb{R}, \cdot \rangle$, és semigrup, ho hem vist en l'exemple de semigrup.

(iii) Per tot $a, b, c \in \mathbb{R}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ per la propietat distributiva del producte respecte la suma.

Definició 2.4. *Un anell és una àlgebra definida per $\langle A, +, \cdot, -, 0 \rangle$; on A és un conjunt, $+$, $\cdot$ són binàries, $-$ unària i 0 nul·lària. A més, es satisfà:*

(i) $\langle A, +, -, 0 \rangle$ és un grup abelià.

(ii) $\langle A, \cdot \rangle$, és semigrup.

(iii) Per tot $a, b, c \in A$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Observem que $\mathcal{R}$ de l'exemple anterior és un anell. Per últim definim una classe d'àlgebres que també seràn important al llarg del treball:

Definició 2.5. *Un reticle és una àlgebra $\langle L, \vee, \wedge \rangle$; on L és un conjunt i els dos símbols funcionals són binaris, a més, es compleix que:*

(i) Per tot $x, y \in L$, $x \vee y = y \vee x$; $x \wedge y = y \wedge x$

(ii) Per tot $x, y, z \in L$, $x \vee (y \vee z) = (x \vee y) \vee z$; $x \wedge (y \wedge z) = (x \wedge y) \wedge z$

(iii) Per tot $x \in L$, $x \vee x = x$; $x \wedge x = x$

(iv) Per tot $x, y \in L$, $x = x \vee (x \wedge y)$; $x = x \wedge (x \vee y)$

L'apartat de reticles es desenvolupa amb més detall en l'annex on es poden observar alguns exemples.

Definició 2.6. *Sigui X un conjunt d'elements que anomenem variables, τ un tipus algebraic, definim $T_\tau(X)$ com els termes de tipus τ en X ; que és el conjunt més petit que compleix:*

$$(i) \ X \cup \mathfrak{F}_0 \subseteq T_\tau(X).$$

$$(ii) \text{ Si } p_1, \dots, p_n \in T_\tau(X) \text{ i } f \in \mathfrak{F}, \text{ n-ària, } n > 0 \text{ aleshores la cadena } f(p_1, \dots, p_n) \in T_\tau(X).$$

Sigui τ i X , si $T_\tau(X) \neq \emptyset$. Anomenem l'àlgebra de termes $\mathbf{T}_\tau(X) = \langle T_\tau(X), \{f^{T_\tau(X)} : f \in \mathfrak{F}\} \rangle$ de tipus τ en X que té per univers a $T(X)$ i les seves operacions fonamentals són les $f^{T_\tau(X)} \in \mathfrak{F}$ de τ . Per tot $f \in \mathfrak{F}$, per tot $p_i \in T_\tau(X), 1 \leq i \leq n$ compleixen:

$$f^{T_\tau(X)}(p_1, \dots, p_n) = f(p_1, \dots, p_n).$$

Donat un terme $p(x_1, \dots, x_n) \in T_\tau(X)$, donada una àlgebra $\mathbf{A}$ del mateix tipus, podem definir una funció $p^{\mathbf{A}} : A^n \rightarrow A$ per recurrència sobre la construcció dels termes:

(i) Si p és una variable x_i , aleshores, $p^{\mathbf{A}}(a_1, \dots, a_n) = a_i \in A$ i.e., és la projecció i-èsima.

(ii) Si p és $f(p_1(x_1, \dots, x_n), \dots, p_k(x_1, \dots, x_n))$ tal que $f \in \mathfrak{F}$ k -ària, aleshores, $p^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{A}}(p_1^{\mathbf{A}}(a_1, \dots, a_n), \dots, p_k^{\mathbf{A}}(a_1, \dots, a_n))$.

Quan quedi clar la τ de $T_\tau(X)$, s'expressarà únicament com $T(X)$.

Exemple 4. Sigui τ format per una sola operació fonamental f tal que $\sigma(f) = 2$ i el conjunt $X = \{x_1, x_2\}$, l'àlgebra de termes $\mathbf{T}(X)$ conté alguns termes com $x_1, x_2, f(x_1, x_2), f(f(x_1, x_2), x_1) \dots$

Siguin $\mathbf{A}$ i $\mathbf{B}$ dues àlgebres del mateix tipus τ :

Definició 2.7. *Direm que $\mathbf{A}$ és una subàlgebra de $\mathbf{B}$, si $A \subseteq B$ i $f^{\mathbf{B}}|_A = f^{\mathbf{A}}$, per a tot $f \in \mathfrak{F}$, ho denotarem per $\mathbf{A} \leq \mathbf{B}$.*

Direm que A és un subunivers de $\mathbf{B}$, si és tancat per tota operació n -ària fonamental de $\mathbf{B}$, i.e., per a tot $f \in \mathfrak{F}$, i tot $a_1, \dots, a_n \in A$, tenim que $f^{\mathbf{A}}(a_1, \dots, a_n) \in A$.

Teorema 2.8. *Tot subunivers de $\mathbf{B} \neq \emptyset$ és univers d'una subàlgebra de $\mathbf{B}$.*

Demostració. Sigui A un subunivers de $\mathbf{B}$, aleshores és tancat per les operacions de $\mathbf{B}$, és a dir, per tot $f \in \mathfrak{F}$, i per tot $a_1, \dots, a_n \in A$, aleshores tenim que $f^{\mathbf{B}}(a_1, \dots, a_n) \in A$.

Observem, per tant, que podem definir l'àlgebra $\mathbf{A} = \langle A, \{f|_A^{\mathbf{B}} : f \in \mathfrak{F}\} \rangle$ i per tant $\mathbf{A} \leq \mathbf{B}$, on A és univers de $\mathbf{A}$. $\square$

Teorema 2.9. *Sigui $\{A_i : i \in I\}$ una família de subàlgebres de $\mathbf{B}$, si $\cap_{i \in I} A_i \neq \emptyset$, aleshores $\cap_{i \in I} A_i$ és subunivers de $\mathbf{B}$.*

Demostració. Sigui la intersecció $A = \cap_{i \in I} A_i$, i $f \in \mathfrak{F}$, una funció n -èsima. Certament es compleix que $A \subseteq B$. Per tot $b_1, \dots, b_n \in A$, tenim que $b_1, \dots, b_n \in A_i$, per tot $i \in I$. Com totes le A_i són subunivers de $\mathbf{B}$, aleshores $f^{\mathbf{B}}(b_1, \dots, b_n) \in A_i$ per tot $i \in I$. Això implica que $f^{\mathbf{B}}(b_1, \dots, b_n) \in A$. Per tant, A és tancat per f i podem afirmar que $A = \cap_{i \in I} A_i$ és subunivers de $\mathbf{B}$. $\square$

Definició 2.10. *Sigui $\mathbf{A}$ una àlgebra, per a tot $X \subseteq A$ definim el subunivers generat per X com:*

$$Sg(X) = \bigcap \{B : X \subseteq B, B \text{ subunivers de } A\}$$

Sabem que $Sg(X)$ existeix degut a que $A \subseteq A$, i per tant:

$\bigcap \{B : X \subseteq B, B \text{ subunivers de } A\} \neq \emptyset$, sempre contindrà com a mínim a A .

Definició 2.11. *Per a $X \subseteq A$, diem que X genera $\mathbf{A}$ (o X és el conjunt de generadors de $\mathbf{A}$) si $Sg(X) = A$.*

3 Homomorfismes

Considerem en tot moment que totes les àlgebres són del mateix tipus τ (excepte que s'indiqui el contrari).

Definició 3.1. Direm que $\alpha : A \rightarrow B$ és un homomorfisme si per a tot $f \in \mathfrak{F}$ tal que $\sigma(f) = n, a_1, \dots, a_n \in A$, compleix que:

$$\alpha(f^A(a_1, \dots, a_n)) = f^B(\alpha(a_1), \dots, \alpha(a_n)).$$

Ho denotarem per $\alpha : \mathbf{A} \rightarrow \mathbf{B}$.

Observem que $\alpha(f^A) = f^B$ si $\sigma(f) = 0$.

Teorema 3.2. Sigui $\alpha : A \rightarrow B$, α és un homomorfisme si, i només si, per tot $p \in T(X)$, si $\{x_1, \dots, x_n\}$ són les variables en p , aleshores per tot $a_1, \dots, a_n \in A$:

$$\alpha(p^A(a_1, \dots, a_n)) = p^B(\alpha(a_1), \dots, \alpha(a_n)).$$

Ho denotem per $\alpha : \mathbf{A} \rightarrow \mathbf{B}$

Demostració. Demostrem-ho per inducció sobre la construcció dels termes. Si $p = x_i \in X$, per $1 \leq i \leq n$, aleshores:

$$\alpha(p^A(a_1, \dots, a_n)) = \alpha(a_i) = p^B(\alpha(a_1), \dots, \alpha(a_n)).$$

Si $p = c$ tal que c és un element de $\mathfrak{F}$ amb $\sigma(c) = 0$, aleshores:

$$\alpha(p^A(a_1, \dots, a_n)) = \alpha(c) = p^B(\alpha(a_1), \dots, \alpha(a_n)).$$

Finalment, si $p = f(p_1, \dots, p_k)$ tal que $f \in \mathfrak{F}$, un símbol funcional k -èssim, $p_1, \dots, p_k \in T(X)$, aleshores:

$$p^A(a_1, \dots, a_n) = f^A(p_1^A(a_1, \dots, a_n), \dots, p_k^A(a_1, \dots, a_n)).$$

Veiem ara que es compleix la propietat desitjada:

$$\begin{aligned} \alpha(p^A(a_1, \dots, a_n)) &= \alpha(f^A(p_1^A(a_1, \dots, a_n), \dots, p_k^A(a_1, \dots, a_n))) \\ &= f^B(\alpha(p_1^A(a_1, \dots, a_n)), \dots, \alpha(p_k^A(a_1, \dots, a_n))) \\ &= f^B(p_1^B(\alpha(a_1), \dots, \alpha(a_n)), \dots, p_k^B(\alpha(a_1), \dots, \alpha(a_n))) \\ &= p^B(\alpha(a_1), \dots, \alpha(a_n)). \end{aligned}$$

□

Definició 3.3. Direm que $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ és un homomorfisme exhaustiu si $\alpha(A) = B$.

Definició 3.4. Direm que $\alpha : A \rightarrow B$ és una immersió si és un homomorfisme injectiu. Ho denotem per $\alpha : \mathbf{A} \hookrightarrow \mathbf{B}$.

Definició 3.5. Direm que $\alpha : A \rightarrow B$ és un isomorfisme si α és un homomorfisme exhaustiu i injectiu.

Indiquem que $\mathbf{A}$ és isomorf a $\mathbf{B}$ mitjançant $\mathbf{A} \cong \mathbf{B}$, és a dir, existeix un isomorfisme de $\mathbf{A}$ a $\mathbf{B}$.

Teorema 3.6. Donades dos àlgebres $\mathbf{A}, \mathbf{B}$, $\mathbf{A} \cong \mathbf{B}$ si, i només si, existeixen dos homomorfismes $h : \mathbf{A} \rightarrow \mathbf{B}, g : \mathbf{B} \rightarrow \mathbf{A}$ tal que $h \circ g = Id_B, g \circ h = Id_A$.

Teorema 3.7. Si $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ és un homomorfisme, aleshores $\alpha(A)$ és un subunivers de $\mathbf{B}$.

Demostració. Sigui $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un homomorfisme, per tot $f \in \mathfrak{F}, a_1, \dots, a_n \in A$ i sigui $b_1, \dots, b_n \in \alpha(A)$, és a dir, $b_1 = \alpha(a_1), \dots, b_n = \alpha(a_n)$, aleshores $f^{\mathbf{B}}(b_1, \dots, b_n) = f^{\mathbf{B}}(\alpha(a_1), \dots, \alpha(a_n)) = \alpha f^{\mathbf{A}}(a_1, \dots, a_n) \in \alpha(A)$; per tant $\alpha(A)$ és tancat per f i podem dir que és subunivers de $\mathbf{B}$. $\square$

Teorema 3.8. Suposem $\alpha : \mathbf{A} \rightarrow \mathbf{B}, \beta : \mathbf{B} \rightarrow \mathbf{C}$ dos homomorfismes. Aleshores tindrem que la composició $\beta \circ \alpha$ és un homomorfisme de $\mathbf{A}$ a $\mathbf{C}$.

Demostració. Per tot $f \in \mathfrak{F}$ i per tot $a_1, \dots, a_n \in A$ tenim que:

$$\begin{aligned} (\beta \circ \alpha)(f^{\mathbf{A}}(a_1, \dots, a_n)) &= \beta(\alpha(f^{\mathbf{A}}(a_1, \dots, a_n))) \\ &= \beta(f^{\mathbf{B}}(\alpha(a_1), \dots, \alpha(a_n))) = f^{\mathbf{C}}(\beta(\alpha(a_1)), \dots, \beta(\alpha(a_n))) \\ &= f^{\mathbf{C}}((\beta \circ \alpha)(a_1), \dots, (\beta \circ \alpha)(a_n)). \end{aligned} \quad \square$$

4 Congruències

Definició 4.1. *Sigui A un conjunt, sigui $r \subseteq A^2$, direm que r és una relació binària en A . Diem que r és una relació d'equivalència si:*

- (i) *Per tot $a \in A$, ara*
- (ii) *Per tot $a, b \in A$, $arb \Rightarrow bra$*
- (iii) *Per tot $a, b, c \in A$, arb i $brc \Rightarrow arc$.*

Denotem per $Eq(A)$ el conjunt de totes les relacions d'equivalència en A .

Donat un conjunt A , denotem $\Delta_A = \{(a, a) : a \in A\}$ com la relació diagonal i $\nabla_A = A \times A$ com la relació total en A . Excepte quan no quedi clar a quin conjunt es refereix indicarem la relació diagonal i total com Δ i ∇ respectivament.

Definició 4.2. *Donada una àlgebra $\mathbf{A}$ i una relació $\theta \in Eq(A)$. Aleshores tenim que θ és una congruència en $\mathbf{A}$ si per a tot $f \in \mathfrak{F}$ n -ària, per tot $a_i, b_i \in A$ tals que $a_i \theta b_i$ per $0 \leq i \leq n$, satisfà:*

$$f^{\mathbf{A}}(a_1, \dots, a_n) \theta f^{\mathbf{A}}(b_1, \dots, b_n).$$

El conjunt de totes les congruències en $\mathbf{A}$ l'anomenarem $Con(\mathbf{A})$.

Proposició 4.3. *$Con(\mathbf{A})$ és tancat per intersecció arbitrària.*

Demostració. Sigui $\{\theta_i, i \in I\} \subseteq Con(\mathbf{A})$, volem veure que $\bigcap_{i \in I} \theta_i \in Con(\mathbf{A})$.

En primer lloc veiem que $\bigcap_{i \in I} \theta_i$ és una relació d'equivalència en A . Per tot $a \in A$, com que $\theta_i \in Con(\mathbf{A})$ per tot $i \in I$, aleshores $(a, a) \in \theta_i$ per tot $i \in I$, per tant $(a, a) \in \bigcap_{i \in I} \theta_i$.

Per tot $a, b \in A$ si $(a, b) \in \bigcap_{i \in I} \theta_i$, aleshores per tot $i \in I$ tenim que $(a, b) \in \theta_i$, i per tant, $(b, a) \in \theta_i$. Com és cert per tot $i \in I$, obtenim que $(b, a) \in \bigcap_{i \in I} \theta_i$.

Per tot $a, b, c \in A$ tals que $(a, b) \in \bigcap_{i \in I} \theta_i$ i $(b, c) \in \bigcap_{i \in I} \theta_i$, aleshores per tot $i \in I$, com $\theta_i \in Con(\mathbf{A})$, $(a, b) \in \theta_i$ i $(b, c) \in \theta_i$, per tant $(a, c) \in \theta_i$. Com el resultat anterior passa per tot $i \in I$, tenim que $(a, c) \in \bigcap_{i \in I} \theta_i$. Per tant, podem afirmar que $\bigcap_{i \in I} \theta_i$ és una relació en A .

Per últim, veiem que és una congruència de $\mathbf{A}$. Sigui $a_1, \dots, a_n, b_1, \dots, b_n \in A$ tals que $(a_j, b_j) \in \bigcap_{i \in I} \theta_i$ per tot $1 \leq j \leq n$, aleshores $(a_j, b_j) \in \theta_i$ per tot $i \in I$ i per tot $1 \leq j \leq n$. Per tant, $f^{\mathbf{A}}(a_1, \dots, a_n) \theta_i f^{\mathbf{A}}(b_1, \dots, b_n)$ per tot $i \in I$, això implica que $f^{\mathbf{A}}(a_1, \dots, a_n) \in \bigcap_{i \in I} \theta_i f^{\mathbf{A}}(b_1, \dots, b_n)$. Per tant, $\bigcap_{i \in I} \theta_i \in Con(\mathbf{A})$. $\square$

Definició 4.4. *Sigui $\mathbf{A}$ una àlgebra i sigui $B \subseteq A \times A$, definim en primer lloc $\Phi(B) = \{\theta \in Con(\mathbf{A}) : B \subseteq \theta\}$. Definim $\Theta(B) = \bigcap \Phi(B)$ que correspon a*

l'operador de clausura algebraic finitament generat per B^1 .

Quan la congruència estigui generada per una sola parella d'elements $a, b \in A$, denotarem $\theta(a, b) = \Theta(\{(a, b)\})$. Sigui $a_1, \dots, a_n \in A$, definim $\Theta(a_1, \dots, a_n) = \Theta(\{(a_i, a_j) : 1 \leq i, j \leq n\})$.

Definició 4.5. Sigui $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$ definim les operacions $\vee$ i $\wedge$. Definim $\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2$. Definim la congruència generada per θ_1 i θ_2 de $\mathbf{A}$ com $\theta_1 \vee \theta_2 = \bigcap \{\theta' \in \text{Con}(\mathbf{A}) : \theta_1 \cup \theta_2 \subseteq \theta'\}$ que correspon a $\theta_1 \vee \theta_2 = \Theta(\theta_1 \cup \theta_2)$.

Definició 4.6. Sigui $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$, definim la composició $\theta_1 \circ \theta_2$, per $a, b \in A$, com $(a, b) \in \theta_1 \circ \theta_2$ si, i només si, existeix $c \in A$ tal que $(a, c) \in \theta_1$ i $(c, b) \in \theta_2$.

Si $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$ direm que θ_1 i θ_2 permuten. Una àlgebra $\mathbf{A}$ és congruent permutable si per tot $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$, θ_1 i θ_2 permuten.

Teorema 4.7. Sigui $\mathbf{A}$ una àlgebra, per tot $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$, per tot $a, b \in A$, direm que $(a, b) \in \theta_1 \vee \theta_2$ si, i només si, existeixen $a_1, \dots, a_n \in A$ tals que $a = a_1 \theta_1 a_2 \theta_2 a_3 \theta_1 \dots \theta_2 a_n = b$.

Demostració.

Sigui $\eta = \{(a, b) : \text{existeix } n \in \mathbb{N} \text{ i } a_1, \dots, a_n \in A \text{ tals que } a = a_1 \theta_1 a_2 \theta_2 a_3 \theta_1 \dots \theta_2 a_n = b\}$. Aleshores volem veure que $\theta_1 \vee \theta_2 = \eta$.

Si tenim que $(a, b) \in \eta$, aleshores $a = a_1 \theta_1 a_2 \theta_2 a_3 \theta_1 \dots \theta_2 a_n = b$, però com $\theta_1, \theta_2 \subseteq \theta_1 \vee \theta_2$ obtenim que $a = a_1 \theta_1 \vee \theta_2 a_2 \theta_1 \vee \theta_2 \dots \theta_1 \vee \theta_2 a_n = b$, per tant, per la transitivitat de $\theta_1 \vee \theta_2$, $(a, b) \in \theta_1 \vee \theta_2$. Aleshores, $\theta_1 \vee \theta_2 \supseteq \eta$.

Per veure l'altra inclusió és necessari veure que $\eta \in \text{Con}(\mathbf{A})$ i que $\theta_1 \cup \theta_2 \subseteq \eta$, ja que $\theta_1 \vee \theta_2 \subseteq \theta_1 \cup \theta_2$. Per tot $a \in A$, $(a, a) \in \eta$, ja que $a \theta_1 a \theta_2 a$. Per tot $a, b \in A$, si $(a, b) \in \eta$, aleshores existeixen $a_1, \dots, a_n \in A$ tals que $a = a_1 \theta_1 a_2 \theta_2 \dots \theta_1 a_{n-1} \theta_2 a_n = b$, però aleshores $b \theta_1 b \theta_2 a_{n-1} \theta_1 \dots \theta_2 a_2 \theta_1 a \theta_2 a$, per tant $(b, a) \in \eta$. Per tot $a, b, c \in A$ tals que $(a, b) \in \eta$, $(b, c) \in \eta$, aleshores tenim que existeixen $a_1, \dots, a_n, b_1, \dots, b_k \in A$ tals que $a = a_1 \theta_1 a_2 \theta_2 \dots \theta_1 a_{n-1} \theta_2 a_n = b$ i $b = b_1 \theta_1 b_2 \theta_2 \dots \theta_1 b_{k-1} \theta_2 b_k = c$, per tant, $a = a_1 \theta_1 a_2 \theta_2 \dots \theta_1 a_{n-1} \theta_2 a_n = b \theta_1 b \theta_2 b = b_1 \theta_1 b_2 \theta_2 \dots \theta_1 b_{k-1} \theta_2 b_k = c$, d'on obtenim que $(a, c) \in \eta$. Hem vist doncs que $\eta \in \text{Eq}(A)$.

Per tot $a_1, \dots, a_n, b_1, \dots, b_n \in A$ tals que $(a_i, b_i) \in \eta$ per tot $i \in \{1, \dots, n\}$, tenim que $a_i = c_1 \theta_1 \dots \theta_2 c_{n_i} = b$ per tot $i \in \{1, \dots, n\}$, on $n_i \in \mathbb{N}$ és diferent per cada parella (a_i, b_i) . Aleshores necessitem fer que la llargada donada per n_i , sigui la mateixa per tots. Sigui $n = \max_{i \in \{1, \dots, n\}}(n_i)$, aleshores per cada $i \in \{1, \dots, n\}$ i cada parella

¹Veure les definicions 12.18, 12.20 i 12.21 per els conceptes d'operador de clausura, operador de clausura algebraic i operador generat respectivament

$(a_i, b_i) \in \eta$, $a_i = c_1 \theta_1 \dots \theta_2 c_{n_i} = b \theta_1 b \theta_2 \dots \theta_2 b$ on hem allargat la cadena fins a tenir n termes. De manera que per $f \in \mathfrak{F}$, n -ària, $(f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)) \in \eta$, ja que com totes les cadenes tenen la mateixa llargada i $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$, ho tenim. Per tant $\eta \in \text{Con}(\mathbf{A})$.

Per últim veiem que si $(a, b) \in \theta_1 \cup \theta_2$, aleshores o $(a, b) \in \theta_1$ o $(a, b) \in \theta_2$. Si $(a, b) \in \theta_1$, aleshores $a \theta_1 b \theta_2 b$, per tant, $(a, b) \in \eta$. Si $(a, b) \in \theta_2$, aleshores $a \theta_2 b \theta_1 b$, per tant, $(a, b) \in \eta$. Tenim doncs que $\theta_1 \vee \theta_2 \subseteq \eta$. $\square$

Teorema 4.8. $\langle \text{Con}(\mathbf{A}), \vee, \wedge \rangle$ és un reticle acotat.

La demostració es pot trobar a l'annex, concretament correspon a la del Teorema 12.27.



Figura 1: Reticle de l'exemple 5

Exemple 5. Si tenim una àlgebra definida pel reticle lineal de la figura 1, $\mathbf{A} = \langle \{0, a, 1\}, \wedge, \vee \rangle$, les congruències estàn formades per:

$$\theta_1 := \theta(a, 1) = \Delta \cup \{(a, 1), (1, a)\}$$

$$\theta_2 := \theta(a, 0) = \Delta \cup \{(a, 0), (0, 1)\}$$

$$\theta(0, 1) = \nabla$$

$$\theta(a, a) = \Delta(0, 0) = \theta(1, 1) = \Delta.$$

Per tant, $\text{Con}(\mathbf{A}) = \{\Delta, \theta_1, \theta_2, \nabla\}$.

Definició 4.9. Una àlgebra $\mathbf{A}$ és congruent distributiva (congruent modular) si $\text{Con}(\mathbf{A})$ és un reticle distributiu (modular).²

Teorema 4.10. (Birkhoff). Si $\mathbf{A}$ és congruent permutable, aleshores és congruent modular.

Demostració. Sigui $\theta_1, \theta_2, \theta_3 \in \text{Con}(\mathbf{A})$, tal que $\theta_1 \subseteq \theta_2$. Volem veure que $\theta_2 \cap (\theta_1 \vee \theta_3) \subseteq \theta_1 \vee (\theta_2 \cap \theta_3)$. Observem que quan tenim congruent permutabilitat, $\theta_1 \circ \theta_2 = \theta_1 \vee \theta_2$, i per tant, considerant la definició de $\theta_1 \vee \theta_2$ tenim que $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2$.

²Veure les definicions 12.8 i 12.10 de l'annex.

Suposem que tenim un element $(a, b) \in \theta_2 \cap (\theta_1 \vee \theta_3)$, aleshores com $(a, b) \in \theta_1 \circ \theta_3$, existeix un element $c \in A$ tal que $a\theta_1 c\theta_2 b$. Per tant, com $(a, c) \in \theta_1$, per simetria $(c, a) \in \theta_2$. D'altra banda com $\theta_1 \subseteq \theta_2$, $(c, a) \in \theta_2$, i com $(a, b) \in \theta_2$, podem aplicar la transitiva i obtenim que $(c, b) \in \theta_2$.

D'altra banda, com $(c, b) \in \theta_3$, tenim que $(c, b) \in \theta_2 \cap \theta_3$. De manera que $a\theta_1 c\theta_2 \cap \theta_3 b$. Això equival a dir que $(a, b) \in \theta_1 \circ (\theta_2 \cap \theta_3)$ i per tant $\theta_2 \cap (\theta_1 \vee \theta_3) \subseteq \theta_1 \vee (\theta_2 \cap \theta_3)$. $\square$

Definició 4.11. Direm que una àlgebra $\mathbf{A}$ és 3-congruent permutable si per a tots els elements $\theta, \phi \in \text{Con}(\mathbf{A})$, tenim que $\theta \circ \phi \circ \theta \subseteq \phi \circ \theta \circ \phi$.

Teorema 4.12. (Jónsson) Si $\mathbf{A}$ és 3-congruent permutable, aleshores és congruent modular.

Demostració. En primer lloc veiem que com a propietat directe de la 3-permutabilitat tenim que per $(a, b) \in \theta_1 \vee \theta_3 \Rightarrow a\theta_1 c\theta_3 d\theta_1 b$.

Volem veure que si $\theta_1 \subseteq \theta_2$, $\theta_1 \vee (\theta_2 \wedge \theta_3) = \theta_2 \cap (\theta_1 \vee \theta_3)$.

$\subseteq$: Directe, degut a $\theta_1 \subseteq \theta_2$.

$\supseteq$: Sigui $(a, b) \in \theta_2 \cap (\theta_1 \vee \theta_3)$, aleshores $(a, b) \in \theta_2$ i existeixen c, d tals que $a\theta_1 c\theta_3 d\theta_1 b$. Com $\theta_1 \subseteq \theta_2$, $(a, c) \in \theta_2$ i $(d, b) \in \theta_2$, per tant $(c, d) \in \theta_2 \Rightarrow (c, d) \in \theta_2 \cap \theta_3$, veiem doncs que $a\theta_1 c\theta_2 \cap \theta_3 d\theta_1 b$ i per tant, $(a, b) \in \theta_1 \vee (\theta_2 \cap \theta_3)$. $\square$

Definició 4.13. Sigui A un conjunt i $\theta \in \text{Con}(\mathbf{A})$. Per tot $a \in A$, la classe d'equivalència de a mòdul θ és el conjunt $a/\theta = \{b \in A : (b, a) \in \theta\}$. El conjunt $\{a/\theta : a \in A\}$ el denotem per A/θ i l'anomenem conjunt quocient.

Denotem per $\mathbf{A}/\theta = \langle A/\theta, \{f^{A/\theta} : f \in \mathfrak{F}\} \rangle$ l'àlgebra quocient de A per θ que correspon a l'àlgebra on l'univers és el conjunt quocient A/θ i per tot $f \in \mathfrak{F}$, i tot $a_1, \dots, a_n \in A$:

$$f^{A/\theta}(a_1/\theta, \dots, a_n/\theta) = f^{\mathbf{A}}(a_1, \dots, a_n)/\theta.$$

Exemple 6. Mitjançant el proper exemple podem veure que els quocients vistos pels grups en les diferents assignatures que s'han cursat al llarg del grau corresponen al quocient que s'acaba de definir per àlgebres.

Sigui $\mathbf{G}$ un grup, es pot establir una correspondència 1 a 1 entre les congruències de $\mathbf{G}$ i els subgrups normals de $\mathbf{G}$.

Sigui $\theta \in \text{Con}(\mathbf{G})$; aleshores tenim que $1/\theta$ és l'univers d'un subgrup normal. De manera que si $\mathbf{N}$ és un subgrup normal de $\mathbf{G}$, tenim que $(a, b) \in \theta \Leftrightarrow a \cdot b^{-1} \in N$.

Exemple 7. Tanmateix el comentari respecte el quocient per als grups i el quocient definit en aquest apartat, també es pot aplicar per a anells. Sigui $\mathbf{R}$ un anell, es pot establir una correspondència 1 a 1 entre les congruències i els ideals de $\mathbf{R}$.

Sigui $\theta \in \text{Con}(\mathbf{R})$; aleshores tenim que $0/\theta$ és un ideal en $\mathbf{R}$. De manera que si $\mathbf{I}$ és un ideal de $\mathbf{R}$, tenim que $(a, b) \in \theta \Leftrightarrow a - b \in I$.

5 Teoremes de Isomorfia

Definició 5.1. *Sigui $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un homomorfisme. Anomenem nucli de α , que escriurem com $\ker(\alpha)$, a:*

$$\ker(\alpha) = \{(a, b) \in A^2 : \alpha(a) = \alpha(b)\}.$$

Teorema 5.2. *Sigui $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un homomorfisme. Aleshores $\ker(\alpha) \in \text{Con}(\mathbf{A})$.*

Demostració. Veiem en primer lloc que $\ker(\alpha)$ és una relació d'equivalència en $\mathbf{A}$. Per tot $a \in A$, $(a, a) \in \ker(\alpha)$, ja que $\alpha(a) = \alpha(a)$. Per tot $a, b \in A$, si $(a, b) \in \ker(\alpha)$, aleshores $\alpha(a) = \alpha(b)$, igualtat que també es compleix per $(b, a) \in \ker(\alpha)$. Per tot $a, b, c \in A$, si $(a, b) \in \ker(\alpha)$ i $(b, c) \in \ker(\alpha)$, aleshores $\alpha(a) = \alpha(b) = \alpha(c)$, per tant, $(a, c) \in \ker(\alpha)$.

Si $(a_i, b_i) \in \ker(\alpha)$ per $1 \leq i \leq n$ i $f \in \mathfrak{F}$ és n -ària en τ , aleshores:

$$\alpha(f^{\mathbf{A}}(a_1, \dots, a_n)) = f^{\mathbf{B}}(\alpha(a_1), \dots, \alpha(a_n))$$

$$f^{\mathbf{B}}(\alpha(b_1), \dots, \alpha(b_n)) = \alpha(f^{\mathbf{A}}(b_1, \dots, b_n)).$$

Per tant $(f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)) \in \ker(\alpha)$; d'on podem concloure fàcilment que $\ker(\alpha)$ és una congruència de $\mathbf{A}$. $\square$

Proposició 5.3. *Sigui $\mathbf{A}$ una àlgebra i $\theta \in \text{Con}(\mathbf{A})$. L'aplicació (natural):*

$$v_\theta : \mathbf{A} \rightarrow \mathbf{A}/\theta, \text{ definida } v_\theta(a) = a/\theta \text{ és un homomorfisme}$$

Demostració. Sigui $\theta \in \text{Con}(\mathbf{A})$, sigui l'aplicació natural $v : \mathbf{A} \rightarrow \mathbf{A}/\theta$. Per a $f \in \mathfrak{F}$ un signe funcional n -ària i $a_1, \dots, a_n \in A$. Tenim que:

$$v(f^{\mathbf{A}}(a_1, \dots, a_n)) = f^{\mathbf{A}}(a_1, \dots, a_n)/\theta = f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta) = f^{\mathbf{A}/\theta}(v(a_1), \dots, v(a_n)).$$

Per tant, v és un homomorfisme.

Teorema 5.4. *(Teorema de l'Homomorfia) Sigui $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ un homomorfisme exhaustiu. Aleshores existeix un isomorfisme β de $\mathbf{A}/\ker(\alpha)$ a $\mathbf{B}$ tal que $\alpha = \beta \circ v$; on v és l'homomorfisme natural entre $\mathbf{A}$ i $\mathbf{A}/\theta$.*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ & \searrow v & \uparrow \beta \\ & & A/\ker(\alpha) \end{array}$$

Demostració. Per tot $a \in A$, definim $\beta(a/\ker(\alpha)) := \alpha(a)$, veiem en primer lloc que la definició té sentit. Suposem $a' \in A$ tal que $(a, a') \in \ker(\alpha)$, aleshores

tenim que $\alpha(a) = \alpha(a')$. Per la definició de β , tenim que $\beta(a/\ker(\alpha)) = \alpha(a) = \alpha(a') = \beta(a'/\ker(\alpha))$, per tant, està ben definida i per la exhaustivitat de α i v , β també serà exhaustiva.

Veiem ara que α és injectiva. Per tot $a, a' \in A$ tals que $\beta(a/\ker(\alpha)) = \beta(a'/\ker(\alpha))$ aleshores $\alpha(a) = \alpha(a')$. Tenim doncs que $(a, a') \in \ker(\alpha)$ i això implica que $(a/\ker(\alpha)) = (a'/\ker(\alpha))$ i per tant β és injectiva.

Per últim veiem que β és un homomorfisme. Per comprovar això anem a suposar que f és una funció n -ària i $a_1, \dots, a_n \in A$, observem que:

$$\beta(f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta)) = \beta(f^{\mathbf{A}}(a_1, \dots, a_n)/\theta) = \alpha f^{\mathbf{A}}(a_1, \dots, a_n) = f^{\mathbf{B}}(\alpha a_1, \dots, \alpha a_n) = f^{\mathbf{B}}(\beta(a_1/\theta), \dots, \beta(a_n/\theta)).$$

Per tant, β és un isomorfisme. □

Alternativament aquest teorema també se'l coneix com a "Primer Teorema de la Isomorfia".

Definició 5.5. Sigui $\mathbf{A}$ una àlgebra i $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$, tals que $\theta_1 \subseteq \theta_2$.

$$\theta_2/\theta_1 = \{(a/\theta_1, b/\theta_1) \in (A/\theta_1)^2 : (a, b) \in \theta_2\}$$

Proposició 5.6. Si $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$, tals que $\theta_1 \subseteq \theta_2$, aleshores θ_2/θ_1 és congruència en $\mathbf{A}/\theta_1$.

Demostració. Sigui f un símbol funcional n -ari, suposem $(a_i/\theta_1, b_i/\theta_1) \in \theta_2/\theta_1$, $1 \leq i \leq n$. Aleshores $(a_i, b_i) \in \theta_2$, per tant:

$$(f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)) \in \theta_2 \Rightarrow (f^{\mathbf{A}}(a_1, \dots, a_n)/\theta_1, f^{\mathbf{A}}(b_1, \dots, b_n)/\theta_1) \in \theta_2/\theta_1$$

$$\text{D'on obtenim que } (f^{\mathbf{A}/\theta_1}(a_1/\theta_1, \dots, a_n/\theta_1), f^{\mathbf{A}/\theta_1}(b_1/\theta_1, \dots, b_n/\theta_1)) \in \theta_2/\theta_1$$

Teorema 5.7. (Segon Teorema de l'Isomorfia) Si $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$, tals que $\theta_1 \subseteq \theta_2$, aleshores la funció:

$$\alpha : (A/\theta_1)/(\theta_2/\theta_1) \rightarrow A/\theta_2$$

Definida per $\alpha((a/\theta_1)/(\theta_2/\theta_1)) = a/\theta_2$ és un isomorfisme.

Demostració.

Sigui $\beta : \mathbf{A}/\theta_1 \rightarrow \mathbf{A}/\theta_2$ definida de la manera següent: Per tot $a \in A$, $\beta(a/\theta_1) = a/\theta_2$ com $\theta_1 \subseteq \theta_2$ està ben definida, veiem en primer lloc que es tracta d'un homomorfisme. Anem a suposar que f és una funció n -ària i $a_1, \dots, a_n \in A$, observem que:

$$\begin{aligned} \beta(f^{\mathbf{A}/\theta}((a_1/\theta_1), \dots, (a_n/\theta_1))) &= \beta(f^{\mathbf{A}}(a_1, \dots, a_n)/\theta_1) = f^{\mathbf{A}}(a_1, \dots, a_n)/\theta_2 = \\ &= f^{\mathbf{A}/\theta_2}((a_1/\theta_2), \dots, (a_n/\theta_2)) = f^{\mathbf{A}/\theta_2}(\beta(a_1/\theta_1), \dots, \beta(a_n/\theta_1)). \end{aligned}$$

Per tant és un homomorfisme. A més β és exhaustiu, ja que tal com s'ha definit per tot element de A/θ_2 és imatge d'un element de A/θ_1 . Per $a, a' \in A$:

$$\ker(\beta) = \{(a/\theta_1, a'/\theta_1) \in \mathbf{A}/\theta_1 : (a, a') \in \theta_2\} = \theta_2/\theta_1.$$

Per tant, aplicant el primer teorema de l'isomorfia tenim que existeix α un isomorfisme entre $(A/\theta_1)/(\theta_2/\theta_1)$ i A/θ_2 . $\square$

Definició 5.8. Sigui B subconjunt de A i $\theta \in \text{Con}(\mathbf{A})$. Definim $B^\theta = \{a \in A : B \cap a/\theta \neq \emptyset\}$. Sigui $\theta \upharpoonright_B := \theta \cap B^2$, l'anomenarem restricció de θ en B .

Lema 5.9. Si $\mathbf{B}$ és subàlgebra de $\mathbf{A}$ i $\theta \in \text{Con}(\mathbf{A})$ tenim que:

- (i) $\mathbf{B}^\theta = \langle B^\theta, \{f^{\mathbf{A}}|_{B^\theta} : f \in \mathfrak{F}\} \rangle$ és una subàlgebra de $\mathbf{A}$ amb univers B^θ .
- (ii) $\theta \upharpoonright_B$ és una congruència en $\mathbf{B}$.

Demostració. Sigui $f \in \mathfrak{F}$ un símbol funcional n -àri de $\mathbf{A}$, sigui $a_1, \dots, a_n \in B^\theta$, podem trobar $b_1, \dots, b_n \in B$ tals que $(a_i, b_i) \in \theta, 1 \leq i \leq n$. Com tots els elements a_i, b_i són de A , tenim que $(f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)) \in \theta$ i per tant, $f^{\mathbf{A}}(a_1, \dots, a_n) \in B^\theta$. Aleshores, B^θ és subunivers de $\mathbf{A}$.

Veiem ara que $\theta \upharpoonright_B$ és congruència en $\mathbf{B}$. És evident que $\theta \upharpoonright_B$ compleix amb les condicions per ser equivalència en B , ja que com $\theta \in \text{Con}(\mathbf{A})$, θ compleix les condicions per ser de $\text{Eq}(A)$, però com $B \subseteq A$, aquestes condicions es compleixen per tot element de $\mathbf{B}$ i per tant, $\theta \cap B^2 \in \text{Eq}(B)$.

D'altra banda, per la definició de $\theta \upharpoonright_B$, per $a_1, \dots, a_n, b_1, \dots, b_n \in B$ tals que $(a_i, b_i) \in \theta \upharpoonright_B, 1 \leq i \leq n$, aleshores $(f^{\mathbf{B}}(a_1, \dots, a_n), f^{\mathbf{B}}(b_1, \dots, b_n)) \in \theta \upharpoonright_B$, ja que $\mathbf{B}$ és subàlgebra de $\mathbf{A}$ i per tant $\theta \upharpoonright_B$ és congruència en $\mathbf{B}$. $\square$

Teorema 5.10. (Tercer Teorema de l'Isomorfia) Si $\mathbf{B}$ és subàlgebra de $\mathbf{A}$ i $\theta \in \text{Con}(\mathbf{A})$ tenim que:

$$\mathbf{B}/\theta \upharpoonright_B \cong \mathbf{B}^\theta/\theta \upharpoonright_{B^\theta}$$

Demostració. Sigui f la composició d'homomorfismes següent: $\mathbf{B} \rightarrow \mathbf{B}^\theta \rightarrow \mathbf{B}^\theta/\theta \upharpoonright_{B^\theta}$, com la composició d'homomorfismes és un homomorfisme, podem afirmar que f és un homomorfisme. Veiem que f és exhaustiva, agafem un element $a/(\theta \upharpoonright_{B^\theta}) \in \mathbf{B}^\theta/\theta \upharpoonright_{B^\theta}$. Com $a \in B^\theta$, existeix $b \in B$ tal que $(a, b) \in \theta$. Però aleshores tenim que $f(a) = a/(\theta \upharpoonright_{B^\theta}) = b/(\theta \upharpoonright_{B^\theta}) = f(b)$ i per tant, $\ker(f) = \theta \upharpoonright_B$. Aplicant el primer teorema d'isomorfia al homomorfisme exhaustiu f obtenim el resultat buscat. $\square$

Degut a que els teoremes d'isomorfia són vàlids per qualsevol tipus d'àlgebra, en podem trobar fàcilment la seva correspondència ja coneguda per grups i per anells. Veiem-ho:

Exemple 8. Pel cas del grups, els teoremes d'isomorfia tindrien els següents enuncisats:

- (i) Siguin G, F dos grups tals que $\alpha : G \twoheadrightarrow F$ morfisme de grups, existeix $\beta : G/\ker(\alpha) \rightarrow F$ tal que $G/\ker(\alpha) \cong F$.
- (ii) Siguin N, H subgrups normals de G tals que $N \triangleleft H$. Aleshores tenim que $G/H \cong (G/N)/(H/N)$.
- (iii) N, H subgrups de G , $N \triangleleft G$, subgrup normal. Aleshores tenim que $H/(H \cap N) \cong (H + N)/N$.

Exemple 9. Pel cas dels anells, els teoremes d'isomorfia tindrien els següents enuncisats:

- (i) Siguin A, B dos anells tals que $\alpha : A \twoheadrightarrow B$ morfisme d'anells, existeix $\beta : A/\ker(\alpha) \rightarrow B$ tal que $A/\ker(\alpha) \cong B$.
- (ii) Siguin I, J dos ideals de A tals que $I \subseteq J$. Aleshores tenim que $A/J \cong (A/I)/(J/I)$.
- (iii) I, J subanells de A , I ideal de A . Aleshores tenim que $J/(I \cap J) \cong (I + J)/J$.

Teorema 5.11. (*Teorema de Correspondència*) *Sigui $\mathbf{A}$ una àlgebra i $\theta \in \text{Con}(\mathbf{A})$. La funció α definida en $[\theta, \nabla_A]$, $\phi \in [\theta, \nabla_A]$, per $\alpha(\phi) = \phi/\theta$ és un isomorfisme entre els reticles $[\theta, \nabla_A]$ i $\mathbf{Con}(\mathbf{A})/\theta^3$. Observem que $[\theta, \nabla_A]$ és un subreticle⁴ de $\mathbf{Con}(\mathbf{A})$.*

Teorema 5.12. *Donats dos homomorfismes $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ i $\beta : \mathbf{A} \rightarrow \mathbf{C}$, si tenim que $\ker(\beta) \subseteq \ker(\alpha)$ i β és exhaustiu; aleshores existeix un homomorfisme $\gamma : \mathbf{C} \rightarrow \mathbf{B}$ tal que $\alpha = \gamma \circ \beta$.*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ & \searrow \beta & \uparrow \gamma \\ & & C \end{array}$$

Demostració. Suposem, en primer lloc, que γ existeix i satisfà $\alpha = \gamma \circ \beta$. Volem veure, doncs, que $\ker(\beta) \subseteq \ker(\alpha)$, sigui $(a, b) \in \ker(\beta)$, $\beta(a) = \beta(b)$, i per tant, $\gamma(\beta(a)) = \gamma(\beta(b))$ que seria el mateix que $\gamma \circ \beta(a) = \gamma \circ \beta(b)$. Com que $\alpha = \gamma \circ \beta$, $\alpha(a) = \alpha(b) \Rightarrow (a, b) \in \ker(\alpha)$, com volíem veure.

³En l'observació posterior a la definició 12.6 de l'annex s'explica què és un isomorfisme entre reticles

⁴En la definició 12.6 de l'annex s'explica que és un subreticle.

Tanmateix si suposem que $\ker(\beta) \subseteq \ker(\alpha)$, definim $\gamma = \alpha \circ \beta^{-1}$, on β^{-1} és una aplicació de $\mathbf{C}$ a $\mathbf{A}$ tal que per tot $c \in C$, $\beta^{-1}(c) = a, a \in A$ sabem que està ben definida ja que β és exhaustiva. Volem veure que γ té les propietats desitjades. El domini de γ ha de ser C degut a l'exhaustivitat de β . Sigui $c \in C$ i $a_1, a_2 \in A$ tals que $\beta(a_1) = \beta(a_2) = c \Rightarrow (a, b) \in \ker(\beta) \Rightarrow (a, b) \in \ker(\alpha)$. Per tant, $\gamma(c) = \alpha \circ \beta^{-1}(c)$ dóna el mateix resultat independentment dels elements a_1, a_2 que usem. Per tant, γ és una funció ben definida de C a B .

Ens queda veure que γ és realment un homomorfisme, suposem $f^{\mathbf{C}}$ una funció n -ària. Sigui $c_1, \dots, c_n \in C$ tal que $g^{-1}(c_i) = a_i, 1 \leq i \leq n$, aleshores:

$$\begin{aligned} \gamma(f^{\mathbf{C}}(c_1, \dots, c_n)) &= \gamma(f^{\mathbf{C}}(\beta(a_1), \dots, \beta(a_n))) = \gamma(\beta(f^{\mathbf{A}}(a_1, \dots, a_n))) = f^{\mathbf{B}}((\gamma \circ \\ &\beta)(a_1), \dots, (\gamma \circ \beta)(a_n)) = f^{\mathbf{B}}(\gamma(c_1), \dots, \gamma(c_n)), \end{aligned}$$

ja que $\alpha = \gamma \circ \beta$ és un homomorfisme. □

6 Producte Directe i Productes Subdirectes

Definició 6.1. Sigui $\mathbf{A}_1, \mathbf{A}_2$ dues àlgebres del mateix tipus τ . Definim el producte directe $\mathbf{A}_1 \times \mathbf{A}_2$, l'àlgebra que té per univers el conjunt $A_1 \times A_2$ i que per $f \in \mathfrak{F}$ n -ària, $a_i \in A_1, a'_i \in A_2, 1 \leq i \leq n$:

$$f^{\mathbf{A}_1 \times \mathbf{A}_2}((a_1, a'_1), \dots, (a_n, a'_n)) = (f^{\mathbf{A}_1}(a_1, \dots, a_n), f^{\mathbf{A}_2}(a'_1, \dots, a'_n))$$

La funció projecció i -èssima de $\mathbf{A}_1 \times \mathbf{A}_2$ és:

$$\pi_i : \mathbf{A}_1 \times \mathbf{A}_2 \rightarrow \mathbf{A}_i, i \in \{1, 2\},$$

$$\pi_i((a_1, a_2)) = a_i.$$

Teorema 6.2. La funció projecció i -èssima és un homomorfisme exhaustiu de $\mathbf{A}_1 \times \mathbf{A}_2$ a $\mathbf{A}_i, i \in 1, 2$. A més, en $\mathbf{Con}(\mathbf{A}_1 \times \mathbf{A}_2)$ es compleix:

$$(i) \ker(\pi_1) \cap \ker(\pi_2) = \Delta.$$

$$(ii) \ker(\pi_1) \text{ i } \ker(\pi_2) \text{ permuten.}$$

$$(iii) \ker(\pi_1) \vee \ker(\pi_2) = \nabla.$$

Demostració. Sigui $f \in \mathfrak{F}$ n -ària, per tot $a_i \in A_1, a'_i \in A_2, 1 \leq i \leq n$, llavors:

$$\pi_1(f^{\mathbf{A}}((a_1, a'_1), \dots, (a_n, a'_n))) = \pi_1((f^{\mathbf{A}_1}(a_1, \dots, a_n), f^{\mathbf{A}_2}(a'_1, \dots, a'_n))) = f^{\mathbf{A}_1}(a_1, \dots, a_n) = f^{\mathbf{A}_1}(\pi_1((a_1, a'_1)), \dots, \pi_1((a_n, a'_n))),$$

Per tant π_1 és un homomorfisme i és trivial veure que és exhaustiu. Anàlogament es pot argumentar per π_2 .

Per tot $i \in \{1, 2\}$, sigui $((a_1, a_2), (b_1, b_2)) \in \ker(\pi_i)$ si, i només si, $\pi_i((a_1, a_2)) = \pi_i((b_1, b_2))$, aleshores $a_i = b_i$, per tant $\ker(\pi_1) \cap \ker(\pi_2) = \Delta$.

D'altra banda, per tot $(a_1, a_2), (b_1, b_2)$ elements de $A_1 \times A_2$:

$$(a_1, a_2)\ker(\pi_1)(a_1, b_2)\ker(\pi_2)(b_1, b_2), \text{ veiem doncs que } \ker(\pi_1) \vee \ker(\pi_2) = \nabla \text{ i per tant } \ker(\pi_1) \text{ i } \ker(\pi_2) \text{ permuten.}$$

Per últim, tenim que $\nabla = \ker(\pi_1) \circ \ker(\pi_2) \subseteq \ker(\pi_1) \vee \ker(\pi_2)$, però com permuten tenim l'igualtat i d'aquesta manera obtenim (iii). $\square$

Definició 6.3. Sigui $\mathbf{A}$ una àlgebra i una congruència $\theta \in \mathbf{Con}(\mathbf{A})$ s'anomena congruència factor si existeix $\theta^* \in \mathbf{Con}(\mathbf{A})$ tal que:

$$\theta \cap \theta^* = \Delta,$$

$$\theta \vee \theta^* = \nabla,$$

$$\theta \text{ i } \theta^* \text{ permuten.}$$

Anomenem parella de congruències factor en $\mathbf{A}$ a θ i θ^* .

Teorema 6.4. Si θ i θ^* és una parella de congruències factor en $\mathbf{A}$, aleshores:

$$\mathbf{A} \cong \mathbf{A}/\theta \times \mathbf{A}/\theta^*$$

usant la funció $\alpha(a) = (a/\theta, a/\theta^*)$.

Definició 6.5. Direm que una àlgebra $\mathbf{A}$ és directament indecomposable si $\mathbf{A}$ no és isomorfa a un producte directe de dues àlgebres no trivials

Generalitzant la primera definició de producte directe es pot obtenir la següent, més completa.

Definició 6.6. Sigui $(\mathbf{A}_i)_{i \in I}$ una família indexada d'àlgebres de tipus τ . Definim el producte directe $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$ com l'àlgebra amb univers $\prod_{i \in I} A_i$ i que per $f \in \mathfrak{F}$ n -ària, $a_1, \dots, a_n \in \prod_{i \in I} A_i$:

$$f^{\mathbf{A}}(a_1, \dots, a_n)(i) = f^{\mathbf{A}_i}(a_1(i), \dots, a_n(i)),$$

per tot $i \in I$.

Sigui $j \in I$, definim:

$$\pi_j : \prod_{i \in I} \mathbf{A}_i \rightarrow \mathbf{A}_j$$

$$\pi_j(a) = a(j)$$

que ens dona homomorfismes π_j exhaustius.

En general no existeix una immersió entre $\mathbf{A}_i$ i $\prod_{i \in I} \mathbf{A}_i$. En alguns casos concrets, com el dels grups si que existeix degut a l'existència d'una subàlgebra trivial.

Teorema 6.7. Tota àlgebra finita és isomorfa a un producte directe d'àlgebres directament indecomposables.

Demostració. Resolem per inducció completa sobre el nombre d'elements de $|A|$. Sigui $\mathbf{A}$ una àlgebra finita, si és trivial, el resultat és evident. Suposem que no ho és i a més per a cada $\mathbf{B}$ tal que $|B| < |A|$ sabem que $\mathbf{B}$ és un producte d'àlgebres indecomposables. Si $\mathbf{A}$ és indecomposable hem acabat, sinó $\mathbf{A} \cong \mathbf{A}_1 \times \mathbf{A}_2$. Tenim doncs que $|A_1|, |A_2| < |A|$ i per hipòtesis d'inducció:

$$\mathbf{A}_1 \cong \mathbf{B}_1 \times \dots \times \mathbf{B}_m,$$

$$\mathbf{A}_2 \cong \mathbf{C}_1 \times \dots \times \mathbf{C}_n,$$

on $\mathbf{C}_j, \mathbf{B}_i$ son indecomposables; per tant, $\mathbf{A} \cong (\mathbf{B}_1 \times \dots \times \mathbf{B}_m) \times (\mathbf{C}_1 \times \dots \times \mathbf{C}_n) \cong \mathbf{B}_1 \times \dots \times \mathbf{B}_m \times \mathbf{C}_1 \times \dots \times \mathbf{C}_n$, també ho és. $\square$

Definició 6.8. Sigui $a_1, a_2 \in A$ i $\alpha : A \rightarrow B$ una funció, es diu que α separa a_1 i a_2 si $\alpha(a_1) \neq \alpha(a_2)$. Direm que α separa punts de l'àlgebra $\mathbf{A}$, si per tot $a, b \in A$, $a \neq b$, aleshores $\alpha(a) \neq \alpha(b)$.

Definició 6.9. Donada una col·lecció d'aplicacions $\alpha_i : A \rightarrow A_i, i \in I$, definim l'aplicació $\alpha : A \rightarrow \prod_{i \in I} A_i$ per $\alpha(a)(i) = \alpha_i(a)$ per tot $i \in I$.

Proposició 6.10. Sigui $\alpha_i : A \rightarrow A_i$ una família d'homomorfismes indexats per $i \in I$, i sigui $\alpha : A \rightarrow \prod_{i \in I} A_i$. Els següents enuncisats són equivalents:

- (i) Les funcions α_i separa punts de A .
- (ii) α és injectiva.
- (iii) $\bigcap_{i \in I} \ker(\alpha_i) = \nabla$.

Demostració. (i) $\Rightarrow$ (ii) Suposem $a_1, a_2 \in A$ tals que $a_1 \neq a_2$. Aleshores per cert $i \in I$, $\alpha_i(a_1) \neq \alpha_i(a_2)$ de manera que $\alpha(a_1)(i) \neq \alpha(a_2)(i)$, per tant $\alpha(a_1) \neq \alpha(a_2)$.

(ii) $\Rightarrow$ (iii) Per $a_1, a_2 \in A$ tals que $a_1 \neq a_2$, tenim que $\alpha(a_1) \neq \alpha(a_2)$, per tant $\alpha(a_1)(i) \neq \alpha(a_2)(i)$ per cert $i \in I$; obtenim doncs que $\alpha_i(a_1) \neq \alpha_i(a_2)$ i això implica que $(a_1, a_2) \notin \ker(\alpha_i)$; per tant $\bigcap_{i \in I} \ker(\alpha_i) = \nabla$.

(iii) $\Rightarrow$ (i) Per $a_1, a_2 \in A$ tals que $a_1 \neq a_2$, $(a_1, a_2) \notin \bigcap_{i \in I} \ker(\alpha_i)$, per tant per a cert $i \in I$, $(a_1, a_2) \notin \ker(\alpha_i)$, d'on obtenim que $\alpha_i(a_1) \neq \alpha_i(a_2)$. $\square$

Definició 6.11. Direm que una àlgebra A és un producte subdirecte d'una família d'àlgebres $(A_i)_{i \in I}$ si: $A \leq \prod_{i \in I} A_i$ i $\pi_i(A) = A_i$, per tot $i \in I$.

Una immersió $\alpha : A \rightarrow \prod_{i \in I} A_i$ és subdirecte si $\alpha(A)$ és un producte subdirecte de $\{A_i\}_{i \in I}$.

Proposició 6.12. Sigui A una àlgebra i $\theta_i \in \text{Con}(A)$, per tot $i \in I$. Si $\bigcap_{i \in I} \theta_i = \Delta$; aleshores, l'homomorfisme (natural) $v : A \rightarrow \prod_{i \in I} A/\theta_i$, on $v(a) = (a/\theta_i)_{i \in I}$, és una immersió subdirecta.

Demostració. Sigui $v_i : A \rightarrow A/\theta_i$, per $i \in I$, com $\ker(v_i) = \theta_i$, de la proposició 6.10, dedim que v és una immersió. Com v_i és exhaustiva, v és una immersió subdirecte. $\square$

Definició 6.13. Una àlgebra A és subdirectament irreductible si per tota immersió subdirecte $\alpha : A \rightarrow \prod_{i \in I} A_i$, existeix $i \in I$ tal que $\pi_i \circ \alpha : A \rightarrow A_i$ és un isomorfisme

Definició 6.14. $\theta \in \text{Con}(A)$ és completament intersecció irreductible si per $\{\theta_i; i \in I\} \subseteq \text{Con}(A)$, si $\theta = \bigcap_{i \in I} \theta_i$, aleshores $\theta = \theta_i$, per cert $i \in I$.

Alternativament es pot definir de la següent forma:

Teorema 6.15. Una àlgebra A és subdirectament irreductible si, i només si, A és trivial o existeix una congruència mínima en $\text{Con}(A) - \{\Delta\}$. Si aquest element existeix, i no ens trobem en el cas trivial, serà $\bigcap(\text{Con}(A) - \{\Delta\})$.

Demostració. ($\Rightarrow$) Resolem-ho per contrarecíproc. Si $\mathbf{A}$ no és trivial i $\text{Con}(\mathbf{A}) - \{\Delta\}$ no té element mínim, aleshores $\bigcap(\text{Con}(\mathbf{A}) - \{\Delta\}) = \Delta$. Sigui $I = \text{Con}(\mathbf{A}) - \{\Delta\}$, aleshores l'aplicació $\alpha : \mathbf{A} \rightarrow \prod_{\theta \in I} \mathbf{A}/\theta$ és una immersió subdirecte per la proposició anterior, i com l'aplicació $\mathbf{A} \rightarrow \mathbf{A}/\theta$ no és injectiva per cap $\theta \in I$ (ja que $\theta \neq \Delta$), es dedueix que $\mathbf{A}$ no pot ser subdirectament irreductible.

($\Leftarrow$) Sigui $\alpha : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}_i$ una immersió subdirecte; si $\mathbf{A}$ és trivial aleshores les $\mathbf{A}_i$ també són trivials; ja que $\pi_i \circ \alpha$ és un isomorfisme.

Suposem ara que $\mathbf{A}$ no és trivial, sigui $\theta = \bigcap(\text{Con}(\mathbf{A}) - \{\Delta\}) \neq \Delta$, ja que $\text{Con}(\mathbf{A}) - \{\Delta\}$ té mínim. Sigui $a, b \in A$ tals que $a \neq b$ i $(a, b) \in \theta$, aleshores per $\alpha : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}_i$ és una immersió subdirecte, i a més $\alpha(a) \neq \alpha(b)$. Per tant, existeix $i \in I$ tal que $\alpha(a)(i) \neq \alpha(b)(i)$; per tant $(\pi_i \circ \alpha)(a) \neq (\pi_i \circ \alpha)(b)$. Aleshores $(a, b) \notin \ker(\pi_i \circ \alpha)$, per tant $\theta \not\subseteq \ker(\pi_i \circ \alpha)$. Però això implica que $\ker(\pi_i \circ \alpha) = \Delta$, i aleshores $\pi_i \circ \alpha$ seria un isomorfisme; per tant $\mathbf{A}$ és subdirectament irreductible.

Si $\text{Con}(\mathbf{A}) - \{\Delta\}$ té un element mínim θ ; aleshores per tot $a \neq b$ tal que $(a, b) \in \theta$ tenim que $\theta(a, b) \subseteq \theta$, d'on deduem que $\theta = \theta(a, b)$. $\square$

Teorema 6.16. *Una àlgebra subdirectament irreductible és directament indecomposable.*

Demostració. És evident que les úniques congruències factors que té una àlgebra subdirectament irreductible són Δ i ∇ ; per tant, pels teoremes 6.2 i 6.4 tenim que l'àlgebra és directament indecomposable. $\square$

Teorema 6.17. (Birkhoff) *Cada àlgebra $\mathbf{A}$ és isomorfa a un producte subdirecte d'àlgebres subdirectament irreductibles.*

Demostració. Com les àlgebres trivials són subdirectament irreductible, tant sols, hem de considerar el cas d'una àlgebra no trivial $\mathbf{A}$. Sigui $\Theta_{a,b} = \{\theta \in \text{Con}(A) : (a, b) \notin \theta\}$ és evident que es tracta d'un conjunt parcialment ordenat no buit. Fent ús del lema de Zorn, al tractar-se d'un conjunt parcialment ordenat no buit on tot subconjunt parcialment ordenat té una cota superior, aleshores tenim una cota maximal i podem trobar una congruència $\theta_{a,b} \in \text{Con}(A)$ que és maximal respecte a la propietat $(a, b) \notin \theta_{a,b}$. Tenim doncs que $\Theta(a, b) \vee \theta_{a,b}$ és la més petita de les congruències de $[\theta_{a,b}, \nabla] - \{\theta_{a,b}\}$ pel teorema 6.15 veiem que $A/\theta_{a,b}$ és subdirectament irreductible. Com $\bigcap\{\theta_{a,b} : a \neq b\} = \Delta$ podem aplicar la proposició 6.12 per veure que existeix una immersió subdirecte de $\mathbf{A}$ al producte d'una família indexada d'àlgebres subdirectament irreductibles $(\mathbf{A}/\theta_{a,b})_{a \neq b}$. $\square$

Teorema 6.18. *$\mathbf{A}/\theta$ és subdirectament irreductible si, i només si θ és completament intersecció irreductible. En particular, $\mathbf{A}$ és subdirectament irreductible si, i només si, Δ és completament intersecció irreductible.*

Demostració. Suposem en primer lloc que $\mathbf{A}$ és subdirectament irreductible. Per veure que Δ és completament intersecció irreductible, sigui $\{\theta_i : i \in I\} \subseteq \text{Con}(\mathbf{A})$, suposem que $\Delta = \bigcap_{i \in I} \theta_i$. Volem veure doncs que per cert $i \in I, \theta_i = \Delta$. Per la proposició 6.12 l'aplicació natural $\mathbf{A} \rightarrow \prod_{i \in I} \mathbf{A}/\theta_i$ és una representació subdirecte. A més, per cert $i \in I, \pi_i : \mathbf{A} \rightarrow \mathbf{A}/\theta_i$ és un isomorfisme. Per tant $\theta_i = \ker(\pi_i) = \Delta$.

Veient l'altra implicació, suposem que Δ és completament intersecció irreductible i suposem que $\alpha : \mathbf{A} \rightarrow \prod_{i \in I} \mathbf{B}_i$ és una representació subdirecte. Per la mateixa proposició anterior tenim que per tot $\{\theta_i : i \in I\} \subseteq \text{Con}(\mathbf{A}), \theta_i = \ker(\pi_i \circ \alpha)$, això implica per la proposició anterior que $\bigcap_{i \in I} \theta_i = \Delta$.

Per tant existeix $i \in I$ tal que $\theta_i = \Delta$, per tant, $\ker(\pi_i \circ \alpha) = \Delta$ d'on obtenim que $\pi_i \circ \alpha$ és un isomorfisme.

Pel cas general, sigui θ una congruència, pel teorema de correspondència 5.11 els reticles $[\theta, \nabla]$ i $\text{Con}(\mathbf{A}/\theta)$ són isomorfs. Per tant, $\mathbf{A}/\theta$ és subdirectament irreductible. $\square$

Corol·lari 6.19. *$\mathbf{A}/\theta$ és subdirectament irreductible si, i només si, Δ/θ és completament intersecció irreductible en $\text{Con}(\mathbf{A}/\theta)$ si, i només si, θ és completament intersecció irreductible en $\text{Con}(\mathbf{A})$.*

Demostració. La prova d'aquest corol·lari és directe aplicant el teorema 6.18.

7 Varietats

Definició 7.1. *Sigui K la classe d'àlgebres similars, definim els següents operadors:*

- (i) $\mathbf{A} \in I(K)$ si, i només si, $\mathbf{A}$ és isomorf a algun membre de K .
- (ii) $\mathbf{A} \in S(K)$ si, i només si, $\mathbf{A}$ és subàlgebra d'algun membre de K .
- (iii) $\mathbf{A} \in H(K)$ si, i només si, $\mathbf{A}$ és la imatge homomorfa d'algun membre de K .
- (iv) $\mathbf{A} \in P(K)$ si, i només si, $\mathbf{A}$ és producte directe d'una família no buida d'àlgebres de K .
- (v) $\mathbf{A} \in P_s(K)$ si, i només si, $\mathbf{A}$ és producte subdirecte d'una família no buida d'àlgebres de K .

Notació. Siguin O_1, O_2 dos operadors de classes d'àlgebres, escriurem $O_1 O_2$ per indicar la composició de dos operadors. Sigui $\leq$ una relació binària en $\{I, S, H, P, P_s\}$. Denotarem per $O_1 \leq O_2$, quan $O_1(K) \subseteq O_2(K)$, per tot classe d'àlgebres K . Direm que l'operador és idempotent quan $O^2 = O$. Indicarem que una classe K d'àlgebres és tancada per un operador O quan $O(K) \subseteq K$.

Lema 7.2. *H, S i IP son idempotents. A més, les desigualtats següents són certes: $SH \leq HS, PS \leq SP$ i $PH \leq HP$.*

Demostració. Veure que H, S i IP són idempotents és trivial, veiem la resta de desigualtats. Suposem $\mathbf{A} \in SH(K)$. Aleshores existeix $\mathbf{B} \in K$ i un homomorfisme exhaustiu $\alpha : \mathbf{B} \rightarrow \mathbf{C}$, tal que $\mathbf{A} \leq \mathbf{C}$. Com $\mathbf{A} \leq \mathbf{C}$, considerant l'homomorfisme $\alpha^{-1} : \mathbf{C} \rightarrow \mathbf{B}$, tenim que $\alpha^{-1}(A) \leq \alpha^{-1}(C) = B$ i per l'homomorfisme exhaustiu anterior $\alpha(\alpha^{-1}(A)) = A$, per tant, $\mathbf{A} \in HS(K)$.

Sigui $\mathbf{A} \in PS(K)$, aleshores existeixen $\{B_i\}_{i \in I} \subseteq K$ tals que $A_i \subseteq B_i$, per tot $i \in I$ i $A = \prod_{i \in I} A_i$. Degut a que $\prod_{i \in I} A_i \leq \prod_{i \in I} B_i$ i $\prod_{i \in I} B_i \in P(K)$, tenim que $\mathbf{A} \in SP(K)$.

Per últim, si $\mathbf{A} \in PH(K)$, aleshores existeixen $\{B_i\}_{i \in I} \subseteq K$ i una família d'homomorfismes exhaustius $\alpha_i : B_i \rightarrow A_i, i \in I$ tal que $\mathbf{A} = \prod_{i \in I} A_i$. Es comprova fàcilment que $\alpha : \prod_{i \in I} B_i \rightarrow \prod_{i \in I} A_i$ és un homomorfisme exhaustiu; i per tant, $\mathbf{A} \in HP(K)$. $\square$

Al 1972, Pigozzi va determinar el reticle format pels 18 operadors generats per H, S, P (Veure: Figura 2).

Definició 7.3. *Anomenem varietat a una classe K (no buida) d'àlgebres del mateix tipus que està tancada sota H, S i P (i.e. $H(K) \subseteq K, S(K) \subseteq K, P(K) \subseteq K$).*

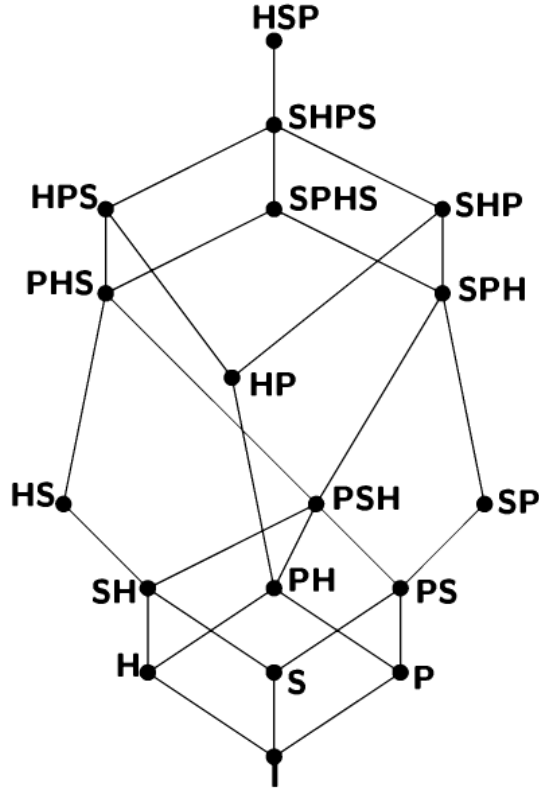


Figura 2: Operadors generats per H,S,P

Sigui $\{V_i\}_{i \in I}$ una família de varietats tal que totes les àlgebres són de tipus τ , volem veure que $\bigcap_{i \in I} V_i$ és una varietat. Tenim que la intersecció és no nul·la, ja que com a mínim contindrà l'àlgebra trivial. Volem veure que $H(\bigcap_{i \in I} V_i) \subseteq \bigcap_{i \in I} V_i$, $S(\bigcap_{i \in I} V_i) \subseteq \bigcap_{i \in I} V_i$ i $P(\bigcap_{i \in I} V_i) \subseteq \bigcap_{i \in I} V_i$. Tenim que per tota àlgebra $\mathbf{A} \in H(\bigcap_{i \in I} V_i)$, aleshores existeix $\mathbf{B} \in \bigcap_{i \in I} V_i$ tal que per cert homomorfisme α , $\alpha(\mathbf{B}) = \mathbf{A}$. Com $\mathbf{B} \in \bigcap_{i \in I} V_i$, tenim que per tot $i \in I$, $\mathbf{B} \in V_i$, i per tant, com V_i és una varietat i està tancada per H , $\alpha(\mathbf{B}) = \mathbf{A} \in V_i$, com això es compleix per tot $i \in I$, tindrem que $\mathbf{A} \in \bigcap_{i \in I} V_i$ i per tant, $H(\bigcap_{i \in I} V_i) \subseteq \bigcap_{i \in I} V_i$. Observem que podem fer una argumentació anàloga pels operadors S i P , de manera que obtenim $S(\bigcap_{i \in I} V_i) \subseteq \bigcap_{i \in I} V_i$ i $P(\bigcap_{i \in I} V_i) \subseteq \bigcap_{i \in I} V_i$. Tenim doncs que $\bigcap_{i \in I} V_i$ és varietat.

Per K , una classe d'àlgebres, sigui ν varietat, definim $V(K) = \bigcap \{\nu : K \subseteq \nu\}$ que és la varietat més petita que conté K , aleshores direm que $V(K)$ és la varietat generada per K .

Teorema 7.4. (Tarski) $V=HSP$. És a dir, la varietat generada per K una classe d'àlgebres, $V(K)$, és el mateix que la composició dels operadors H , S , P aplicats en K , $HSP(K)$.

Demostració. Sigui K una classe d'àlgebres, per veure que $HSP(K)$ és una

varietat usarem el lema anterior:

$$H(HSP) = HSP, S(HSP) \leq HS^2P = HSP, P(HSP) \leq HSP^2 = HSP.$$

Com $HV = SV = IPV = V$ i $I \leq V$, deduïm que $HSP \leq HSPV = V$. Tenim doncs que per qualsevol K , $HSP(K)$ és tancat sota H, S, P i és la més petita de les varietats contingudes en K , per tant, $V = HSP$. $\square$

Exemple 10. Sigui K la classe dels semigrups, pel fet de ser semigrups tenim que compleixen que $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Veiem que K és tancat per HSP de manera que sigui varietat.

Sigui α un homomorfisme entre les àlgebres $\mathbf{A} = \langle A; f \rangle$ i $\mathbf{B} = \langle B; g \rangle$, $\alpha(A)$ segueix sent semigrup, sigui $a, b, c \in B$, tals que $a = \alpha(x), b = \alpha(y), c = \alpha(z)$, on $x, y, z \in A$:

$$\alpha(f(x, f(y, z))) = g(\alpha(x), \alpha(f(y, z))) = g(\alpha(x), g(\alpha(y), \alpha(z))).$$

Per tant $H(K) \subseteq K$.

Tenim també que $S(K) \subseteq K$. Ja que per $\mathbf{A}$ subàlgebra de $\mathbf{B}$, tenim que $A \subseteq B$ i $f^{\mathbf{A}} = f^{\mathbf{B}}|_A$. Per tant conserva la propietat per ser semigrup i pertany a K .

Per últim és evident que $P(K) \subseteq K$, ja que donada una família de semigrups $G_i, i \in I$, aleshores per $G \leq \prod_{i \in I} G_i$, tenim que els elements de G compleixen la propietat de semigrup, ja que tots els elements de cada G_i la compleix

Com $P(K)$ és semigrup, $S(P(K))$ també ho és i $H(S(P(K)))$ també ho serà; tenim doncs que $HSP(K) \subseteq K$ i per tant, és varietat.

Definició 7.5. Anomenarem cos a una àlgebra $\langle K, +, \cdot, -, 0, 1 \rangle$ amb símbols funcionals d'ordre $\langle 2, 2, 1, 0, 0 \rangle$ respectivament, i K un conjunt, a més compleix que:

- (i) $\langle K, +, \cdot, -, 0 \rangle$ és un anell commutatiu.
- (ii) El neutre 1 és una operació nul·laria tal que $1 \cdot a = a \cdot 1 = 1$, per tot $a \in K$. A més, $0 \neq 1$.
- (iii) Tot element no nul del cos és invertible, és a dir, per tot $a \in K$ existeix $b \in K$ tal que $a \cdot b = 1$.

Exemple 11. Sigui K la classe dels cossos, veiem que no és una varietat. Pel teorema 7.4 n'hi ha prou en veure que K no és tancat per un dels tres operadors H, S o P , ja que si no ho és per un, aleshores $HSP(K)$ no pot ser tancat. Veiem que els cossos no estan tancats per $P(K)$.

Un domini d'integritat és un anell commutatiu tal que $1 \neq 0$ i no té més divisors de zero que el zero. Els cossos són domini d'integritat, veiem-ho. Sigui $\mathbf{R} \in K$ un

cos, per $a \in R, a \neq 0$, podem considerar cert $b \in R$ tal que $a \cdot b = 1$. Sigui $c \in R$ tal que $c \cdot a = 0, 0 = 0 \cdot b = c \cdot a \cdot b = c \cdot 1 = c$, per tant l'únic divisor de zero és zero en un cos.

Siguin $\mathbf{R}, \mathbf{Q} \in K$ dos cossos, veiem que el producte directe $\mathbf{R} \times \mathbf{Q}$ no és domini d'integritat ja que podem agafar $(1, 0), (0, 1) \in R \times Q$ tals que $(1, 0) \times (0, 1) = (0, 0)$. Tenim doncs un divisor de zero diferent a zero, per tant, no és domini d'integritat i no pot ser un cos. Hem vist que $P(K)$ no és tancat i podem afirmar que la classe dels cossos no és una varietat.

Teorema 7.6. *Sigui K una varietat, aleshores cada membre de K és isomorf a un producte subdirecte de membres irreductibles de K . Ho denotem per $K = P_S(K_{SI})$.*

Demostració. Sigui $\mathbf{A}$ una àlgebra de K . Pel teorema 6.17, $\mathbf{A}$ té una representació de productes subdirectes d'àlgebres subdirectament irreductibles $\prod_{i \in I} \mathbf{A}_i$, on $\{\mathbf{A}_i : i \in I\}$ és una família d'àlgebres subdirectament irreductibles. Per cada $i \in I$, l'aplicació projecció $\pi_i : \mathbf{A} \rightarrow \mathbf{A}_i$ és un homomorfisme exhaustiu. Tanmateix, $\mathbf{A}_i \in H(\mathbf{A}) \subseteq K$. Per tant, $\mathbf{A} \in P_S(K_{SI})$, és a dir, $K \subseteq P_S(K_{SI})$. Per l'invers n'hi ha prou en veure que $P_S(K_{SI}) \subseteq SP(K_{SI}) \subseteq SP(K) \subseteq K$. $\square$

8 Àlgebres Lliures

Definició 8.1. Sigui K una classe d'àlgebres de tipus τ i sigui $\mathbf{U}(X)$ una àlgebra del mateix tipus generada per X . Direm que $\mathbf{U}(X)$ té la propietat universal d'aplicacions sobre K amb conjunt de generadors X si per tot $\mathbf{A} \in K$, i per qualsevol:

$\alpha : X \rightarrow A$ existeix un homomorfisme $\beta : \mathbf{U}(X) \rightarrow \mathbf{A}$ tal que és una extensió de α ($\beta(x) = \alpha(x)$, per tot $x \in X$).

Anomenem a X conjunt de generadors lliures de $\mathbf{U}(X)$, i $\mathbf{U}(X)$ està lliurament generat per X .

Lema 8.2. Sigui $\mathbf{U}(X)$ tal que té la propietat universal d'aplicacions sobre K amb conjunt de generadors X . Si tenim $\mathbf{A} \in K$ i $\alpha : X \rightarrow A$; β extensió de α aleshores β és única.

Teorema 8.3. Siguin $\mathbf{U}_1(X_1) \in K$ i $\mathbf{U}_2(X_2) \in K$, K classe d'àlgebres, amb la propietat universal d'aplicacions per K en els conjunts indicats; si $|X_1| = |X_2|$, aleshores, $\mathbf{U}_1(X_1) \cong \mathbf{U}_2(X_2)$.

Demostració. Degut a que X_1, X_2 tenen la mateixa cardinalitat, podem definir una bijecció $\alpha : X_1 \rightarrow X_2$. Com $\mathbf{U}_2(X_2) \in K$ i $\mathbf{U}_1(X_1)$ està lliurament generat, existeix un homomorfisme $\beta_1 : \mathbf{U}_1(X_1) \rightarrow \mathbf{U}_2(X_2)$ que extén α . Anàlogament per $\mathbf{U}_2(X_2)$ i una funció $\beta_2 : \mathbf{U}_2(X_2) \rightarrow \mathbf{U}_1(X_1)$ que extén α^{-1} .

Veiem que $\beta_2 \circ \beta_1$ és un homomorfisme exhaustiu de $\mathbf{U}_1(X_1)$ que és una extensió de la funció identitat en X_1 , igual que la extensió en $\mathbf{U}_1(X_1)$. Pel lema anterior $\beta_2 \circ \beta_1$ és l'identitat en $\mathbf{U}_1(X_1)$. S'argumenta ànalogament per veure que $\beta_1 \circ \beta_2$ és la identitat en $\mathbf{U}_2(X_2)$. I obtenim que $\mathbf{U}_1(X_1) \cong \mathbf{U}_2(X_2)$. $\square$

Teorema 8.4. Sigui X un conjunt no buit i τ un tipus, l'àlgebra de termes $\mathbf{T}(X)$ té la propietat universal d'aplicacions per la classe de totes les àlgebres de tipus τ amb conjunt de generadors X .

Demostració. Sigui $\alpha : X \rightarrow A$, on $\mathbf{A}$ és de tipus τ . Definim $\beta : \mathbf{T}(X) \rightarrow A$ de la següent forma:

- (i) Per $x \in X$: $\beta(x) = \alpha(x)$.
- (ii) Per $p_1, \dots, p_n \in \mathbf{T}(X)$, $f \in \mathfrak{F}$ n -ària: $\beta(f(p_1, \dots, p_n)) = f^{\mathbf{A}}(\beta(p_1), \dots, \beta(p_n))$. Aleshores $\beta(p(x_1, \dots, x_n)) = p^{\mathbf{A}}(\alpha(x_1), \dots, \alpha(x_n))$ i β és l'homomorfisme d'extensió desitjat. $\square$

A continuació es presentaran dues definicions alternatives per al concepte d'àlgebra lliure que en realitat consisteix en una representació alternativa de la mateixa definició mitjançant un isomorfisme.

Definició 8.5. Sigui K una classe d'àlgebres de tipus τ i X un conjunt. Direm que B , una àlgebra de tipus τ , és lliure en K en un conjunt de generadors X , si B té la propietat universal d'aplicacions amb conjunt de generadors X i $B \in K$.

Alternativament veiem que:

Sigui K una família d'àlgebres de tipus τ . Donat un conjunt X de variables definim la congruència $\theta_K(X)$ de $\mathbf{T}(X)$ com:

$$\theta_K(X) = \bigcap \Phi_K(X), \text{ on } \Phi_K(X) = \{\phi \in \text{Con } \mathbf{T}(X) : \mathbf{T}(X)/\phi \in IS(K)\}.$$

Anomenarem $\mathbf{F}_K(\bar{X}) := \mathbf{T}(X)/\theta_K(X)$ l'àlgebra lliure sobre K amb conjunt de generadors $\bar{X}$, on $\bar{X} = X/\theta_K(X)$.

Sigui $\mathbf{F}_K(\bar{X})$ l'àlgebra lliure sobre K en $\bar{X}$, denotem per $\bar{x}$ als elements de la forma $x/\theta_K(X)$, $x \in X$. Per $p(x_1, \dots, x_n) \in T(X)$, denotem $\bar{p}$ pels elements de la forma $p^{\mathbf{F}_K(\bar{X})}(\bar{x}_1, \dots, \bar{x}_n)$.

Teorema 8.6. (Birkhoff) Supposem que $\mathbf{T}(X)$ existeix, aleshores, $\mathbf{F}_K(\bar{X})$ té la propietat universal d'aplicacions sobre K amb conjunt de generadors $\bar{X}$.

Demostració. Sigui $A \in K$, $\alpha : \bar{X} \rightarrow A$ una funció. Si $v : \mathbf{T}(X) \rightarrow \mathbf{F}_K(\bar{X})$ és l'homomorfisme natural, aleshores, $\alpha \circ v : X \rightarrow A$ i per la propietat universal de funcions hi ha un homomorfisme $\mu : \mathbf{T}(X) \rightarrow A$ que exté $\alpha \circ v \upharpoonright_X$. Per la definició de $\theta_K(X)$, $\theta_K(X) \subseteq \ker(\mu)$. Per tant hi ha un homomorfisme $\beta : \mathbf{F}_K(\bar{X}) \rightarrow A$ tal que $\mu = \beta \circ v$. Però aleshores, per $x \in X$, $\beta(\bar{x}) = \beta \circ v(x) = \mu(x) = \alpha \circ v(x) = \alpha(\bar{x})$.

Per tant, β és extensió de α i podem afirmar que $\mathbf{F}_K(\bar{X})$ té la propietat universal de funcions sobre K en $\bar{X}$. $\square$

Teorema 8.7. Sigui K una família d'àlgebres de tipus τ , si A és lliure en K amb conjunt de generadors X (i.e. A té la propietat universal d'aplicacions sobre K amb conjunt de generadors X i $A \in K$). Tenim que $A \cong \mathbf{F}_K(\bar{X})$.

Demostració. Sigui $\alpha : X \rightarrow A$ una immersió. Com A és una àlgebra de tipus τ , pel lema 8.2, $\alpha : X \rightarrow A$ es pot estendre mitjançant $\beta : \mathbf{T}(X) \rightarrow A$. Aquest homomorfisme és exhaustiu, ja que la seva imatge conté $\alpha(X)$ que genera A . Pel teorema de la homomorfia tenim doncs que A és isomorf al quocient $\mathbf{T}(X)/\ker(\beta)$. Només ens queda provar que $\ker(\beta) = \theta_K(X)$.

Com $A \in K$, tenim que $\theta_K(X) \subseteq \ker(\beta)$, per la definició del conjunt $\theta_K(X)$. Falta veure que $\ker(\beta) \subseteq \theta_K(X)$. Per qualsevol $B \in K$ definim una funció $f : X \rightarrow B$. Com A té la propietat universal de funcions, podem veure que hi ha un únic homomorfisme $f' : A = U(X) \rightarrow B$ que exté f . Però, aleshores, $f' \circ \beta$ es l'únic homomorfisme de $\mathbf{T}(X)$ a B que exté f , i per tant, tenim que $\ker(\beta) \subseteq \ker(f' \circ \beta)$, que ens mostra el que volíem, $\ker(\beta) \subseteq \theta_K(X)$. $\square$

Corol·lari 8.8. *Segui K una classe d'àlgebres de tipus τ i $\mathbf{A} \in K$, aleshores, per X suficientment gran, $\mathbf{A} \in H(\mathbf{F}_K(\bar{X}))$*

Teorema 8.9. *Segui $\mathbf{T}(X)$, tal que $X \neq 0$ o $\mathfrak{F}_0 \neq \emptyset$ aleshores, per $K \neq \emptyset$ tenim que $\mathbf{F}_K(\bar{X}) \in ISP(K)$. Si a més, K és varietat, aleshores $\mathbf{F}_K(\bar{X}) \in K$.*

Demostració. Per la definició de $\theta_K(X)$, $\mathbf{F}_K(\bar{X}) = \mathbf{T}(X)/\theta_K(X) \in IP_s(\{\mathbf{T}(X)/\theta : \theta \in \Phi_K(X)\}) \Rightarrow \mathbf{F}_K(\bar{X}) \in IP_s IS(K)$, però degut a que $P_s \leq SP$, $\mathbf{F}_K(\bar{X}) \in ISP(K)$. $\square$

Corol·lari 8.10. *Si K és una varietat d'àlgebres de tipus τ , X un conjunt, tal que $X \cup \mathfrak{F}_0 \neq \emptyset$, existeix $F_K(\bar{X})$ lliure en K .*

Demostració. Per la definició 8.5 com K és una varietat, podem interpretar-la com una classe d'àlgebres del mateix tipus i per tant podem construir $F_K(\bar{X})$ sense cap problema, a més pel teorema 8.7 si $F_K(\bar{X})$ existeix serà lliure. $\square$

9 Identitats i Teorema de Birkhoff

Definició 9.1. Sigui X un conjunt, donat un llenguatge τ , definim el conjunt d'identitats com $Id_\tau(X) = \{p \approx q; p, q \in T_\tau(X)\}$.

Sigui $p \approx q \in Id_\tau(X)$ i $\mathbf{A}$ una τ -àlgebra, direm que $\mathbf{A}$ satisfà la identitat $p \approx q$, $\mathbf{A} \models p \approx q$, quan si $\{(x_1, \dots, x_n)\} \subseteq X$ és el conjunt de variables de p i q , per tot $a_1, \dots, a_n \in A$:

$$p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n).$$

Donada una classe K d'àlgebres, direm que $K \models p \approx q \Leftrightarrow \mathbf{A} \models p \approx q$ per a tot $\mathbf{A} \in K$.

Sigui $\Sigma \subseteq Id_\tau(X)$, $\mathbf{A} \models \Sigma$ si $\mathbf{A} \models p \approx q$ per tot $p \approx q \in \Sigma$.

Altrament, $K \models \Sigma$ si $K \models p \approx q$ per tot $p \approx q \in \Sigma$.

Definim $Id_K(X) = \{p \approx q \in Id_\tau(X) : K \models p \approx q\}$.

Quan no hi hagi dubte sobre el tipus τ , indicarem $Id(X)$ per $Id_\tau(X)$.

Lema 9.2. Sigui K una classe d'àlgebres de tipus τ i $p \approx q \in Id_\tau(X)$ una identitat del mateix tipus en X , aleshores $K \models p \approx q$ si, i només si, per tot $\mathbf{A} \in K$ i per cada homomorfisme $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ es compleix que $\alpha(p) = \alpha(q)$.

Demostració. ($\Rightarrow$) Suposem que $K \models p \approx q$. Sigui $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ tal que pel teorema 2.2 $\alpha(p) = p^{\mathbf{A}}(\alpha(x_1), \dots, \alpha(x_n))$ i $\alpha(q) = q^{\mathbf{A}}(\alpha(x_1), \dots, \alpha(x_n))$. Aleshores com $K \models p \approx q$ tenim que $\mathbf{A} \models p \approx q$. Això implica per tant que per tot $a_1, \dots, a_n \in A$, $p^{\mathbf{A}}(\alpha(a_1), \dots, \alpha(a_n)) = q^{\mathbf{A}}(\alpha(a_1), \dots, \alpha(a_n)) = \alpha(q)$ obtenint el resultat que volíem.

($\Leftarrow$) Ara volem veure que qualsevol àlgebra $\mathbf{A} \in K$ de tipus τ i $a_1, \dots, a_n \in A$ compleixen la identitat, i.e., $p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n)$. Sigui $\alpha_0 : X \rightarrow A$ una funció tal que $\alpha_0(x_i) = a_i, 1 \leq i \leq n$. Pel teorema 8.2, α_0 es pot estendre a un homomorfisme $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$. Com suposem que $\alpha(p) = \alpha(q)$, tenim que $p^{\mathbf{A}}(a_1, \dots, a_n) = p^{\mathbf{A}}(\alpha(x_1), \dots, \alpha(x_n)) = \alpha(p^{\mathbf{T}(X)}(x_1, \dots, x_n)) = \alpha(p) = \alpha(q) = q^{\mathbf{A}}(\alpha(x_1), \dots, \alpha(x_n)) = q^{\mathbf{A}}(a_1, \dots, a_n)$. $\square$

Lema 9.3. Per qualsevol classe K de tipus τ , les classes $K, I(K), S(K), H(K), P(K)$ i $V(K)$ satisfan les mateixes identitats en qualsevol conjunt de variables X .

Demostració. Sigui $K \subseteq K'$ implica que $Id_{K'} \subseteq Id_K$. Volem veure que $K, I(K), S(K), H(K), P(K)$ i $V(K)$ satisfan els mateixes identitats en X . Per tant voldrem veure que $Id_K \subseteq Id_{S(K)}, Id_{H(K)}, Id_{P(K)}, Id_{I(K)}$.

Sigui $K \models p \approx q$, $\mathbf{A} \in K$, aleshores $\mathbf{A} \models p \approx q$. Sigui $\mathbf{B} \in S(K)$ aleshores $\mathbf{B} \leq \mathbf{A}$ per alguna $\mathbf{A} \in K$ veiem que:

$p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n)$ per tot $a_1, \dots, a_n \in A$, en particular, $p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n)$ per tot $a_1, \dots, a_n \in B \Rightarrow p^{\mathbf{B}}(a_1, \dots, a_n) = q^{\mathbf{B}}(a_1, \dots, a_n)$ per tot $a_1, \dots, a_n \in B \Rightarrow B \models p \approx q$. Tenim doncs que $Id_K \subseteq Id_{S(K)}$.

Sigui $\mathbf{B} \in H(K)$ aleshores existeix $A \in K$ tal que $\mathbf{B} \in H(\{\mathbf{A}\})$. Existeix doncs un homomorfisme $\alpha : \mathbf{A} \rightarrow \mathbf{B}$, de manera que sigui $b_1, \dots, b_n \in B$, existeixen $a_1, \dots, a_n \in A$ tals que $b_1 = \alpha(a_1), \dots, b_n = \alpha(a_n)$ i s'observa que:

$$p^{\mathbf{B}}(b_1, \dots, b_n) = p^{\mathbf{B}}(\alpha(a_1), \dots, \alpha(a_n)) = \alpha(p^{\mathbf{A}}(a_1, \dots, a_n)) = \alpha(q^{\mathbf{A}}(a_1, \dots, a_n)) = q^{\mathbf{B}}(\alpha(a_1), \dots, \alpha(a_n)) = q^{\mathbf{B}}(b_1, \dots, b_n).$$

Obtenint doncs que $Id_K \subseteq Id_{H(K)}$.

Sigui $\{A_i\}_{i \in I} \subseteq K$ una família d'àlgebres. Com $K \models p \approx q$ aleshores $\mathbf{A}_i \models p \approx q$, per tot $i \in I$. Sigui $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$, $a_1, \dots, a_n \in A$.

Com que per tot $i \in I$, $A_i \models p \approx q$, aleshores $p^{\mathbf{A}_i}(a_1(i), \dots, a_n(i)) = q^{\mathbf{A}_i}(a_1(i), \dots, a_n(i)) \Leftrightarrow$

Per tot $i \in I$, $p^{\mathbf{A}}(a_1, \dots, a_n)(i) = q^{\mathbf{A}}(a_1, \dots, a_n)(i) \Leftrightarrow p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n)$.

Obtenim doncs que $\mathbf{A} \models p \approx q$ i per tant $Id_{P(K)}(X) = Id_K(X)$.

$I(K)$ satisfà les identitats degut a que tenim que $I \leq H$, aleshores $Id_{H(K)} \subseteq Id_{I(K)} \subseteq Id_K$, com hem vist que $Id_{H(K)} = Id_K$ aleshores $Id_{I(K)} = Id_K$.

Per últim pel teorema 7.4 tenim que $V = HSP$ i per tant $V(K)$ satisfà també les identitats degut als últims tres casos. $\square$

El següent teorema en permet establir una connexió entre les àlgebres lliures i les identitats.

Definició 9.4. Sigui X un conjunt i K una classe d'àlgebres de tipus τ , per tot $p \in T(X)$ indicarem $\bar{p} = p/\theta_K(X)$, on $\theta_K(X)$ ve donat per la definició 8.5.

Teorema 9.5. Donada una classe d'àlgebres K de tipus τ i els termes $p, q \in T(X)$ del mateix tipus, tenim:

$$K \models p \approx q \Rightarrow \mathbf{F}_K(\bar{X}) \models p \approx q \Rightarrow \bar{p} = \bar{q} \text{ en } \mathbf{F}_K(\bar{X}).$$

Observació. Podem afegir que $\bar{p} = \bar{q}$ en $\mathbf{F}_K(\bar{X}) \Leftrightarrow (p, q) \in \theta_K(X)$.

Demostració. Sigui $v : \mathbf{T}(X) \rightarrow \mathbf{F}_K(\bar{X})$ l'homomorfisme natural. Si $K \models p \approx q$, com $\mathbf{F}_K(\bar{X}) \in ISP(K)$, aleshores pel lema anterior, $\mathbf{F}_K(\bar{X}) \models p \approx q$. La següent implicació és trivial degut a que $\mathbf{F}_K(\bar{X}) \models p \approx q$ implica que $p^{\mathbf{F}_K(\bar{X})}(x_1/\theta_K(X), \dots, x_n/\theta_K(X)) = q^{\mathbf{F}_K(\bar{X})}(x_1/\theta_K(X), \dots, x_n/\theta_K(X)) \Leftrightarrow \bar{p} = \bar{q}$. $\square$

Sigui p, q tals que $\bar{p} = \bar{q}$ en $\mathbf{F}_K(\bar{X})$, equivalentment $v(p) = v(q)$, aleshores és

evident que $(p, q) \in \theta_K(X)$ ($= \ker(v)$).

Només queda una implicació per veure, suposem que $(p, q) \in T(X)$. Donat $\mathbf{A} \in K$ i $a_1, \dots, a_n \in A$ sigui $\alpha : \mathbf{T}(X) \rightarrow \mathbf{A}$ tal que $\alpha(x_i) = a_i, 1 \leq i \leq n$, com $\ker(\alpha) \in \Phi_K(X)$ tenim que $\ker(\alpha) \supseteq \ker(v) = \theta_K(X)$, d'on podem extreure que existeix un homomorfisme $\beta : \mathbf{F}_K(\bar{X}) \rightarrow \mathbf{A}$ tal que $\alpha = \beta \circ v$. Tenim doncs que $\alpha(p) = (\beta \circ v)(p) = (\beta \circ v)(q) = \alpha(q)$; per tant pel lema 9.2, $K \models p \approx q$.

Corol·lari 9.6. *Segui K una classe d'àlgebres de tipus τ , $p, q \in T(X)$. Per qualsevol conjunt de variables Y tal que $|X| \leq |Y|$ es compleix que $K \models p \approx q \Leftrightarrow \mathbf{F}_K(\bar{Y}) \models p \approx q$.*

Corol·lari 9.7. *Segui K una classe d'àlgebres de tipus τ i X un conjunt. Aleshores, per qualsevol conjunt infinit de variables Y , $\text{Id}_K(X) = \text{Id}_{\mathbf{F}_K(\bar{Y})}(X)$.*

Demostració. Si es té que $p \approx q \in \text{Id}_K(X)$, $p(x_1, \dots, x_n) = q(x_1, \dots, x_n)$, es té que $p, q \in T(\{x_1, \dots, x_n\})$. Com $|\{x_1, \dots, x_n\}| < |Y|$, pel corol·lari anterior, $K \models p \approx q \Leftrightarrow \mathbf{F}_K(\bar{Y}) \models p \approx q$. $\square$

Definició 9.8. *Segui Σ un conjunt d'identitats de tipus τ , definim $\text{Mod}(\Sigma) = \{\mathbf{A} : \mathbf{A} \models \Sigma, \mathbf{A} \text{ de tipus } \tau\}$. Es diu que una classe K és equacional si existeix $\Sigma \subseteq \text{Id}_\tau(X)$ tal que $K = \text{Mod}(\Sigma)$, aleshores es diu que K està definida o axiomatitzada per Σ . On $\text{Mod}(\Sigma)$ s'anomena classe de models de Σ .*

Proposició 9.9. *Segui K una classe d'àlgebres, Σ un conjunt d'identitats i X un conjunt, $K \subseteq \text{Mod}(\text{Id}_K(X))$, $\Sigma \subseteq \text{Id}_{\text{Mod}(\Sigma)}(X)$, $\text{Id}_{\text{Mod}(\text{Id}_K(X))}(X) = \text{Id}_K(X)$ i $\text{Mod}_{\text{Id}(\text{Mod}(\Sigma))} = \text{Mod}(\Sigma)$.*

El resultat presentat a continuació és conegut com el Teorema de Birkhoff. En primer lloc, serà enunciat tal i com es pot trobar en la majoria de llibres sobre àlgebra universal. En segon lloc, serà enunciat tal i com el va presentar Birkhoff per primera vegada.

Teorema 9.10. *K és una classe equacional si, i només si, K és una varietat.*

Demostració.

Suposem que $K = \text{Mod}(\Sigma)$. Volem veure que és varietat, com l'operador V és de clausura, $K \subseteq V(K)$, volem veure l'altre inclusió per veure que K és una varietat. Per això usant que $V(K) \models \Sigma$ i pel lema 9.3, tenim que $V(K) \subseteq \text{Mod}(\Sigma)$ de manera que podem afirmar que $K = V(K)$, i.e. la classe equacional és una varietat.

Falta veure que si K és varietat aleshores K és de classe equacional. N'hi ha prou en veure que si V és varietat i X un conjunt infinit de variables, aleshores

$V = \text{Mod}(Id_V(X))$, i.e. si V és una varietat aquesta està axiomatitzada per $Id_V(X)$ i per tant és equacional. Sigui $V' = \text{Mod}(Id_V(X))$ clarament V' és varietat pel lema 9.3 que donada una classe, en aquest cas V' , té les mateixes identitats que la varietat obtinguda d'ella, i tenim doncs que $V \subseteq V', Id_{V'}(X) = Id_V(X)$.

Aplicant el teorema 9.4, $\mathbf{F}_{V'}(\bar{X}) = \mathbf{F}_V(\bar{X})$. Per qualsevol conjunt infinit de variables Y , pel corol·lari 8.6, $Id_{V'}(Y) = Id_{\mathbf{F}_{V'}(\bar{X})}(Y) = Id_{\mathbf{F}_V(\bar{X})}(Y) = Id_V(Y)$.

Usant de nou el teorema 9.4, es té que $\theta_{V'}(Y) = \theta_V(Y) \Rightarrow \mathbf{F}_{V'}(\bar{Y}) = \mathbf{F}_V(\bar{Y})$. Sigui $\mathbf{A} \in V'$, per un conjunt prou gran Z i pel corol·lari 9.8, $A \in H(\mathbf{F}_{V'}(\bar{Z}))$, aleshores $A \in H(\mathbf{F}_V(\bar{Z}))$ i obtenim que $A \in V$, per tant, $V' \subseteq V$. $\square$

Alternativament Birkhoff va arribar a aquest resultat el 1935 que va enunciar de la següent forma⁵:

Teorema 9.11. *La correspondència de cada família $\mathfrak{F}$ d'àlgebres de tipus Σ amb una família $\Phi(\mathfrak{F})$ d'equacions entre funcions de tipus Σ tal que compleix les lleis de $\mathfrak{F}$, i per cada família Φ d'equacions entre funcions de tipus Σ amb una família $\mathfrak{F}(\Phi)$ d'àlgebres de tipus Σ tals que les equacions de Φ són lleis, és recíproca. És a dir, $\mathfrak{F}(\Phi(\mathfrak{F})) = \mathfrak{F}$ i $\Phi(\mathfrak{F}(\Phi)) = \Phi$.*

Notació. En la notació utilitzada fins ara, les àlgebres de tipus Σ correspon al tipus τ . La primera part del teorema enuncia que donada una varietat V , $\mathfrak{F}$ al teorema, aleshores existeix $Id_V(X)$, $\Phi(\mathfrak{F})$ al teorema, per cert X un conjunt infinit, tal que $Id_V(X)$ són les identitats que es compleixen en V .

La segona part del teorema enuncia que per K classe d'àlgebres, donat $Id_K(X)$, Φ al teorema, existeix $\text{Mod}(Id_K(X))$, $\mathfrak{F}(\Phi)$ al teorema, tal que $\text{Mod}(Id_K(X))$ és la classe de models de $Id_K(X)$.

Per últim, el teorema recalca la reciprocitat, que equival a enunciar que K és equacional si, i només si, és variacional. Observem que $\mathfrak{F}(\Phi(\mathfrak{F})) = \mathfrak{F}$ equival a dir que $\text{Mod}(Id_V(X)) = V$ i $\Phi(\mathfrak{F}(\Phi)) = \Phi$ a que $Id_{\text{Mod}(Id_V(X))}(X) = Id_K(X)$.

Corol·lari 9.12. *Sigui K una classe d'àlgebres de tipus τ . Si $\mathbf{T}(X)$ existeix i K' és una classe d'àlgebres tal que $K \subseteq K' \subseteq V(K)$, aleshores, $\mathbf{F}_{K'}(\bar{X}) = \mathbf{F}_K(\bar{X})$. En particular, $\mathbf{F}_{K'}(\bar{X}) \in \text{ISP}(K)$.*

Demostració. Com $Id_K(X) = Id_{V(K)}(X)$ pel lema 9.3, podem deduir que $Id_K(X) = Id_{K'}(X)$. Pel teorema 9.5, aleshores, $\theta_{K'}(X) = \theta_K(X)$, $\mathbf{F}_{K'}(\bar{X}) = \mathbf{F}_K(\bar{X})$. Pel teorema 8.9 tenim que $\mathbf{F}_{K'}(\bar{X}) \in \text{ISP}(K)$. $\square$

Proposició 9.13. *Si V és varietat i X és infinit, $V = \text{HSP}(\mathbf{F}_V(\bar{X}))$.*

⁵Veure Teorema 10 de la pàgina 441 de [2]

Demostració. Usant part de la demostració del teorema de Birkhoff, podem afirmar que $V = Mod(Id_V(X))$, pel corol·lari 9.2 tenim que si X és infinit, $Id_V(X) = Id_{\mathbf{F}_V(\bar{X})}(X)$. Per tant, $V(\mathbf{F}_V(\bar{X})) = Mod(Id_{V(\mathbf{F}_V(\bar{X}))}(X))$ pel teorema de Birkhoff, a més, $Mod(Id_{V(\mathbf{F}_V(\bar{X}))}(X)) = Mod(Id_{\mathbf{F}_V(\bar{X})}(X)) = Mod(Id_V(X)) = V$, resultat d'aplicar de nou el teorema de Birkhoff a la última igualtat. $\square$

Comentari. Sigui V una varietat i X finit, sigui $Id_V(X)$, en general no és cert que $V = HSP(\mathbf{F}_V(\bar{X}))$.

Demostració. Ja hem vist en la proposició anterior que no hi havia cap problema quan era infinit. Veiem que passa quan X és finit. Trobem una varietat V :

$$F_V(\{\bar{X}\}) \models x = y \quad i \quad V \not\models x = y.$$

Si agafem com a varietat els grupoides contractius definits per $\langle G, * \rangle$ tals que $x = x * x$. Aquesta varietat està definida només per una variable. Obtenim que l'àlgebra lliure dels grupoides és la varietat trivial que difereix del grupoides.

Un altre cas més interessant és el l'àlgebra lliure dels reticles generats per dos elements, sigui aquesta àlgebra lliure $F_R(\{\bar{z}_1, \bar{z}_2\})$, aleshores els seus elements són: $\{\bar{z}_1, \bar{z}_2, \bar{z}_1 \vee \bar{z}_2, \bar{z}_1 \wedge \bar{z}_2\}$. Per la definició 12.4 de l'annex, s'observa que no poden haver-hi més elements que els indicats. D'altra banda, pel teorema 12.15 de l'annex, com ni $\mathbf{M}_5$ ni $\mathbf{N}_5$ són encaixables, $F_R(\{\bar{z}_1, \bar{z}_2\})$ només té quatre elements, aleshores $F_R(\{\bar{z}_1, \bar{z}_2\})$ és distributiu. En canvi, el reticle format per dos elements no és distributiu, i per tant:

$$F_R(\{\bar{z}_1, \bar{z}_2\}) \models x \wedge (y \vee z) = (x \vee y) \wedge (x \vee z) \quad i \quad R \not\models x \wedge (y \vee z) = (x \vee y) \wedge (x \vee z).$$

$\square$

Teorema 9.14. $V = HP_S$

Demostració. Com $P_s \leq SP \Rightarrow HP_S \leq HSP = V$. Donada una classe K d'àlgebres amb X suficientment gran, tenim que $\mathbf{F}_{V(K)}(\bar{X}) \in IP_s(K)$, usant el corol·lari 8.8 tenim que $V(K) \subseteq HP_S(K)$, d'on obtenim el resultat buscat. $\square$

10 Les condicions de Mal'cev

Un altre resultat interessant relacionat amb les varietats prové dels estudis de Mal'cev als anys 50 on va trobar la relació entre certes identitats de la varietat i la permutabilitat de les congruències per totes les àlgebres d'aquesta varietat. Aquests resultats se'ls coneix com les condicions de Mal'cev.

Lema 10.1. *Sigui V una varietat de tipus τ , i sigui $p(x_1, \dots, x_m, y_1, \dots, y_n), q(x_1, \dots, x_m, y_1, \dots, y_n)$ dos termes tals que en $\mathbf{F}_V(\bar{X})$, $X = \{x_1, \dots, x_m, y_1, \dots, y_n\}$, es té que $(p^{\mathbf{F}_V(\bar{X})}(\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n))^6$, $q^{\mathbf{F}_V(\bar{X})}(\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n) \in \Theta(\bar{y}_1, \dots, \bar{y}_n)$. Aleshores obtenim que:*

$$V \models p(x_1, \dots, x_m, y, \dots, y) \approx q(x_1, \dots, x_m, y, \dots, y)$$

Demostració. Donat l'homomorfisme $\alpha : \mathbf{F}_V(\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n) \rightarrow \mathbf{F}_V(\bar{x}_1, \dots, \bar{x}_m, \bar{y}, \dots, \bar{y})^7$, definit per $\alpha(\bar{x}_i) = \bar{x}_i, 1 \leq i \leq m$, i $\alpha(\bar{y}_i) = \bar{y}, 1 \leq i \leq n$. Aquests homomorfisme compleix que $\Theta(\bar{y}_1, \dots, \bar{y}_n) \subseteq \ker(\alpha)$, per tant:

$$\alpha(p(\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n)) = \alpha(q(\bar{x}_1, \dots, \bar{x}_m, \bar{y}_1, \dots, \bar{y}_n)).$$

Aplicant α obtenim: $p(\bar{x}_1, \dots, \bar{x}_m, \bar{y}, \dots, \bar{y}) = q(\bar{x}_1, \dots, \bar{x}_m, \bar{y}, \dots, \bar{y})$ en $\mathbf{F}_V(\bar{x}_1, \dots, \bar{x}_m, \bar{y}, \dots, \bar{y})$ pel teorema 8.2, $V \models p(x_1, \dots, x_m, y, \dots, y) \approx q(x_1, \dots, x_m, y, \dots, y)$. $\square$

Teorema 10.2. *Sigui V una varietat de tipus τ . La varietat V és congruent permutable si, i només si existeix un terme $p(x, y, z)$ tal que: $V \models p(x, x, y) = y$ i $V \models p(x, y, y) = x$.*

Demostració. $(\Rightarrow)$ Sigui V congruent permutable, aleshores es té que en $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ es té que $(\bar{x}, \bar{z}) \in \theta(\bar{x}, \bar{y}) \circ \theta(\bar{y}, \bar{z})$; per tant, $(\bar{x}, \bar{z}) \in \theta(\bar{y}, \bar{z}) \circ \theta(\bar{x}, \bar{y})$.

Com $p(\bar{x}, \bar{y}, \bar{z}) \in \mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$, tal que $\bar{x}\theta(\bar{y}, \bar{z})p(\bar{x}, \bar{y}, \bar{z})\theta(\bar{x}, \bar{y})$, pel lema anterior obtenim que $V \models p(x, y, y) = x$ i $V \models p(x, x, z) = z$.

$(\Leftarrow)$ Sigui $\mathbf{A} \in V$, suposem que $\theta_1, \theta_2 \in \text{Con}(\mathbf{A})$. Si $(a, b) \in \theta_1 \circ \theta_2$, aleshores existeix cert $c \in A$ tal que $a\theta_1 c\theta_2 b$, ho podem expressar com $b = p(c, c, b)\theta_1 p(a, c, b)\theta_2 p(a, b, b) = a$; i per tant. $(b, a) \in \theta_1 \circ \theta_2$. Obtenint doncs el resultat desitjat, $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$. $\square$

Exemple 12. Sigui K la classe de tots el grups. Sabem que és una varietat, i pel teorema anterior tenim que és congruent permutable. Usant el terme $p(x, y, z) = xy^{-1}z$, observem que per les propietats dels símbols funcionals, per qualsevol grup de la classe esmentada tenim:

$$p(x, x, y) = xx^{-1}y = 1y = y \text{ i } p(x, y, y) = xy^{-1}y = x1 = x.$$

Per tant, pel teorema 10.2 els grups són congruent permutables.

⁶Els elements $\bar{x} \in \bar{X}$ es descriuen en la definició 8.5.

⁷S'escriu $\mathbf{F}_V(\bar{x}_1, \dots, \bar{x}_n)$ per referir-se a l'àlgebra lliure generada pel conjunt $\bar{X} = \{\bar{x}_1, \dots, \bar{x}_n\}$.

Exemple 13. Sigui K la classe de tots els anells. Sabem que és una varietat, i pel teorema anterior tenim que és congruent permutable. Usant el terme $p(x, y, z) = x - y + z$, observem que per les propietats dels símbols funcionals, per qualsevol anell de la classe esmentada tenim:

$$p(x, x, y) = x - x + y = 0 + y = y \text{ i } p(x, y, y) = x - y + y = x + 0 = x.$$

Per tant, pel teorema 10.2 els anells són congruent permutables.

Teorema 10.3. *Sigui V una varietat de tipus τ . Si existeix un terme de majoria $M(x, y, z)$ tal que:*

$$V \models M(x, x, y) = M(x, y, x) = M(y, x, x) = x.$$

Aleshores V és congruent distributiva.

Demostració Sigui $\theta_1, \theta_2, \theta_3 \in \text{Con}(\mathbf{A})$, tal que $\mathbf{A} \in V$. Si $(a, b) \in \theta_1 \wedge (\theta_2 \vee \theta_3)$, aleshores $(a, b) \in \theta_1$ i existeixen $c_1, \dots, c_n$ tals que:

$$a\theta_2c_1\theta_3c_2\dots\theta_2c_n\theta_3b.$$

Però aleshores com per cada $i \in \{1, \dots, n\}$, $M(a, c_i, b)\theta_1M(a, c_i, a) = a$, tenim que:

$$a = M(a, a, b)(\theta_1 \wedge \theta_2)M(a, c_1, b)(\theta_1 \wedge \theta_3)M(a, c_2, b)\dots M(a, c_n, b)(\theta_1 \wedge \theta_3)M(a, b, b) = b.$$

Per tant, $(a, b) \in (\theta_1 \wedge \theta_2) \vee (\theta_1 \wedge \theta_3)$.

En deduem doncs que $\theta_1 \wedge (\theta_2 \vee \theta_3) = (\theta_1 \wedge \theta_2) \vee (\theta_1 \wedge \theta_3)$. Tenim que V és congruent distributiva. $\square$

Exemple 14. Usant el teorema anterior podem veure que la varietat formada per tots els reticles és congruent distributiva.

Sigui $M(x, y, z) := (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$; per a qualsevol reticle, usant les lleis d'idempotència i absorció obtenim que:

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

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

$$M(y, x, x) = (y \vee x) \wedge (y \vee x) \wedge (x \vee x) = (y \vee x) \wedge x = x. \quad \square$$

Teorema 10.4. *Una varietat V és congruent distributiva si, i només si, existeix n finit i certs termes $p_0(x, y, z), \dots, p_n(x, y, z)$ tals que V satisfà:*

$$(i) \ p_i(x, y, x) = x, 0 \leq i \leq n$$

$$(ii) \ p_0 = (x, y, z) = x$$

$$(iii) \ p_n(x, y, z) = z$$

(iv) $p_i(x, x, y) = p_{i+1}(x, x, y)$, per i parell

(v) $p_i(x, y, y) = p_{i+1}(x, y, y)$, per i senar.

Demostració. Sigui V congruent distributiva, en particular tenim que l'àlgebra lliure $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ és congruent distributiva. Sigui $\theta(\bar{x}, \bar{y}), \theta(\bar{x}, \bar{z}), \theta(\bar{y}, \bar{z}) \in \text{Con}(\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z}))$, tenim que:

$$(\theta(\bar{x}, \bar{y}) \wedge \theta(\bar{x}, \bar{z})) \vee (\theta(\bar{y}, \bar{z}) \wedge \theta(\bar{x}, \bar{z})) = (\theta(\bar{x}, \bar{y}) \vee \theta(\bar{y}, \bar{z})) \wedge \theta(\bar{x}, \bar{z}).$$

Com $(\bar{x}, \bar{y}), (\bar{y}, \bar{z}) \in \theta(\bar{x}, \bar{y}) \vee \theta(\bar{y}, \bar{z})$, i aquesta relació és una congruència, tenim que $(\bar{x}, \bar{z}) \in \theta(\bar{x}, \bar{y}) \vee \theta(\bar{y}, \bar{z})$. Degut a la igualtat anterior obtinguda pel fet de ser congruent distributiu, tenim que $(\bar{x}, \bar{z}) \in (\theta(\bar{x}, \bar{y}) \wedge \theta(\bar{x}, \bar{z})) \vee (\theta(\bar{y}, \bar{z}) \wedge \theta(\bar{x}, \bar{z}))$. Pel teorema 4.6 i l'operació suprem tenim que existeixen un nombre n finit d'elements $p_0, \dots, p_n \in \mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ tals que $p_0 = x, p_n = z, (p_0, p_1) \in \theta(\bar{y}, \bar{z}), (p_1, p_2) \in \theta(\bar{x}, \bar{y})$, on la parella (p_{n-1}, p_n) es troba en $\theta(\bar{y}, \bar{z})$ o $\theta(\bar{x}, \bar{y})$ depenent de que n sigui parell o senar.

Però tenim que aquests elements es troben en la varietat i per tant, podem definir els termes $p_i = p_i(x, y, z)$ per $1 \leq i \leq n$. Quan i és parell tenim que:

$$(p_i(x, y, z), p_{i+1}(x, y, z)) \in \theta(\bar{y}, \bar{z}) \Rightarrow (p_i(x, x, z), p_{i+1}(x, x, z)) \in \theta(\bar{y}, \bar{z}).$$

Fent la restricció de $\theta(\bar{y}, \bar{z})$ a la subàlgebra de $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ generada per $\bar{x}$ i $\bar{z}$ obtenim que $p_i(x, x, z) = p_{i+1}(x, x, z)$. Les altres identitats s'obtenen de forma anàloga.

($\Leftarrow$) Per a $\theta_1, \theta_2, \theta_3 \in \text{Con}(\mathbf{A})$, tal que $\mathbf{A} \in V$, volem veure que:

$$\theta_1 \wedge (\theta_2 \vee \theta_3) \subseteq (\theta_1 \wedge \theta_2) \vee (\theta_1 \wedge \theta_3),$$

sigui $(a, b) \in \theta_1 \wedge (\theta_2 \vee \theta_3)$. Com que $(a, b) \in \theta_1$, tenim que per certs $c_1, \dots, c_t$ obtenim:

$$a\theta_2c_1\theta_3\dots c_t\theta_3b.$$

D'on dedum per a $0 \leq i \leq n$:

$$p_i(a, a, b)\theta_2p_i(a, c_1, b)\theta_3\dots p_i(a, c_t, b)\theta_3(a, b, b), \text{ aleshores } p_i(a, a, b)(\theta_1 \wedge \theta_2)p_i(a, c_1, b)(\theta_1 \wedge \theta_3)\dots p_i(a, c_t, b)(\theta_1 \wedge \theta_3)(a, b, b), \text{ i per tant obtenim que } p_i(a, b, b)[(\theta_1 \wedge \theta_2) \vee (\theta_1 \wedge \theta_3)]p_i(a, b, b).$$

D'on podem concloure que V és congruent distributiva. $\square$

Definició 10.5. Donada una varietat V direm que és aritmètica si és congruent distributiva i congruent permutable.

Teorema 10.6. Una varietat V és aritmètica si, i només si, satisfà una de les següents condicions:

- (i) *Existeixen termes p i M com els definits en els teoremes 10.2 i 10.3.*
- (ii) *Existeix un terme $\frac{2}{3}$ minoria $m(x, y, z)$ tal que $V \models m(x, y, x) = m(x, y, y) = m(y, y, x) = x$.*

Demostració. Si V és aritmètica aleshores existeix cert terme p degut a que V és congruent permutable. Sigui l'àlgebra lliure $\mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$, aleshores:

$$(\bar{x}, \bar{z}) \in (\theta(\bar{x}, \bar{y}) \vee \theta(\bar{y}, \bar{z})) \wedge \theta(\bar{x}, \bar{z}) \Rightarrow (\bar{x}, \bar{z}) \in (\theta(\bar{x}, \bar{y}) \wedge \theta(\bar{x}, \bar{z})) \vee (\theta(\bar{y}, \bar{z}) \wedge \theta(\bar{x}, \bar{z})) \text{ per ser congruent permutable, } (\bar{x}, \bar{z}) \text{ pertany a } (\theta(\bar{x}, \bar{y}) \wedge \theta(\bar{x}, \bar{z})) \text{ o } (\theta(\bar{y}, \bar{z}) \wedge \theta(\bar{x}, \bar{z})) \text{ i per tant existeix.}$$

Sigui $M(\bar{x}, \bar{y}, \bar{z}) \in \mathbf{F}_V(\bar{x}, \bar{y}, \bar{z})$ tal que $\bar{x}[\theta(\bar{x}, \bar{y}) \wedge [\theta(\bar{x}, \bar{z})]M(\bar{x}, \bar{y}, \bar{z})[\theta(\bar{y}, \bar{z}) \wedge \theta(\bar{x}, \bar{z})]]$.

Pel teorema 10.3, $V \models M(x, y, x) = M(x, y, y) = M(y, y, x) = x$. Si es compleix (i), definim $m(x, y, z) := p(x, M(x, y, z), z)$. Si en canvi, es compleix (ii) definim $p(x, y, z)$ com $m(x, y, z)$ i $M(x, y, z)$ com $m(x, m(x, y, z), z)$, finalment usant els teoremes 10.2 i 10.3 obtenim que (i) implica que V és aritmètica.

Definició 10.7. *Una àlgebra de Boole és una àlgebra $\langle B, \vee, \wedge, ', 0, 1 \rangle$ amb dos operacions binàries, una unària i dos nul·làries que compleixen:*

- (i) *$\langle B, \vee, \wedge \rangle$ és un reticle distributiu.*
- (ii) *Per tot $a \in B$, $a \wedge 0 = 0$; $a \vee 1 = 1$*
- (iii) *Per tot $a \in B$, $a \wedge a' = 0$; $a \vee a' = 1$*

Exemple 15. Com que una àlgebra de Boole és un reticle distributiu és expansible per equacions i les condicions (i) i (ii) també són equacionals. Sigui $\mathbf{B}$ la classe de les àlgebres de Boole, és equacional, i per tant, varietat. És fàcil veure que si definim:

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

compleix la condició (ii) del teorema 10.6, i per tant, $\mathbf{B}$ és varietat aritmètica.

11 Lògica Equacional

Definició 11.1. *Sigui θ una congruència en $\mathbf{A}$ direm que és plenament invariant si per tot homomorfisme α de $\mathbf{A}$ en $\mathbf{A}$ compleix:*

$$(a, b) \in \theta \Rightarrow (\alpha(a), \alpha(b)) \in \theta.$$

Denotem $Con_{PI}(\mathbf{A})$ el conjunt de totes les congruències plenament invariants de $\mathbf{A}$.

Proposició 11.2. *La intersecció arbitrària de congruències plenament invariants és plenament invariant.*

Demostració. Sigui $\mathbf{A}$ una àlgebra de tipus τ , donada una família $\{\theta_i \in Con_{PI}(\mathbf{A}) : i \in I\}$ volem veure que $\bigcap_{i \in I} \theta_i \in Con_{PI}(\mathbf{A})$.

Com per tot $i \in I$, si $\theta_i \in Con_{PI}(\mathbf{A})$ es té que $\theta_i \in Con(\mathbf{A})$, aleshores per la demostració vista a la proposició 4.3, tenim que $\bigcap_{i \in I} \theta_i \in Con(\mathbf{A})$.

Falta veure que $\bigcap_{i \in I} \theta_i$ és congruència plenament invariant de $\mathbf{A}$. Sigui $a_1, \dots, a_n, b_1, \dots, b_n \in A$ tals que $(a_j, b_j) \in \bigcap_{i \in I} \theta_i$ per tot $1 \leq j \leq n$, aleshores $(a_j, b_j) \in \theta_i$ per tot $i \in I$, com $\theta_i \in Con_{PI}(\mathbf{A})$ tenim que per tot homomorfisme $\alpha : \mathbf{A} \rightarrow \mathbf{A}$, $(\alpha(a_j), \alpha(b_j)) \in \theta_i$, i això és vàlid per tot $\theta_i, i \in I$. Per tant, $\bigcap_{i \in I} \theta_i \in Con_{PI}(\mathbf{A})$. $\square$

Definició 11.3. *Sigui $\mathbf{A}$ una àlgebra i $S \subseteq A \times A$, sigui $\Theta_{PI}(S)$ la menor congruència plenament invariant en $\mathbf{A}$ que conté S , la definim com la congruència plenament invariant generada per S .*

Donat un conjunt de variable X i un tipus d'àlgebra τ , definim:

$$\tau' : Id(x) \rightarrow T(X) \times T(X).$$

On la bijecció està definida per $\tau'(p = q) = (p, q)$.

Lema 11.4. *Per a una classe d'àlgebres K de tipus τ i X un conjunt de variables, $\tau'(Id_K(X))$ és una congruència plenament invariant en $\mathbf{T}(X)$.*

Demostració. Veiem en primer lloc que $\tau'(Id_K(X))$ és una relació d'equivalència en $T(X)$. Com per $p \in T(X), p \approx p \in Id_K(X); p \approx q \in Id_K(X) \Rightarrow q \approx p \in Id_K(X); p \approx q, q \approx r \in Id_K(X) \Rightarrow p \approx r \in Id_K(X)$ es compleix el que buscàvem.

Si $p_i \approx q_i \in Id_K(X)$ per $1 \leq i \leq n$ i $f \in \tau$ n -ària, veiem fàcilment que $f(p_1, \dots, p_n) \approx f(q_1, \dots, q_n) \in Id_K(X)$, per tant $\tau(Id_K(X))$ és una relació de congruència en $\mathbf{T}(X)$. Sigui α un morfisme de $\mathbf{T}(X)$ en $\mathbf{T}(X)$ i $p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n) \in Id_K(X)$, és fàcil veure que $p(\alpha(x_1), \dots, \alpha(x_n)) \approx q(\alpha(x_1), \dots, \alpha(x_n)) \in Id_K(X)$: d'on arribem a la conclusió que $\tau'(Id_K(X))$ és plenament invariant. $\square$

Lema 11.5. *Donat un conjunt de variables X i una congruència plenament invariant $\theta \in \mathbf{T}(X)$, tenim que per a $p = q \in Id(X)$:*

$$\mathbf{T}(X)/\theta \models p = q \Leftrightarrow (p, q) \in \theta.$$

Per tant, $\mathbf{T}(X)/\theta$ és lliure en $V(\mathbf{T}(X)/\theta)$.

Demostració. $(\Rightarrow)$ Sigui $p = p(x_1, \dots, x_n), q = q(x_1, \dots, x_n) \in T(X)$ aleshores per $\mathbf{T}(X)/\theta \models p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n) \Rightarrow p(x_1/\theta, \dots, x_n/\theta) = q(x_1/\theta, \dots, x_n/\theta) \Rightarrow p(x_1, \dots, x_n)/\theta = q(x_1, \dots, x_n)/\theta \Rightarrow (p(x_1, \dots, x_n), q(x_1, \dots, x_n)) \in \theta$.

$(\Leftarrow)$ Donats $r_1, \dots, r_n \in T(X)$ podem trobar un morfisme α de $\mathbf{T}(X)$ en $\mathbf{T}(X)$ tal que $\alpha(x_i) = r_i, 1 \leq i \leq n$. Veiem que per $(p(x_1, \dots, x_n), q(x_1, \dots, x_n)) \in \theta \Rightarrow (\alpha(p(x_1, \dots, x_n)), \alpha(q(x_1, \dots, x_n))) \in \theta \Rightarrow (p(r_1, \dots, r_n), q(r_1, \dots, r_n)) \in \theta \Rightarrow p(r_1/\theta, \dots, r_n/\theta) = q(r_1/\theta, \dots, r_n/\theta)$.

Per tant, $\mathbf{T}(X)/\theta \models p \approx q$. Per últim, donats $p \approx q \in Id(X), (p, q) \in \theta \Leftrightarrow \mathbf{T}(X)/\theta \models p \approx q \Leftrightarrow V(\mathbf{T}(X)/\theta) \models p \approx q$ pel lema 9.3; per tant $\mathbf{T}(X)/\theta$ és lliure en $V(\mathbf{T}(X)/\theta)$ pel teorema 9.5. $\square$

Teorema 11.6. *Donat un subconjunt Σ de $Id(X)$, podem trobar una K tal que $\Sigma = Id_K(X)$ si, i només si, $\tau'(\Sigma)$ és una congruència plenament invariant en $\mathbf{T}(X)$.*

Demostració. La implicació cap a la dreta ja s'ha demostrat en el lema 11.4

Per veure la implicació cap a l'esquerra, suposant que $\tau'(\Sigma)$ és una congruència plenament invariant θ , per a $K = \{\mathbf{T}(X)/\theta\}$ i el lema 11.5 veiem que:

$$K \models p \approx q \Leftrightarrow (p, q) \in \theta \Leftrightarrow p \approx q \in \Sigma.$$

Per tant $\Sigma = Id_K(X)$. $\square$

Definició 11.7. *Un subconjunt $\Sigma \in Id(X)$ és una teoria equacional en X si hi ha una classe d'àlgebres K tal que:*

$$\Sigma = Id_K(X).$$

Corol·lari 11.8. *Les teories equacionals de tipus τ en X formen un reticle algebraic que és isomorf al reticle de les congruències plenament invariants en $\mathbf{T}(X)$.*

Demostració 1. *Sigui X un conjunt de variables i Σ el conjunt d'identitats de tipus τ en X . Per a $p, q \in T(X)$ diem que $\Sigma \models p = q$ si, donada qualsevol àlgebra $\mathbf{A}$, $\mathbf{A} \models \Sigma$ implica que $\mathbf{A} \models p = q$.*

Teorema 11.9. *Si Σ és un conjunt d'identitats sobre X i $p \approx q$ és una identitat sobre X , aleshores:*

$$\Sigma \models p \approx q \Leftrightarrow (p, q) \in \Theta_{PI}(\tau'(\Sigma)).$$

Demostració. Donada una àlgebra $\mathbf{A}$ tal que $\mathbf{A} \models \Sigma$. Com $\tau'(Id_{\mathbf{A}}(X))$ és una congruència plenament invariant de $\mathbf{T}(X)$ pel lema 10.4 obtenim $\Theta_{PI}(\tau'(\Sigma)) \subseteq \tau'(Id_{\mathbf{A}}(X))$. Per la suposició inicial tenim que per $(p, q) \in \Theta_{PI}(\tau'(\Sigma)) \Rightarrow \mathbf{A} \models p \approx q$; i per tant, $\Sigma \models p \approx q$.

Per l'aplicació contrària i pel lema 11.5 obtenim que $\mathbf{T}(X)/\Theta_{PI}(\tau'(\Sigma)) \models \Sigma$. Per tant si $\Sigma \models p \approx q$ aleshores $\mathbf{T}(X)/\Theta_{PI}(\tau'(\Sigma)) \models p \approx q$ i pel lema 10.5 obtenim el que volíem $(p, q) \in \Theta_{PI}(\tau'(\Sigma))$. $\square$

Definició 11.10. Donat un terme p , els subtermes de p es defineixen com:

- (i) p és subterme de p .
- (ii) Si $f(p_1, \dots, p_n)$ és un subterme de p i $f \in \mathfrak{F}$ n -ària, aleshores cada p_i és un subterme de p .

Definició 11.11. Un conjunt d'identitats Σ sobre X és tancat per reemplaçament si donada una identitat $p \approx q \in \Sigma$, i per a tot $t \in T(X)$ si p és un subterme de t aleshores $t(p) \approx t(q) \in \Sigma$.

Un conjunt d'identitats Σ en X és tancat per substitució si per cada $p \approx q \in \Sigma$ i cada $r \in T(X)$, aleshores $p(\frac{r}{x}) \approx q(\frac{r}{x}) \in \Sigma$, on $p(\frac{r}{x})$ és la substitució de cada ocurrència de x per r .

Definició 11.12. Donat un conjunt d'identitats Σ en X , la clausura deductiva $D(\Sigma)$ de Σ és el subconjunt més petit de $Id(X)$ que conté Σ tal que:

- $p = p \in D(\Sigma)$ per a tot $p \in T(X)$.
- $p = q \in D(\Sigma) \Rightarrow q = p \in D(\Sigma)$.
- $p = q, q = r \in D(\Sigma) \Rightarrow p = r \in D(\Sigma)$.
- $D(\Sigma)$ és tancat per reemplaçament.
- $D(\Sigma)$ és tancat per substitució.

Teorema 11.13. Donat $\Sigma \subseteq Id(X)$, $p = q \in Id(X)$ tenim que $\Sigma \models p \approx q \Leftrightarrow p \approx q \in D(\Sigma)$.

Demostració. Les tres primeres propietats de la clausura permeten que $\tau'(D(\Sigma))$ sigui una relació d'equivalència continguda en $\tau'(\Sigma)$, la quarta verifica que és congruència i la última propietats ens assegura que $\tau'(D(\Sigma))$ és una congruència plenament invariant. De manera que obtenim que $\tau'(D(\Sigma)) \supseteq \Theta_{PI}(\tau'(\Sigma))$.

Tanmateix, com $\tau'^{-1}(\Theta_{PI}(\theta\Sigma))$ compleix les cinc propietats per ser clausura deductiva i conté Σ , podem afirmar doncs que $\tau'(D(\Sigma)) = \Theta_{PI}(\tau'(\Sigma))$.

Per tant usant el teorema 11.9 observem que $\Sigma \models p \approx q \Leftrightarrow (p, q) \in \Theta_{PI}(\tau'(\Sigma)) \Leftrightarrow p \approx q \in D(\Sigma)$. $\square$

Definició 11.14. Donat un conjunt d'identitats Σ en X . Per a $p \approx q \in Id(X)$ diem que $\Sigma \vdash p \approx q$ (Σ prova $p \approx q$) si hi ha una seqüència d'identitats $p_1 \approx q_1, \dots, p_n \approx q_n$ de $Id(X)$ tal que cada $p_i \approx q_i \in \Sigma$, $1 \leq i \leq n$, o és de la forma $p \approx p$, o és el resultat d'aplicar qualsevol de les quatre regles de clausura, és a dir:

- (i) Per $p \approx q \in Id(X)$, $\frac{p \approx q}{q \approx p}$
- (ii) Per $p \approx q, q \approx r \in Id(X)$, $\frac{p \approx q, q \approx r}{p \approx r}$
- (iii) Per $p \approx q \in Id(X)$ i per tot $t \in T(X)$ on p és subterme de t , $\frac{p \approx q}{t(p) \approx t(q)}$
- (iv) Per $p \approx q \in Id(X)$ i per $r \in T(X)$, $\frac{p \approx q}{p(\frac{r}{x}) \approx q(\frac{r}{x})}$,

i la última identitat $p_n \approx q_n$ és $p \approx q$.

La seqüència $p_1 \approx q_1, \dots, p_n \approx q_n$ s'anomena deducció formal de $p \approx q$ i n és la llargada de la deducció.

Teorema 11.15. Donat $\Sigma \subseteq Id(X)$, $p \approx q \in Id(X)$, tenim que:

$$\Sigma \models p \approx q \Leftrightarrow \Sigma \vdash p \approx q.$$

Demostració. Usant les propietats que venen de que $D(\Sigma)$ sigui tancat en la construcció d'una deducció formal $p_1 \approx q_1, \dots, p_n \approx q_n$ de $p \approx q$, veiem que $\Sigma \vdash p \approx q \Rightarrow p \approx q \in D(\Sigma)$.

Per a l'altre sentit, $\Sigma \vdash p \approx q$ per $p \approx q \in \Sigma$ i $\Sigma \vdash p \approx p, p \in T(X)$.

Si $\Sigma \vdash p \approx q$ aleshores hi ha una deducció formal $p_1 \approx q_1, \dots, p_n \approx q_n$ de $p \approx q$. Però aleshores $p_1 \approx q_1, \dots, p_n \approx q_n, q_n \approx p_n$, és una deducció formal de $q \approx p$.

Si $\Sigma \vdash p \approx q$ i $\Sigma \vdash q \approx r$, sigui $p_1 \approx q_1, \dots, p_n \approx q_n$ una deducció formal de $p \approx q$ i sigui $p'_1 \approx q'_1, \dots, p'_n \approx q'_n$ una deducció formal de $q \approx r$. Aleshores $p_1 \approx q_1, \dots, p_n \approx q_n, p'_1 \approx q'_1, \dots, p'_n \approx q'_n, p_n \approx q'_n$ és una deducció formal de $p \approx r$.

Si $\Sigma \vdash p \approx q$ aleshores hi ha una deducció formal $p_1 \approx q_1, \dots, p_n \approx q_n$ de $p \approx q$. Sigui $r(\dots, p, \dots)$ un terme que conté el subterme p . Aleshores $p_1 \approx q_1, \dots, p_n \approx q_n, r(\dots, p_n, \dots) \approx r(\dots, q_n, \dots)$ és una deducció formal de $r(\dots, p, \dots) \approx r(\dots, q, \dots)$.

Finalment, si $\Sigma \vdash p_i \approx q_i, 1 \leq i \leq n$, i $f \in \mathfrak{F}$ n -ària, sigui la successió de cada $p_i \approx q_i$ i afegint $f(p_1, \dots, p_n) \approx f(q_1, \dots, q_n)$ al final la deducció formal de $\dots, p_1 \approx q_1, \dots, p_2 \approx q_2, \dots, p_n \approx q_n, f(p_1, \dots, p_n) \approx f(p_1, \dots, p_{n-1}, q_n), \dots$

Com $D(\Sigma) \subseteq \{p \approx q : \Sigma \vdash p \approx q\}$ tenim la igualtat $D(\Sigma) = \{p \approx q : \Sigma \vdash p \approx q\}$ i pel teorema 11.13, $\Sigma \models p \approx q \Leftrightarrow \Sigma \vdash p \approx q$. $\square$

12 Annex: Reticles

L'objectiu d'aquest apartat consisteix en introduir aquells conceptes i definicions que tot i no ser explícitament d'àlgebra universal, es troben directament relacionats amb la temàtica tractada al llarg del treball.

Podem definir el reticle des de dues perspectives diferents. Per un costat tenim la noció de reticle mitjançant la definició d'ordre; i per altra banda, des d'una visió més algebraica.

Definició 12.1. *Sigui A un conjunt i $\leq$ una relació binària en A . Diem que $\leq$ és un ordre parcial en A (o $(A, \leq)$ és un conjunt parcialment ordenat) si compleix:*

(i) *Per tot $a \in A$, $a \leq a$ (Reflexiva)*

(ii) *Per tot $a, b \in A$, $a \leq b$ i $b \leq a \Rightarrow a = b$ (Antisimètrica)*

(iii) *Per tot $a, b, c \in A$, $a \leq b$ i $b \leq c \Rightarrow a \leq c$ (Transitiva)*

Definició 12.2. *Sigui un conjunt parcialment ordenat P , tal que $A \subseteq P$, direm que un element $p \in P$ és una cota superior (cota inferior) de A si $a \leq p$ ($p \leq a$), per tot $a \in A$. Definim el suprem de A , $\sup A$ (infim de A , $\inf A$), com la més petita (gran) de les cotes superiors (inferiors) de A .*

A no ser que s'indiqui el contrari quan es parli d'un reticle $\mathbf{L}$ considerarem que el conjunt que el forma és L .

Definició 12.3. *Un conjunt parcialment ordenat $\mathbf{L}$ és un reticle, si i només si, per tot $a, b \in L$, existeixen $\sup\{a, b\} \in L$ i $\inf\{a, b\} \in L$.*

Alternativament podem definir un reticle de la següent forma:

Definició 12.4. *Sigui L un conjunt no buit, i $\vee, \wedge$ dos operacions binàries en $\mathbf{L}$, direm que és un reticle si satisfà:*

(i) *Per tot $x, y \in L$, $x \vee y = y \vee x$; $x \wedge y = y \wedge x$ (Commutativa)*

(ii) *Per tot $x, y, z \in L$, $x \vee (y \vee z) = (x \vee y) \vee z$; $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (Associativa)*

(iii) *Per tot $x \in L$, $x \vee x = x$; $x \wedge x = x$ (Idempotent)*

(iv) *Per tot $x, y \in L$, $x = x \vee (x \wedge y)$; $x = x \wedge (x \vee y)$ (Absorció)*

Proposició 12.5. *Les dues definicions de reticle són equivalents.*

Demostració. Si utilitzem la primera definició de reticle, per $a, b \in L$, n'hi ha prou en definir les operacions $\wedge$ i $\vee$ de la següent forma: $a \vee b = \sup\{a, b\}$ i

$a \wedge b = \inf\{a, b\}$. Les propietats es poden extreure fàcilment fent ús del canvi definit:

- (i) $a \vee b = \sup\{a, b\} = \sup\{b, a\} = b \vee a$.
- (ii) $a \vee (b \vee c) = \sup\{a, \sup\{b, c\}\} = \sup\{\sup\{a, b\}, c\} = (a \vee b) \vee c$.
- (iii) $a \vee a = \sup\{a, a\} = a$.
- (iv) $a = a \vee (b \wedge a) = \sup\{a, \inf\{a, b\}\}$, que és clarament cert degut a que $\inf\{a, b\} \leq a$.

Els casos per $a \wedge$ són anàlegs als presentats.

Si definim un reticle com en el segon cas. Definint $\leq$ en $\mathbf{L}$ de manera que $a \leq b \Leftrightarrow a = a \wedge b$, veiem que és un ordre parcial:

- (i) Per tot, $a \in L$, com $a \wedge a = a$, $a \leq a$.
- (ii) Per tot $a, b \in L$, si $a \leq b$ i $b \leq a$, aleshores $a = a \wedge b$ i $b = b \wedge a$; com que $a \wedge b = b \wedge a$, aleshores, $a = b$.
- (iii) Per tot $a, b, c \in L$, si $a \leq b$ i $b \leq c$, tenim que $a = a \wedge b$ i $b = b \wedge c$; de manera que, $a = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c$, és a dir, $a \leq c$.

Tenim que $\leq$ defineix un ordre parcial.

Falta veure que el suprem i l'ínfim es troben en L . Observem que com $a = a \wedge (a \vee b)$, $b = b \wedge (a \vee b)$, aleshores, $a \leq a \vee b$ i $b \leq a \vee b$; per tant $a \vee b$ és una cota superior de a, b , veiem que és la més petita. Sigui $a \leq u, b \leq u$, aleshores, $a \vee u = (a \wedge u) \vee u = u$, anàlogament $b \vee u = u$, per tant, $(a \vee u) \vee (b \vee u) = (a \vee b) \vee u = u$, de manera que $(a \vee b) \wedge u = (a \vee b) \wedge [(a \vee b) \vee u] = a \vee b$ per absorció $\Rightarrow a \vee b \leq u$. Tenim doncs que $a \vee b = \sup\{a, b\}$. Anàleg pel cas de l'ínfim. $\square$

Observació. Com els reticles són una classe d'àlgebres, tots els resultats obtinguts per homomorfismes entre àlgebres són igualment vàlids per reticles.

Definició 12.6. Un subreticle d'un reticle $\mathbf{L}$ és una subàlgebra de $\mathbf{L}$.

Definició 12.7. Diem que un reticle $\mathbf{L}_1$ es pot encaixar en un reticle $\mathbf{L}_2$, si existeix $\mathbf{L}'_2$ un subreticle de $\mathbf{L}_2$ tal que $\mathbf{L}'_2 \cong \mathbf{L}_1$.

Definició 12.8. Direm que un reticle $\mathbf{L}$ és distributiu si per tot $x, y, z \in L$:

- (i) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
- (ii) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Teorema 12.9. Un reticle L , per tot $x, y, z \in L$ satisfà $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ si, i només si, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Demostració. Sigui $x, y, z \in L$, suposem que es compleix que $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ fent ús de les lleis de la definició 12.4:

$$\begin{aligned}
(x \vee y) \wedge (x \vee z) &= [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z] \\
&= x \vee [z \wedge (x \vee y)] \\
&= x \vee [(z \wedge x) \vee (z \wedge y)] \\
&= [x \vee (z \wedge x)] \vee (z \wedge y) \\
&= x \vee (z \wedge y)
\end{aligned}$$

Hem obtingut doncs una de les implicacions, s'observa que l'altre implicació es pot obtenir amb una argumentació equivalent. $\square$

Definició 12.10. Direm que un reticle $\mathbf{L}$ és modular si satisfà la llei modular.

Per tot $x, y \in \mathbf{L}$, si $x \leq y$, aleshores $x \vee (y \wedge z) = y \wedge (x \vee z)$.

Teorema 12.11. Si un reticle és distributiu, aleshores és modular.

Demostració. Sigui $\mathbf{L}$ un reticle distributiu, per tot $a, b, c \in L$ tals que $a \leq b$, per la distributivitat de $\mathbf{L}$ tenim que $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, a més com $a \leq b$ tenim que $a \vee b = b$, per tant, veiem que $a \vee (b \wedge c) = b \wedge (a \vee c)$, obtenint que $\mathbf{L}$ és modular. $\square$

Definició 12.12. Anomenarem $\mathbf{M}_5$ i $\mathbf{N}_5$ als reticles de cinc elements que descriu la Figura 3.

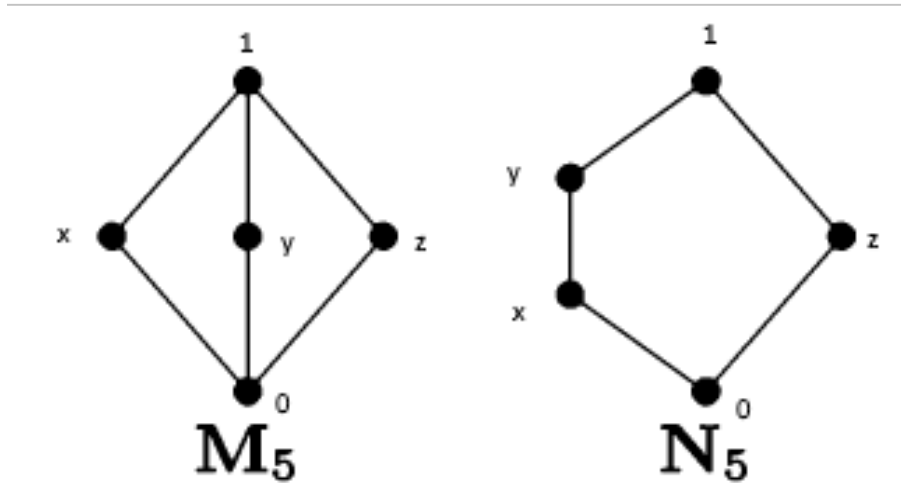


Figura 3: $\mathbf{M}_5$ i $\mathbf{N}_5$

Proposició 12.13. M_5 i N_5 no són distributius. A més, N_5 no és modular.

Demostració. Siguin x, y, z elements de N_5 i M_5 descrits en la figura 3, observem que $x \vee (y \wedge z) \neq (x \vee y) \wedge (y \vee z)$; per tant, no poden ser distributius. A més, per $x \leq y$ en N_5 , $x \vee (y \wedge z) \neq y \wedge (x \vee z)$; per tant, tampoc seria modular. $\square$

Teorema 12.14. Sigui L un reticle, les proposicions següents són equivalents:

- (i) L és modular.
- (ii) Per tot $x, y, z \in L$, L satisfà $((x \wedge z) \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$.
- (iii) N_5 no és encaixable a L .

Demostració. En primer lloc suposem que (i) és cert i demostrem (ii). Sigui $a, b, c \in L$ tals que $a = z, b = y, c = x \wedge z$. Com $c \leq a$, per modularitat $a \wedge (b \vee c) = (a \wedge b) \vee c$. Equivalentment: $((x \wedge z) \vee y) \wedge z = (y \wedge z) \vee (x \wedge z)$.

Etiquetant els elements de N_5 com $0 < x < z < 1, 0 < y < 1$, observem que no compleix (ii). Per tant (ii) implica (iii)

Suposem ara que L no és modular. Volem trobar un subreticle de L isomorf a N_5 . Tenim elements $x, y, z \in L$ amb $x \geq z$ i $x \wedge (y \vee z) > (x \wedge y) \vee z$, construint doncs un subreticle de L (Veure Figura 4).

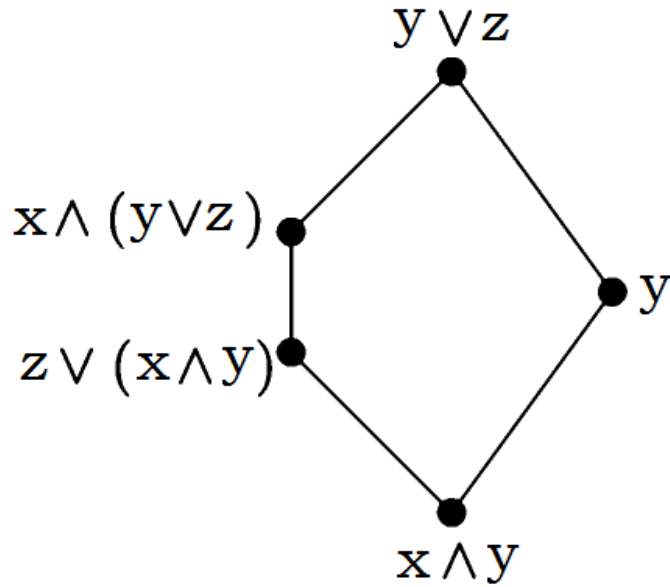


Figura 4: Subreticle isomorf a N_5

Falta veure que els cinc elements són diferents i formen un subreticle isomorf a N_5 . Certament $x \wedge y \leq y \leq y \vee z$ i $x \wedge y \leq z \vee (x \wedge y) < x \wedge (y \vee z) \leq y \vee z$. A més:

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

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

La resta de suprems i ínfims són trivials. Com $z \vee (x \wedge y) \neq x \wedge (y \vee z)$, ja ho tenim. $\square$

Teorema 12.15. *Segui $\mathbf{L}$ un reticle, les proposicions següents són equivalents:*

(i) $\mathbf{L}$ és distributiva.

(ii) Per tot $x, y, z \in L$, $\mathbf{L}$ satisfà $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$.

(iii) Ni $\mathbf{M}_5$, ni $\mathbf{N}_5$ són encaixables a $\mathbf{L}$.

Demostració. Observem que (i) implica (iii) degut que ni $\mathbf{M}_5$, ni $\mathbf{N}_5$ són distributius. Veiem que (iii) implica (ii). Si $\mathbf{L}$ no conté cap còpia de $\mathbf{N}_5$, pel teorema anterior $\mathbf{L}$ és modular. Suposem que $\mathbf{L}$ no compleix (ii), com la condició per $\leq$ es compleix sempre, sigui $x, y, z \in L$:

$$w = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) < (x \vee y) \wedge (x \vee z) \wedge (y \vee z) = u.$$

Aplicant modularitat i amb les següents definicions:

$$x' = (w \vee x) \wedge u = w \vee (x \wedge u)$$

$$y' = (w \vee y) \wedge u = w \vee (y \wedge u)$$

$$z' = (w \vee z) \wedge u = w \vee (z \wedge u)$$

obtenint un subreticle format per w, x', y', z', u de $\mathbf{L}$ isomorf a $\mathbf{M}_5$ (Veure Figura 5).

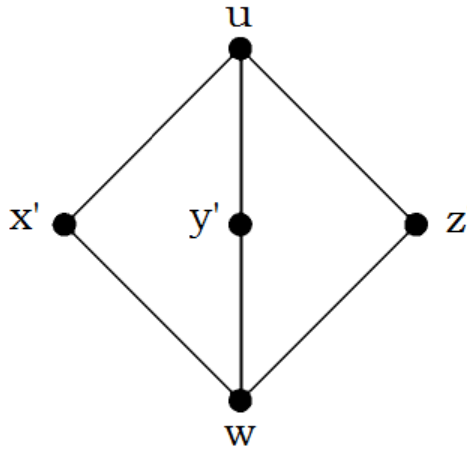


Figura 5: Reticle isomorf a $\mathbf{M}_5$

Veiem que realment és així; per la simetria vista en les definicions anteriors, n'hi

ha prou en veure que $x' \wedge y' = w$. Observem que $x \vee w = x \vee (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = x \vee (y \wedge z)$, per tant:

$$x' = (x \vee w) \wedge u = (x \vee (y \wedge z)) \wedge (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = (x \vee (y \wedge z)) \wedge (y \vee z) = (y \wedge z) \vee (x \wedge (y \vee z)).$$

Anàlogament obtenim $y' = (y \vee (x \wedge z)) \wedge (x \vee z)$. Obtenim doncs que:

$$x' \wedge y' = (y \wedge z) \vee (x \wedge (y \vee z)) \wedge (y \vee (x \wedge z)) \wedge (x \vee z) \stackrel{(1)}{=} (x \vee (y \wedge z)) \wedge (y \vee (x \wedge z)) \stackrel{(2)}{=} (x \wedge (y \vee (x \wedge z))) \vee (y \wedge z) \stackrel{(3)}{=} (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = w.$$

Podem veure que (1) s'obté de que $(x \vee (y \wedge z)) \leq (x \vee z)$ i $(y \vee (x \wedge z)) \leq (y \wedge z)$. La igualtat (2), l'obtenim de que $b \vee (x \wedge z) \geq y \wedge z$ i la modularitat. Finalment (3), l'obtenim de que $x \geq (x \wedge z)$ i la modularitat. La prova de que els cinc elements són diferents és trivial.

Tant sols queda veure que (ii) implica (i). Veiem primer que $\mathbf{L}$ és modular, sigui $x \geq z$, $x \wedge (y \vee z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = (x \wedge y) \vee z$. Veiem que és distributiu:

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

Com $x \geq (x \wedge y) \vee (x \wedge z)$ i usant la modularitat obtenim:

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

Definició 12.16. Direm que un reticle $\mathbf{L}$ és complet si és un conjunt parcialment ordenat i per a cada subconjunt A de L , $\sup A$ i $\inf A$ existeixen en L .

Notació. Siguí A un subconjunt de P ordre parcial, si existeixen el suprem i l'ínfim de A , els denotarem per $\bigvee A$ i $\bigwedge A$ respectivament.

Definició 12.17. Siguí $\mathbf{L}$ un reticle. Diem que $a \in L$ és compacte si, i només si, per to $A \subseteq L$, tal que $a \leq \bigvee A$, existeix $B \subseteq A$ finit, tal que $a \leq \bigvee B$.

Direm que $\mathbf{L}$ està generat per compactes si, i només si cada element de L és un suprem d'elements compactes.

Siguí $\mathbf{L}$ un reticle compactament generat i complet, aleshores direm que és algebraic.

Definició 12.18. Donat un conjunt A , l'aplicació $C : P(A) \rightarrow P(A)$ l'anomenem operador de clausura en A , si satisfà per tot $X, Y \subseteq A$:

- (i) $X \subseteq C(X)$
- (ii) $C^2(X) = C(X)$
- (iii) $X \subseteq Y \Rightarrow C(X) \subseteq C(Y)$

A més, direm que un subconjunt X és tancat si $C(X) = X$. L'ordre parcial del conjunts tancat de A amb el conjunt inclusió es denota per $\mathbf{L}_C$.

Teorema 12.19. *Tots els reticles complets són isomorfs al reticle dels subconjunts tancats per cert conjunt A i un operador clausura C .*

Demostració. Sigui $\mathbf{L}$ un reticle complet. Per $X \subseteq L$ definim $C(X) = \{a \in L : a \leq \bigvee X\}$. Aleshores C és operador de clausura a L i l'aplicació $a \mapsto \{b \in L : b \leq a\}$ dóna l'isomorfisme que volíem entre $\mathbf{L}$ i $\mathbf{L}_C$. $\square$

Definició 12.20. *Un operador de clausura C en un conjunt A és un operador de clausura algebraica si per cada $X \subseteq A$:*

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

Definició 12.21. *Si C és un operador de clausura en A i Y és un subconjunt de A tancat. Direm que un conjunt X és un conjunt generador de Y si $C(X) = Y$. Direm que Y es troba finitament generat si el conjunt X és finit. El conjunt de X és el generador minimal de Y si X genera Y i no hi ha cap altre subconjunt de X que ho fagi.*

Proposició 12.22. *Sigui C un operador de clausura algebraic en A . Aleshores els subconjunts finitament generats de A són precisament els elements compactes de $\mathbf{L}_C$.*

Teorema 12.23. *Tot reticle algebraic és isomorf al reticle de subconjunts tancats de cert conjunt A amb l'operador de clausura algebraic C .*

Demostració. Sigui $\mathbf{L}$ un reticle algebraic, i sigui A el subconjunt d'elements compactes. Per a $X \subseteq A$ podem definir:

$$C(X) = \{a \in A : a \leq \bigvee X\}.$$

C és un operador de clausura i de la definició d'element compacte podem concloure que C és algebraic. Per l'aplicació $a \mapsto \{b \in A : b \leq a\}$, obtenim l'isomorfisme que volíem ja que $\mathbf{L}$ és compactament generat. $\square$

Definició 12.24. *Donada una àlgebra $\mathbf{A}$, $S(\mathbf{A})$ denota el conjunt de subuniversos de $\mathbf{A}$.*

Teorema 12.25. *Si $\mathbf{L}$ és un reticle algebraic, aleshores $\mathbf{L} \cong S(\mathbf{A})$, per a certa àlgebra $\mathbf{A}$.*

Demostració. Pel teorema 12.23 tenim un conjunt A i un operador de clausura algebraic C en A tal que $\mathbf{L} \cong \mathbf{L}_C$. L'objectiu és veure que $\mathbf{L}_C = S(\mathbf{A})$.

Per tot B subconjunt finit de A (tal que $n = |B|$), cada $a \in C(B)$ defineix un operador funcional n -àri f en A tal que:

$$f_{B,a}(x_1, \dots, x_n) = \begin{cases} a, & \text{si } \{x_1, \dots, x_n\} = B \\ x_1, & \text{la resta de casos} \end{cases}$$

Els símbols funcionals definits juntament amb el conjunt A , defineixen l'àlgebra **A**. Tenim doncs que $f_{B,a}(x_1, \dots, x_n) \in C(x_1, \dots, x_n)$, per tant obtenim que per $X \subseteq A$, $Sg(X) \subseteq C(X)$.

Per altra banda, $C(X) = \bigcup \{C(B) : B \subseteq X, B \text{ finit}\}$. Obtenim doncs que: $C(B) = \{f_{B,a}(x_1, \dots, x_n) : B = \{x_1, \dots, x_n\}, a \in C(B)\} \subseteq Sg(B) \subseteq Sg(X)$.

Això implica que $C(X) \subseteq Sg(X)$, i per tant, $C(X) = Sg(X)$. D'aquesta manera veiem que com $\mathbf{L}_C = S(\mathbf{A})$, $S(\mathbf{A}) \cong \mathbf{L}$. $\square$

Corol·lari 12.26. *Si sigui una àlgebra $\mathbf{A}$, aleshores $\langle S(\mathbf{A}), \cap, \vee \rangle$ defineix una àlgebra $S(\mathbf{A})$.*

Demostració. Pel teorema anterior tenim que $S(\mathbf{A}) \cong \mathbf{L}$, on $\mathbf{L}$ és un reticle algebraic, en aquest cas $\cap$ i $\vee$ compleixen amb les condicions per ser reticle. $\square$

Teorema 12.27. *Donada $\mathbf{A}$ una àlgebra qualsevol, aleshores tenim que $\langle Con(\mathbf{A}), \cap, \vee \rangle$ és un reticle algebraic.*

Demostració. En primer lloc veiem que $Con(\mathbf{A})$ és un reticle. Per tot $\theta_1, \theta_2 \in Con(\mathbf{A})$, $\theta_1 \vee \theta_2 = \bigcap \{\theta' \in Con(\mathbf{A}) : \theta_1 \cup \theta_2 \subseteq \theta'\} = \bigcap \{\theta' \in Con(\mathbf{A}) : \theta_2 \cup \theta_1 \subseteq \theta'\} = \theta_2 \vee \theta_1$; evidentment $\theta_1 \cap \theta_2 = \theta_2 \cap \theta_1$.

Per tot $\theta_1, \theta_2, \theta_3 \in Con(\mathbf{A})$, per les definicions donades de $\vee$ i $\cap$ es compleix que $\theta_1 \vee (\theta_2 \vee \theta_3) = (\theta_1 \vee \theta_2) \vee \theta_3$ i $\theta_1 \cap (\theta_2 \cap \theta_3) = (\theta_1 \cap \theta_2) \cap \theta_3$.

Per tot $\theta \in Con(\mathbf{A})$, $\theta_1 \vee \theta_1 = \bigcap \{\theta' \in Con(\mathbf{A}) : \theta \cup \theta \subseteq \theta'\} = \theta$ i $\theta \cap \theta = \theta$.

Per últim, per tot $\theta_1, \theta_2 \in Con(\mathbf{A})$, $\theta_1 \vee (\theta_1 \cap \theta_2) = \theta_1$, ja que $\theta_1 \cap \theta_2 \subseteq \theta_1$; $\theta_1 \cap (\theta_1 \vee \theta_2) = \theta_1$, ja que $\theta_1 \subseteq \theta_1 \vee \theta_2$. Per tant, $Con(\mathbf{A})$ és un reticle.

Falta veure que el reticle és algebraic, per veure-ho construirem un operador de clausura tal que els subconjunts tancat de $A \times A$ són les congruències en $\mathbf{A}$. Sigui $f \in \mathfrak{F}$ un símbol funcional n -àri de $\mathbf{A}$, definim f per $A \times A$ com:

$$f((a_1, b_1), \dots, (a_n, b_n)) = (f^{\mathbf{A}}(a_1, \dots, a_n), f^{\mathbf{A}}(b_1, \dots, b_n)).$$

Afegim l'operació nul·lària per (a, a) per cada $a \in A$; una operació unària $s((a, b)) = (b, a)$ i una binària $t((a, b), (c, d)) = \begin{cases} (a, d), & \text{si } b = c \\ (a, b), & \text{la resta de casos.} \end{cases}$

És fàcil veure que B serà un subunivers d'aquesta nova àlgebra si, i només si

és congruència en $\mathbf{A}$. Com Θ l'operador de clausura Sg sobre $A \times A$ per l'àlgebra descrita és algebraic; $\mathbf{L}_{Sg} = \mathbf{Con}(\mathbf{A})$ ha de ser un reticle algebraic. $\square$

Teorema 12.28. *Sigui R un reticle, $c, d \in R$, $\theta \in Con(R)$. Sigui:*

$[c, d] = \{x \in R, c \leq x \leq d\}$. Per tot $a, b \in R$, són equivalents:

- (i) $(a, b) \in \theta$*
- (ii) $(a \wedge b, a \vee b) \in \theta$*
- (iii) Per tot $x, y \in [a \wedge b, a \vee b]$, $(x, y) \in \theta$.*

Demostració. $(i) \Rightarrow (ii)$. Tenim que $(a \wedge b)\theta b$, ja que $a \wedge b \leq b$, i $b\theta(a \vee b)$, ja que $b \leq (a \vee b)$, per tant:

$(a \wedge b)\theta b\theta b\theta(a \vee b)$, per transitivitat de θ , $(a \wedge b)\theta(a \vee b)$.

$(ii) \Rightarrow (iii)$. En general tenim que $x\theta(a \wedge b)$ i $y\theta(a \vee b)$, per tot $x, y \in [a \wedge b, a \vee b]$, per tant:

$x\theta(a \wedge b)\theta(a \vee b)\theta y$, de nou, per transitivitat, $x\theta y$.

$(iii) \Rightarrow (i)$. N'hi ha prou en veure que $a, b \in [a \wedge b, a \vee b]$ i aplicar (iii). És evident que es compleix, ja que $a \wedge b \leq b \leq a \vee b$ i $a \wedge b \leq a \leq a \vee b$. $\square$

Exemple 16. Veiem un exemple d'un reticle linial $\mathbf{A}$ i la construcció del seu reticle de congruències $Con(\mathbf{A})$.

Sigui $A = \{0, b, a, 1\}$ un reticle linial tal que $b \leq a$ com es pot observar en la Figura 6.



Figura 6: Reticle linial $\mathbf{A}$

Anem a construir $Con(\mathbf{A})$, per això hem de veure com són les congruències generades per tots els elements de $\mathbf{A}$. Evidentment, $\Delta \in Con(\mathbf{A})$, veiem la resta:

$$\theta(a, b) = \Delta \cup \{(a, b), (b, a)\}$$

$$\theta(a, 0) = \Delta \cup \{(a, 0), (0, a), (a, b), (b, a), (b, 0), (0, b)\}$$

$$\theta(b, 0) = \Delta \cup \{(0, b), (b, 0)\}$$

$$\theta(1, a) = \Delta \cup \{(a, 1), (1, a)\}$$

$$\theta(1, b) = \Delta \cup \{(a, b), (b, a), (1, a), (a, 1), (1, b), (b, 1)\}$$

$$\theta(0, 1) = \Delta \cup \{(a, b), (b, a), (1, a), (a, 1), (1, b), (b, 1), (a, 0), (0, a), (b, 0), (0, b)\} = \nabla$$

A més, s'han de considerar les congruències generades per la combinació de les anteriors, la única congruència que es diferencia de les obtingudes és:

$$\Psi := \theta((0, b), (1, a)) = \Delta \cup \{(1, a), (a, 1), (0, b), (b, 0)\}$$

Per tant tenim el reticle $Con(\mathbf{A}) = \{\Delta, \theta(a, b), \theta(a, 0), \theta(a, 1), \theta(0, b), \theta(1, b), \Psi, \nabla\}$ tal i com s'observa en la Figura 7.

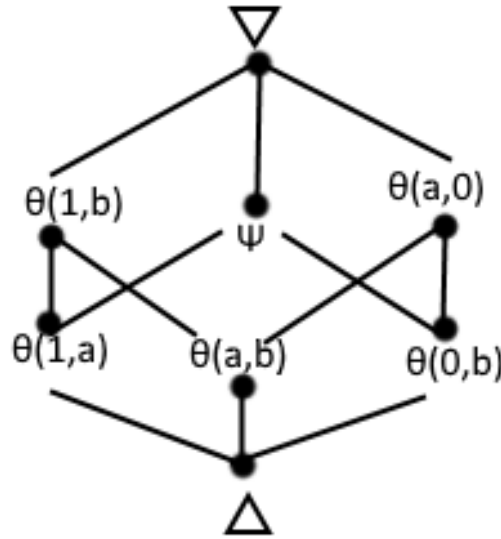


Figura 7: Reticle $Con(\mathbf{A})$

D'altra banda pels teoremes 12.14 i 12.15 podem veure que el reticle serà modular i distributiu, ja que ni N_5 ni M_5 són encaixables a $Con(\mathbf{A})$.

13 Conclusions

Més enllà del Teorema de Birkhoff, la possibilitat d'estudiar alguns dels resultats que s'havien vist en altres assignatures d'àlgebra ha significat una experiència realment gratificant. Entre aquests destacaria l'oportunitat de veure i demostrar els teoremes de isomorfia per a qualsevol àlgebra, previàment s'havien vist per a grups i per anells.

La possibilitat d'estudiar un teorema des de zero enunciant i demostrant tots aquells resultats previs necessaris per arribar-hi ha significat un repte en moltes ocasions degut a la novetat dels conceptes tractats. Destacaria la dificultat de l'apartat on es presenta l'àlgebra lliure, que és un dels pilars per desenvolupar la demostració del Teorema de Birkhoff juntament amb les identitats, sobretot per la complexitat que ha significat comprendre l'estructura mencionada. A més de [4], ha estat de significant ajuda l'apartat sobre l'àlgebra lliure de [5].

Davant les diferents demostracions que s'han consultat del Teorema de Birkhoff s'ha optat per treballar la presentada en [4] degut a la seva elegància i senzillesa, tot hi que també s'han consultat les presentades en [6] i en [1]. Una de les principals motivacions que van portar-me a escollir el tema presentat, s'ha vist assolida, comprendre i estudiar un teorema que ens permet relacionar les demostracions vistes des de perspectives algebraiques i lògiques.

Més enllà del que he après sobre àlgebra universal, l'estudi desenvolupat al llarg de la memòria, ha significat la porta d'entrada a una part de les matemàtiques que no havia vist durant el grau, la teoria de models. En particular aquest tema es presenta com una oportunitat per profunditzar en aquesta part de les matemàtiques i seguir estudiant en aquest sentit per comprendre més i millor el paper de la teoria de models en la lògica matemàtica.

Referències

- [1] Bergman, C.: *Univesal Algebra. Fundamental and Selected Topics*, Chapman & Hall/CRC Press, Florida, 2012.
- [2] Birkhoff, G.: On the structures of Abstract Algebras, *Proc. Camb. Philos. Soc.*, 31(4):433-454, 1935.
- [3] Birkhoff, G.: Lattice Theory, *Colloquium Publications, Amer. Math. Soc.*, 25:1-158, Providence, 1940.
- [4] Burris, S.; Sankapappanavar, H. P.: *A Course in Universal Algebra*, Springer-Verlag, New York, 1981.
- [5] Denecke, K.; Wismath, S. L.: *Universal Algebra and apllications in theoretical computer science*, Chapman & Hall/CRC Press, Florida, 2002.
- [6] Grätzer, G.: *Universal Algebra*, D. Van Nostrand Company, 2012, Princeton.
- [7] Hobby, D.; McKenzie R.; The Structure of Finite Algebra, *Contemporany Mathematics, Amer. Math. Soc.*, 76, Providence, 1988.
- [8] McKenzie, R.; McNulty, G. F.; Taylor, W. F.: *Algebras, Lattices, Varieties. Vol. I*, Wadsworth & Brooks, Belmont, 1987.