Álgebra Universal e Categorias

Lic. Ciências da Computação
Lic. Matemática

Universidade do Minho 2018/2019

Introdução

O programa da unidade curricular Álgebra Universal e Categorias prevê o estudo de conceitos e resultados básicos de álgebra universal e da teoria de categorias, pelo que a escolha dos tópicos abordados ao longo deste texto teve em consideração os conteúdos programáticos referidos.

No Capítulo 1 são apresentados noções e resultados básicos de teoria de conjuntos, os quais são essenciais para a compreensão dos conteúdos abordados nos restantes capítulos.

No Capítulo 2 é feita uma breve introdução à teoria de reticulados. No estudo de álgebra universal são relevantes conceitos e resultados desta teoria. Além de fornecerem exemplos importantes de álgebras, os reticulados são fundamentais no estudo de propriedades comuns a diversas estruturas algébricas e, em certos casos, no estudo de propriedades que distinguem umas classes de álgebras de outras.

O Capítulo 3 é dedicado à apresentação de conceitos fundamentais e de resultados relevantes de álgebra universal. Com a evolução do estudo na área da matemática foram surgindo diversas estruturas algébricas, tais como grupos, anéis, corpos, anéis de Boole, reticulados, etc. Estas estruturas, embora diferentes, partilham várias propriedades em comum. Encontrar e estudar propriedades comuns às diversas estruturas algébricas é o principal objetivo da álgebra universal.

Por último, no Capítulo 4 apresentam-se conceitos e alguns resultados básicos da teoria de categorias. Numa primeira aproximação, podemos considerar a teoria de categorias como o estudo abstrato de álgebras de funções. Duas álgebras isomorfas têm essencialmente as mesmas propriedades, um par de espaços métricos isométricos são praticamente equivalentes, e dois espaços homeomorfos são indistinguíveis (exceptо nos nomes dos seus pontos). Assim, muitas das propriedades de diversas estruturas matemáticas podem ser formuladas recorrendo às transformações admissíveis entre estas estuturas e à composição destas transformações. A teoria de categorias surgiu com o objetivo de estudar e caracterizar as mais diversas estruturas em função das transformações admissíveis entre elas.

1. Preliminares

Neste capítulo recordam-se conceitos básicos de: teoria de conjuntos, relações, funções, operações, relações de ordem e relações de equivalência. Os conceitos e resultados aqui apresentados podem ser encontrados em qualquer livro básico de teoria de conjuntos e de matemática discreta.

1.1 Conjuntos e Relações

Para a compreensão dos conteúdos abordados nestes apontamentos é suficiente considerar uma teoria intuitiva de conjuntos e de classes.

Um **conjunto** é definido como uma coleção de objetos, designados por **elementos** ou **membros** do conjunto. Escreve-se $a \in A$, se a é um elemento de um conjunto A; caso contrário, escreve-se $a \notin A$.

Se A e B são conjuntos tais que todo o elemento de A é também um elemento de B, diz-se que A **está contido em** B ou que A é um **subconjunto** de B, e escreve-se $A \subseteq B$. Se A e B são conjuntos tais que $A \subseteq B$ e existe $b \in B$ tal que $b \notin A$, diz-se que A é um **subconjunto próprio** de B e escreve-se $A \subset B$. Um conjunto A não está contido num conjunto B, $A \nsubseteq B$, caso exista um elemento a tal que $a \in A$ e $a \notin B$.

Dados conjuntos A e B, diz-se que os conjuntos são **iguais**, $A = B$, se $A \subseteq B$ e $B \subseteq A$; caso contrário, os conjuntos dizem-se **diferentes**, $A \neq B$.

O **conjunto vazio**, isto é, o conjunto sem elementos, é representado por $\emptyset$ ou por $\{\}$. Para qualquer conjunto A, tem-se $\emptyset \subseteq A$.

As operações de conjuntos $\cup$, $\cap$ e $\setminus$ têm o significado usual.

Se A é um conjunto, o conjunto das partes de A é representado por $\mathcal{P}(A)$; $\mathcal{P}(A) = \{X \mid X \subseteq A\}$. Um subconjunto Π de A diz-se uma **partição de** A se $\emptyset \notin \Pi$ e, para qualquer $a \in A$, existe um, e um só, $X \in \Pi$ tal que $a \in X$. Note-se que, para qualquer conjunto A, $\emptyset \in \mathcal{P}(A)$ e $A \in \mathcal{P}(A)$.

Dados conjuntos A e B, o **produto cartesiano** de A e B, representado por $A \times B$, é o conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$,

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

O conceito de produto cartesiano pode ser generalizado para uma coleção finita de conjuntos. Se $A_1, A_2, \ldots, A_n$ são conjuntos, com $n \in \mathbb{N}$, define-se

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \,|\, a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Se $A_1 = A_2 = \ldots = A_n = A$, representa-se $A_1 \times A_2 \times \ldots \times A_n$ por A^n. Se $n = 0$, define-se $A^n = \{\emptyset\}$.

Dados um número natural n e conjuntos $A_1, A_2, \ldots, A_n$, dá-se a designação de **relação n-ária nos conjuntos** $A_1, A_2, \ldots, A_n$ a um subconjunto de $A_1 \times A_2 \times \ldots \times A_n$; no caso em que $A_1 = A_2 = \ldots = A_n = A$, a relação n-ária nos conjuntos $A_1, A_2, \ldots, A_n$ diz-se uma **relação n-ária em** A. Se ρ é uma relação n-ária nos conjuntos $A_1, A_2, \ldots, A_n$ e $a_1, a_2, \ldots, a_n$ são elementos tais que $(a_1, a_2 \ldots, a_n) \in \rho$, diz-se que que os elementos $a_1, a_2, \ldots, a_n$ estão **relacionados por** ρ e escreve-se $\rho(a_1, a_2, \ldots, a_n)$.

Uma relação 2-ária nos conjuntos A e B diz-se uma **relação binária de A em B**. Se ρ é uma relação binária de A em B e a e b são elementos tais que $(a, b) \in \rho$, também se escreve $a \,\rho\, b$ em alternativa a $\rho(a, b)$. Se $(a, b) \notin \rho$, escrevemos $a \not\rho b$ e dizemos que a **e** b **não estão relacionados por** ρ.

Uma vez que as relações binárias são conjuntos, faz sentido considerar as operações de união, interseção e complementação na construção de novas relações binárias. Além destas operações, existem outros processos que permitem a construção de novas relações binárias.

Se A, B, C e D são conjuntos, ρ é uma relação binária de A em B e ϱ é uma relação binária de C em D, chama-se:

- **relação inversa de** ρ, e representa-se por ρ^{-1}, a relação de B em A definida por
$$\rho^{-1} = \{(b, a) \in B \times A \,|\, (a, b) \in \rho\}.$$
- **relação composta de** ϱ **com** ρ, e representa-se por $\varrho \circ \rho$, a relação binária de A em D definida por
$$\varrho \circ \rho = \{(x, y) \in A \times D \,|\, \exists_{z \in B \cap C} \;\; ((x, z) \in \rho \wedge (z, y) \in \varrho)\}.$$

1.2 Funções e operações

Uma relação binária f de um conjunto A num conjunto B diz-se uma **função de A em B** se, para cada $a \in A$, existe um e um só $b \in B$ tal que $(a, b) \in f$. Escrevemos $f : A \to B$ para indicar que f é uma função de A em B. Para cada $a \in A$, o único elemento b de B tal que $(a, b) \in f$ representa-se por $f(a)$, a este elemento dá-se a designação de **imagem de a por f**. Pode, então, escrever-se

$$\begin{array}{rccc} f: & A & \to & B \\ & a & \mapsto & f(a) \end{array}$$

Em $f : A \to B$, chamamos: **domínio** ou **conjunto de partida** de f ao conjunto A; **codomínio** ou **conjunto de chegada** de f ao conjunto B; **imagem** ou **contradomínio** de f ao conjunto $\mathrm{Im}f = \{f(x) : x \in A\}$.

Se f é uma função de A em B e $C \subseteq A$, então $f \cap (C \times B)$ é uma função de C em B, designada por **restrição de f a C** e representada por $f_{|C}$.

O conjunto de todas as funções de A em B representa-se por B^A. Dado um conjunto A, chama-se **aplicação vazia** à aplicação $\emptyset : \emptyset \to A$; esta é a única aplicação de $\emptyset$ em A e, portanto, $A^\emptyset = \{\emptyset\}$. Se A não é um conjunto vazio, não existem aplicações de A em $\emptyset$, pelo que $\emptyset^A = \emptyset$.

Dados conjuntos A e B, uma função $f : A \to B$, $X \subseteq A$ e $Y \subseteq B$, designamos por: **imagem de X por f** o conjunto $f(X) = \{f(x) : x \in X\}$; **imagem inversa** (ou **pré-imagem) de Y por f** o conjunto $f^{\leftarrow}(Y) = \{x \in A : f(x) \in Y\}$.

Existem alguns tipos de funções que desempenham um papel relevante no estudo da matemática.

Uma função $f : A \to B$ diz-se:

- **injetiva** se

$$\forall a, b \in A \;\; (a \neq b \Rightarrow f(a) \neq f(b))$$

  ou equivalentemente, se

$$\forall a, b \in A \;\; (f(a) = f(b) \Rightarrow a = b).$$

- **sobrejetiva** se

$$\forall b \in B \; \exists a \in A \;\; f(a) = b$$

  ou equivalentemente se

$$f(A) = B.$$

- **bijetiva** se f é injetiva e sobrejetiva, i.e., se

$$\forall b \in B \; \exists^1 a \in A \;\; f(a) = b.$$

Uma **família $(a_i \,|\, i \in I)$ de elementos de A**, também representável por $(a_i)_{i\in I}$, é uma função φ do conjunto I no conjunto A tal que $\varphi(i) = a_i$; o conjunto I é o **conjunto índice** da família $(a_i)_{i\in I}$. A imagem de I por φ é representada por $\{a_i \,|\, i \in I\}$.

Se $(A_i)_{i\in I}$ é uma família de subconjuntos de um certo conjunto A, a união e a interseção destes subconjuntos são representadas, respetivamente, por

$$\bigcup(A_i \,|\, i \in I), \;\; \bigcup\{A_i \,|\, i \in I\} \;\; \text{ou} \;\; \bigcup_{i\in I} A_i$$

e

$$\bigcap(A_i \,|\, i \in I), \quad \bigcap\{A_i \,|\, i \in I\} \quad \text{ou} \quad \bigcap_{i\in I} A_i$$

e são definidas por

$$\bigcup_{i\in I} A_i = \{x \in A \,|\, x \in A_i, \text{ para algum } i \in I\},$$

$$\bigcap_{i\in I} A_i = \{x \in A \,|\, x \in A_i, \text{ para todo } i \in I\}.$$

Se $I = \emptyset$, tem-se $\bigcup_{i\in I} A_i = \emptyset$ e $\bigcap_{i\in I} A_i = A$.

Sejam I um conjunto e $(A_i)_{i\in I}$ uma família de conjuntos. Designa-se por ***produto cartesiano*** da família $(A_i)_{i\in I}$, e representa-se por $\prod_{i\in I} A_i$, o conjunto de todas as funções f de I em $\bigcup_{i\in I} A_i$ tais que, para todo $i \in I$, $f(i) \in A_i$, i.e.,

$$\prod_{i\in I} A_i = \big\{f : I \to \bigcup_{i\in I} A_i \,|\, f(i) \in A_i, \forall i \in I\big\}.$$

Cada conjunto A_i designa-se por ***fator*** do produto cartesiano. Se $A_i = \emptyset$, para algum $i \in I$, tem-se $\prod_{i\in I} A_i = \emptyset$. No caso em que $I = \emptyset$, o conjunto $\prod_{i\in I} A_i$ tem exatamente um elemento, a função vazia; i.e., $\prod_{i\in I} A_i = \{\emptyset\}$. Se $A_i = A$, para todo $i \in I$, representa-se $\prod_{i\in I} A_i$ por A^I. No sentido de relacionar a definição de produto cartesiano da família $(A_i)_{i\in\{1,2,\ldots,n\}}$ com a definição de $A_1 \times A_2 \ldots \times A_n$, convenciona-se o uso do n-uplo $(a_1, a_2, \ldots, a_n)$ de elementos de A como uma representação da função $f \in A^{\{1,2,\ldots,n\}}$ tal que $a_1 = f(1)$, $a_2 = f(2)$, $\ldots a_n = f(n)$. Assim, $A_1 \times A_2 \times \ldots \times A_n = \prod_{i\in\{1,2,\ldots,n\}} A_i$.
Para cada $j \in I$, designa-se por ***projeção-j*** a aplicação $p_j : \prod_{i\in I} A_i \to A_j$ tal que $p_j(f) = f(j)$, para todo $f \in \prod_{i\in I} A_i$.

Dados um conjunto A e $n \in \mathbb{N}_0$, chama-se ***operação n-ária em*** A a qualquer função f de A^n em A e ao inteiro n dá-se a designação de ***aridade de*** f. Uma ***operação finitária*** é uma operação n-ária, para algum $n \in \mathbb{N}_0$. Atendendo a que todas as operações consideradas ao longo do texto são operações finitárias, em geral será omitida a palavra "finitária" e usa-se somente o termo "operação" para significar operação finitária. Se f é uma operação finitária num conjunto A e $(a_1, \ldots, a_n) \in A^n$, a imagem de $(a_1, \ldots, a_n)$ por f é representada por $f(a_1, \ldots, a_n)$. Se A é um conjunto não vazio, a aridade de uma operação em A é bem determinada. A uma operação em A de aridade 0 dá-se a designação de ***operação nulária***. Uma operação nulária é uma função $c : \{\emptyset\} \to A$, sendo esta função completamente determinada pelo elemento $c(\emptyset) \in A$ e usualmente identificada com esse elemento; por este motivo, as operações nulárias são também designadas por ***constantes***. Às operações de aridade 1, 2 e 3 é usual dar a designação de operações ***unárias***, ***binárias*** e ***ternárias***, respetivamente.

1.3 Relações de ordem parcial

Existem muitas propriedades que podem ser satisfeitas por uma relação binária definida num conjunto A. Nesta secção recordam-se noções básicas relacionadas com um tipo particular de relações binárias designadas por *relações de ordem*. A noção de ordem pode ser encontrada nas mais diversas situações do dia a dia, e sob variadas formas, quando fazemos referência a expressões tais como: primeiro, segundo, terceiro; maior versus menor; melhor versus pior; precedência, preferência, etc.

Definição 1.3.1. *Sejam P um conjunto e ρ uma relação binária em P. Diz-se que ρ é uma relação de* ***ordem parcial*** *em P se são satisfeitas as seguintes condições:*

(i) *para todo $a \in P$, $(a,a) \in \rho$.* *(reflexividade)*

(ii) *para quaisquer $a, b \in P$, $((a,b) \in \rho \text{ e } (b,a) \in \rho) \Rightarrow a = b$.* *(antissimetria)*

(iii) *para quaisquer $a, b, c \in P$, $((a,b) \in \rho \text{ e } (b,c) \in \rho) \Rightarrow (a,c) \in \rho$.* *(transitividade)*

Se adicionalmente, para quaisquer $a, b \in P$,

(iv) *$(a,b) \in \rho$ ou $(b,a) \in \rho$,*

a relação ρ diz-se uma relação de ***ordem total****.*
Se P é um conjunto não vazio e ρ é uma relação de ordem parcial em P, ao par (P,ρ) dá-se a designação de ***conjunto parcialmente ordenado*** *(c.p.o.); se ρ é uma relação de ordem total em P, o par (P,ρ) designa-se por* ***conjunto totalmente ordenado*** *ou por* ***cadeia****.*

Exemplo 1.3.2.
(1) *Sendo A um dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ e $\leq$ a relação "menor ou igual" usual em A, o par $(A,\leq)$ é um c.p.o..*
(2) *O par $(\mathbb{N},|)$, onde $|$ é a relação* divide *em $\mathbb{N}$, é um c.p.o..*
(3) *Dado um conjunto A, $(\mathcal{P}(A),\subseteq)$ é um c.p.o..*
(4) *Os c.p.o.s $(\mathbb{N},\leq)$, $(\mathbb{Z},\leq)$, $(\mathbb{Q},\leq)$ e $(\mathbb{R},\leq)$ são cadeias.*

Usualmente, representa-se uma ordem parcial definida num conjunto P por $\leq$ e o respetivo conjunto parcialmente ordenado por $(P,\leq)$. Dado um conjunto parcialmente ordenado $(P,\leq)$ e dados elementos $a, b \in P$, escrevemos:

- $a \leq b$, e lemos "a ***é menor ou igual a*** b", para representar $(a,b) \in \leq$;
- $a \not\leq b$, e lemos "a ***não é menor ou igual a*** b", para representar $(a,b) \notin \leq$;
- $a < b$, e lemos "a ***é menor do que*** b", se $a \leq b$ e $a \neq b$;
- $a \prec b$, e lemos "b ***é sucessor de*** a" (ou b ***cobre*** a ou a ***é coberto por*** b), se $a < b$ e $\neg(\exists\, c \in P, a \leq c \leq b)$.

Os elementos a e b dizem-se ***comparáveis*** se $a \leq b$ ou $b \leq a$; caso contrário, ou seja, se $a \not\leq b$ e $b \not\leq a$, diz-se que a e b são ***incomparáveis*** e escreve-se $a \parallel b$.

Um subconjunto A de P diz-se:

- uma ***cadeia em*** $(P, \leq)$ ou um ***conjunto totalmente ordenado em*** $(P, \leq)$ se, para quaisquer $a, b \in A$, a e b são comparáveis;
- uma ***anticadeia em*** $(P, \leq)$ se, para quaisquer $a, b \in A$ tais que $a \neq b$, $a \parallel b$.

O ***intervalo fechado*** $[a, b]$ representa o conjunto $\{c \in P \mid a \leq c \leq b\}$ e o ***intervalo aberto*** (a, b) representa o conjunto $\{c \in P \mid a < c < b\}$. Os intervalos $(a, b]$ e $[a, b)$ representam, respetivamente, os conjuntos $\{c \in P \mid a < c \leq b\}$ e $\{c \in P \mid a \leq c < b\}$.

Dado um subconjunto A de P, diz-se que A é um ***subconjunto convexo de*** P se, para quaisquer $a, b \in A$ e $c \in P$,

$$a \leq c \leq b \Rightarrow c \in A.$$

Claramente, para quaisquer $a, b \in P$, o intervalo fechado $[a, b]$ é um subconjunto convexo de P.

Dado um subconjunto A de P, podem existir elementos com propriedades especiais relativamente a A. Dado $m \in P$, diz-se que m é:

- um ***maximal*** de A se $m \in A$ e $\neg(\exists\, a \in A, m < a)$;
- um ***minimal*** de A se $m \in A$ e $\neg(\exists\, a \in A, a < m)$;
- um ***majorante*** de A se, para todo $a \in A$, $a \leq m$;
- um ***minorante*** de A se, para todo $a \in A$, $m \leq a$;
- um ***supremo*** de A se m é um majorante de A e $m \leq m'$, para qualquer majorante m' de A;
- um ***ínfimo*** de A se m é um minorante de A e $m' \leq m$, para qualquer minorante m' de A;
- um ***máximo*** de A se m é um majorante de A e $m \in A$;
- um ***mínimo*** de A se m é um minorante de A e $m \in A$.

O conjunto dos majorantes de A e o conjunto dos minorantes de A são representados por $\mathrm{Maj}(A)$ e $\mathrm{Min}(A)$, respetivamente. Caso exista, o supremo (ínfimo, máximo, mínimo) de um subconjunto A de P é único e representa-se por $\sup A$ ou $\bigvee A$ (respetivamente, $\inf A$ ou $\bigwedge A$, $\max A$, $\min A$). Se $A = \{a, b\}$, é usual escrever $a \vee b$ e $a \wedge b$ para representar $\bigvee A$ e $\bigwedge A$, respetivamente. Um conjunto parcialmente ordenado $(P, \leq)$ pode não ter elemento máximo nem elemento mínimo. O elemento máximo (mínimo) de $(P, \leq)$, caso exista, é representado por 1 (respetivamente, 0). Um conjunto parcialmente ordenado que tenha elemento máximo e elemento mínimo diz-se um ***conjunto parcialmente ordenado limitado***.

Das definições anteriores são imediatos os resultados seguintes, cuja prova fica ao cuidado do leitor.

Teorema 1.3.3. *Num conjunto parcialmente ordenado $(P, \leq)$ são equivalentes as seguintes afirmações, para quaisquer $a, b \in P$:*

(1) $a \leq b$;

(2) $\sup\{a, b\} = b$;

(3) $\inf\{a, b\} = a$.

Teorema 1.3.4. *Seja $(P, \leq)$ um conjunto parcialmente ordenado e sejam a, b, c, d elementos de P tais que $a \leq b$ e $c \leq d$.*

(1) *Se existem* $\inf\{a, c\}$ *e* $\inf\{b, d\}$, *então* $\inf\{a, c\} \leq \inf\{b, d\}$.

(2) *Se existem* $\sup\{a, c\}$ *e* $\sup\{b, d\}$, *então* $\sup\{a, c\} \leq \sup\{b, d\}$.

Diagramas de Hasse

Os conjuntos parcialmente ordenados finitos podem ser representados por meio de diagramas, designados por ***diagramas de Hasse***. Dado um conjunto parcialmente ordenado finito P, cada elemento de P é representado por um ponto do plano. Se a e b são elementos de P tais que $a \prec b$, o ponto associado ao elemento b é representado acima do ponto associado ao elemento a e unem-se os dois pontos por meio de um segmento de reta. A partir do diagrama de Hasse de um c.p.o. $(P, \leq)$ é possível identificar os elementos (a, b) de $\leq$; note-se que, dados $a, b \in P$, $a < b$ se e só se existe uma sequência finita de elementos $c_1, c_2 \ldots, c_{n-1}, c_n \in P$ tais que $a = c_1 \prec c_2 \prec \ldots \prec c_{n-1} \prec c_n = b$. Na figura seguinte apresentam-se alguns exemplos de diagramas de Hasse.

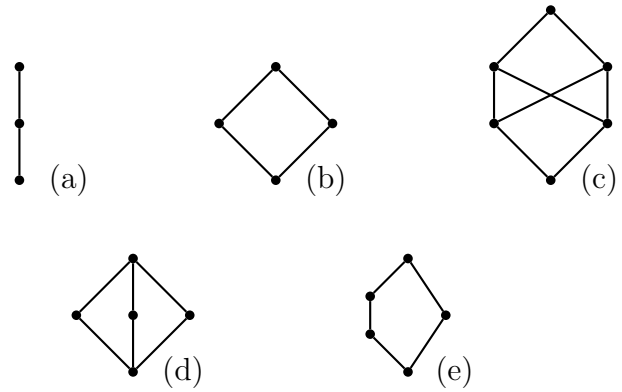


Figura 1.1

Construção de conjuntos parcialmente ordenados

Seguidamente descrevem-se alguns processos de construção de conjuntos parcialmente ordenados a partir de outros conjuntos parcialmente ordenados dados.

Se $(P, \leq)$ é um conjunto parcialmente ordenado e A é um subconjunto não vazio de P, a relação $\leq_{|_A}$ definida, para quaisquer $a, b \in A$, por

$$a \leq_{|_A} b \text{ se e só se } a \leq b$$

é uma relação de ordem parcial em A. A relação $\leq_{|_A}$ designa-se por ***ordem parcial induzida por*** $\leq$ em A.

Dado um conjunto parcialmente ordenado $(P, \leq)$, define-se a partir da relação $\leq$ uma outra relação de ordem parcial em P. A relação $\leq_d$ definida em P por

$$a \leq_d b \text{ se e só se } b \leq a$$

é também uma relação de ordem parcial em P. A relação $\leq_d$ designa-se por ***relação de ordem dual de*** $\leq$ e o conjunto parcialmente ordenado $(P, \leq_d)$ designa-se por ***conjunto parcialmente ordenado dual de*** $(P, \leq)$. É simples perceber que $(\leq_d)_d = \leq$ e que o c.p.o. dual de $(P, \leq_d)$ é $(P, \leq)$. Os c.p.o.s $(P, \leq)$ e $(P, \leq_d)$ dizem-se ***conjuntos parcialmente ordenados duais***.

Se Φ é uma afirmação sobre um conjunto parcialmente ordenado $(P, \leq)$, a afirmação Φ_d, obtida de Φ substituindo toda a ocorrência de $\leq$ por $\leq_d$, designa-se por ***afirmação dual de*** Φ. Note-se que se Φ é uma afirmação verdadeira em $(P, \leq)$, então Φ_d é verdadeira em $(P, \leq_d)$, pelo que é válido o princípio a seguir enunciado.

Princípio de dualidade para c.p.o.s Uma afirmação é verdadeira em qualquer conjunto parcialmente ordenado se e só se o mesmo acontece com a respetiva afirmação dual.

Observe-se que os conceitos de majorante, supremo, elemento máximo e elemento maximal são duais dos conceitos de minorante, ínfimo, elemento mínimo e elemento minimal, respetivamente. Assim, se Φ é uma afirmação sobre c.p.o.s envolvendo algum destes conceitos, a afirmação Φ_d é obtida substituindo cada um destes conceitos pelo conceito dual e substituindo toda a ocorrência de $\leq$ por $\leq_d$.

Dados dois conjuntos parcialmente ordenados $(P_1, \leq_1)$ e $(P_2, \leq_2)$, existem diferentes processos para construir novos c.p.o.s a partir dos c.p.o.s dados. Por exemplo, a relação binária $\leq$ definida em $P_1 \times P_2$ por

$$(a_1, a_2) \leq (b_1, b_2) \text{ se e só se } a_1 \leq_1 b_1 \text{ } e \text{ } a_2 \leq_2 b_2$$

é uma relação de ordem parcial e, por conseguinte, $(P_1 \times P_2, \leq)$ é um conjunto parcialmente ordenado, designado por ***produto de*** $(P, \leq_1)$ e $(P_2, \leq_2)$ e representado por $P_1 \times P_2$.
Este tipo de construção pode ser generalizado a um número finito de conjuntos parcialmente ordenados: se $(P_1, \leq_1)$, ..., $(P_n, \leq_n)$, com $n \in \mathbb{N}$, são conjuntos parcialmente ordenados, então $(P_1 \times \cdots \times P_n, \leq)$, onde $\leq$ é a relação definida em $P_1 \times \cdots \times P_n$ por

$$(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n) \text{ se e só se } a_1 \leq_1 b_1, \ldots, a_n \leq_n b_n,$$

é um conjunto parcialmente ordenado. Se $P_1 = P_2 = \ldots = P_n = P$ e $\leq_1 = \leq_2 = \ldots = \leq_n$, representa-se o c.p.o. $(P_1 \times \cdots \times P_n, \leq)$ por P^n.

Exemplo 1.3.5. *Considerando as cadeias* **2** *e* **3** *a seguir representadas*

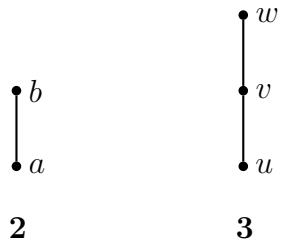


Figura 1.2

o c.p.o. produto destas duas cadeias, $(\mathbf{2}\times\mathbf{3},\leq)$*, pode ser representado pelo diagrama seguinte*

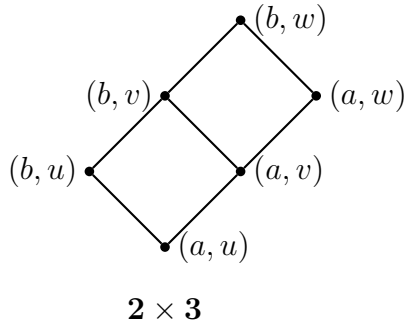


Figura 1.3

Aplicações entre conjuntos parcialmente ordenados

No estudo de aplicações entre conjuntos parcialmente ordenados têm particular interesse aquelas que preservam a ordem.

Definição 1.3.6. *Sejam* $(P_1,\leq_1)$ *e* $(P_2,\leq_2)$ *dois conjuntos parcialmente ordenados e* $\alpha : P_1 \to P_2$ *uma aplicação. Diz-se que:*

- *a aplicação* α ***preserva a ordem*** *ou que* α *é* ***isótona*** *se, para quaisquer* $a, b \in P_1$*,*

$$a \leq_1 b \Rightarrow \alpha(a) \leq_2 \alpha(b).$$

- *a aplicação* α *é* ***antítona*** *se, para quaisquer* $a, b \in P_1$*,*

$$a \leq_1 b \Rightarrow \alpha(b) \leq_2 \alpha(a).$$

- α *é um* ***mergulho de ordem*** *se, para quaisquer* $a, b \in P_1$*,*

$$a \leq_1 b \Leftrightarrow \alpha(a) \leq_2 \alpha(b).$$

- α *é um* ***isomorfismo de c.p.o.s*** *se* α *é um mergulho de ordem e é uma aplicação sobrejetiva.*

Caso exista um isomorfismo de c.p.o.s de $(P_1,\leq_1)$ *em* $(P_2,\leq_2)$*, diz-se que o c.p.o.* $(P_1,\leq_1)$ *é isomorfo ao c.p.o.* $(P_2,\leq_2)$*.*

Um isomorfismo de c.p.o.s é uma aplicação bijetiva. Assim, se α é um isomorfismo de um c.p.o. $(P_1, \leq_1)$ num c.p.o. $(P_2, \leq_2)$, então $\alpha^{-1} : P_2 \to P_1$ também é um isomorfismo de $(P_2, \leq_2)$ em $(P_1, \leq_1)$. Caso exista um isomorfismo entre os c.p.o.s $(P_1, \leq_1)$ e $(P_2, \leq_2)$ diz-se que os c.p.o.s são ***isomorfos*** e escreve-se $(P_1, \leq_1) \cong (P_2, \leq_2)$.

Note-se que, embora um isomorfismo de c.p.o.s seja uma aplicação isótona e bijetiva, uma aplicação bijetiva e isótona não é necessariamente um isomorfismo de c.p.o.s. Por exemplo, sendo $(P_1, \leq_1)$ e $(P_2, \leq_2)$ os c.p.o.s com os diagramas de Hasse a seguir apresentados

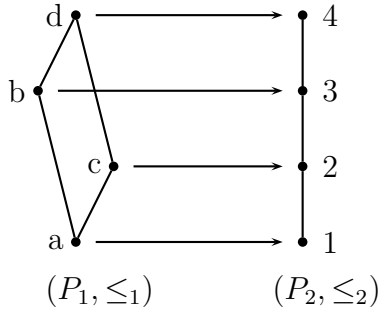


Figura 1.4

a aplicação α definida de P_1 em P_2 por $\alpha(a) = 1$, $\alpha(b) = 3$, $\alpha(c) = 2$ e $\alpha(d) = 4$, é isótona e bijetiva, mas não é um isomorfismo de c.p.o.s.

De entre as aplicações isótonas destacam-se as que a seguir se definem.

Definição 1.3.7. *Seja $(P, \leq)$ um conjunto parcialmente ordenado. Uma aplicação $f : P \to P$ diz-se um **operador de fecho em** $(P, \leq)$ se, para quaisquer $x, y \in P$, são satisfeitas as seguintes condições:*

F1: $x \leq f(x)$;

F2: $f^2(x) \leq f(x)$;

F3: $x \leq y \Rightarrow f(x) \leq f(y)$.

*Dado um operador de fecho $f : P \to P$ e dado $p \in P$, designa-se o elemento $f(p)$ por **fecho de** p. O elemento p diz-se **fechado para** f se $f(p) = p$. O conjunto dos elementos de P fechados para f é representado por $Fc_f(P)$.*

Dado um conjunto A, já observámos anteriormente que $(\mathcal{P}(A), \subseteq)$ é um conjunto parcialmente ordenado. Um operador de fecho f em $(\mathcal{P}(A), \subseteq)$ é usualmente designado por ***operador de fecho em*** A.
O conjunto parcialmente ordenado dos subconjuntos de A fechados para f, com a relação de inclusão, é representado por $(Fc_f(\mathcal{P}(A)), \subseteq)$.
Dados subconjuntos X e Y de A tais que X é fechado para f, diz-se que Y é um ***conjunto gerador de*** X se $f(Y) = X$; caso exista um conjunto gerador de X que

seja finito, o conjunto X diz-se ***finitamente gerado***.
Um operador de fecho f em $(\mathcal{P}(A), \subseteq)$ diz-se um ***operador de fecho algébrico*** se, para qualquer $X \subseteq A$,

F4: $f(X) = \bigcup\{f(Y) : Y \subseteq X \text{ e } Y \text{ é finito }\}$.

1.4 Relações de equivalência

No estudo de álgebra universal também são relevantes as relações binárias designadas por *relações de equivalência*.

Sejam A um conjunto e θ uma relação binária em A. Diz-se que θ é uma ***relação de equivalência*** em A se são satisfeitas as seguintes condições:

(i) para todo $a \in A$, $(a, a) \in \theta$, (reflexividade)

(ii) para quaisquer $a, b \in A$, $(a, b) \in \theta \Rightarrow (b, a) \in \theta$, (simetria)

(iii) para quaisquer $a, b, c \in A$, $(a, b) \in \theta$ e $(b, c) \in \theta \Rightarrow (a, c) \in \theta$. (transitividade)

Uma relação de equivalência θ definida num conjunto A determina uma partição de A em subconjuntos não vazios e disjuntos. Dado um elemento $x \in A$, chama-se **classe de equivalência de x módulo θ** ou, caso não haja ambiguidade, **classe de equivalência de x**, ao conjunto

$$[x]_\theta = \{y \in A \mid x\,\theta\,y\}.$$

Ao conjunto de todas as classes de equivalência dos elementos de A chamamos **conjunto quociente de A módulo θ** e representamo-lo por A/θ, ou seja,

$$A/\theta = \{[x]_\theta \mid x \in A\}.$$

O conjunto de todas as relações de equivalência definidas num conjunto A é representado por $\mathrm{Eq}(A)$.

Teorema 1.4.1. *Seja A um conjunto. Então, para quaisquer $\theta_1, \theta_2 \in \mathrm{Eq}(A)$,*

(a) $\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2$,

(b) $\theta_1 \vee \theta_2 = \{(x, y) \in A^2 \mid \exists\, n \in \mathbb{N}, \exists\, z_0, z_1, \ldots, z_n \in A : x = z_0, y = z_n$
$e\ \forall 1 \leq k \leq n, z_{k-1}\,\theta_1\,z_k$ *ou* $z_{k-1}\,\theta_2\,z_k\}$. □

Observe-se que se θ_1 e θ_2 são relações de equivalência num conjunto A, tem-se

$$\theta_1 \vee \theta_2 = \theta_1 \cup (\theta_1 \circ \theta_2) \cup (\theta_1 \circ \theta_2 \circ \theta_1) \cup (\theta_1 \circ \theta_2 \circ \theta_1 \circ \theta_2) \cup \ldots.$$

O teorema anterior pode ser generalizado a famílias de relações de equivalência definidas num conjunto A.

Teorema 1.4.2. *Sejam A um conjunto, I um conjunto e $(\theta_i \mid i \in I)$ uma família de relações de equivalência em A. Então*

(a) $\bigwedge_{i\in I} \theta_i = \bigcap_{i\in I} \theta_i$,

(b) $\bigvee_{i\in I} \theta_i = \bigcup \{\theta_{i_0} \circ \theta_{i_1} \circ \ldots \circ \theta_{i_k} \mid i_0, i_1, \ldots, i_k \in I, k \in \mathbb{N}_0\}$. □

2. Reticulados

Na primeira metade do século dezanove, o estudo de George Boole para formalizar a lógica proposicional conduziu ao conceito de álgebras de Boole. Posteriormente, Charles S. Pierce e Ernst Schröder ao investigarem a axiomatização das álgebras de Boole acharam relevante introduzir o conceito de reticulado. Num estudo independente, a investigação de Richard Dedekind sobre ideais de números algébricos conduziu ao mesmo conceito. Embora muitos dos resultados desenvolvidos por estes matemáticos fossem de grande relevância, tais resultados não atraíram a atenção da comunidade científica da altura. O desenvolvimento da teoria de reticulados só veio a acontecer mais tarde, impulsionado pelo trabalho levado a cabo por Garret Birkhoff.

Duas definições de reticulados

Os reticulados podem ser definidos de duas formas equivalentes: como conjuntos parcialmente ordenados e como estruturas algébricas. Nesta secção apresentamos estas definições e verificamos a equivalência das duas.

Definição 2.0.3. *Um conjunto parcialmente ordenado* $(R, \leq)$ *diz-se um* ***reticulado*** *se, para quaisquer* $a, b \in R$*, existem* $\inf\{a, b\}$ *e* $\sup\{a, b\}$*.*

Exemplo 2.0.4.
(1) *Com excepção do conjunto parcialmente ordenado apresentado na figura* 1.1 *em* (c)*, todos os restantes conjuntos parcialmente ordenados apresentados nessa figura são reticulados.*
(2) *Todas as cadeias são reticulados.*
(3) *Dado um conjunto* A*, o conjunto parcialmente ordenado* $(\mathcal{P}(A), \subseteq)$ *é um reticulado, tendo-se, para quaisquer* $X, Y \subseteq A$*,*

$$\inf\{X, Y\} = X \cap Y \text{ e } \sup\{X, Y\} = X \cup Y.$$

(4) *Sendo* $\mathrm{Subg}(G)$ *o conjunto dos subgrupos de um grupo* G *e* $\subseteq$ *a relação de inclusão usual, o par* $(\mathrm{Subg}(G), \subseteq)$ *é um reticulado, tendo-se, para quaisquer* G_1, $G_2 \in \mathrm{Subg}(G)$*,*

$$\inf\{G_1, G_2\} = G_1 \cap G_2 \text{ e } \sup\{G_1, G_2\} = < G_1 \cup G_2 > .$$

Se $(R, \leq)$ é um reticulado, o seu c.p.o. dual $(R, \leq_d)$ também é um reticulado. Sendo assim, é válido o princípio seguinte.

Princípio de Dualidade para Reticulados Uma afirmação é verdadeira em qualquer reticulado se e só se o mesmo acontece com a respetiva afirmação dual.

Um reticulado, enquanto estrutura algébrica, é definido com base em duas operações binárias que satisfazem as propriedades a seguir indicadas.

Definição 2.0.5. *Um triplo $\mathcal{R} = (R; \wedge, \vee)$, onde R é um conjunto não vazio e $\wedge$ e $\vee$ são operações binárias em R, diz-se um* ***reticulado*** *se, para quaisquer $x, y, z \in R$,*

R1:	$x \wedge y = y \wedge x$,	$x \vee y = y \vee x$	*(leis comutativas);*
R2:	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$,	$x \vee (y \vee z) = (x \vee y) \vee z$	*(leis associativas);*
R3:	$x \wedge x = x$,	$x \vee x = x$	*(leis de idempotência);*
R4:	$x \wedge (x \vee y) = x$,	$x \vee (x \wedge y) = x$	*(leis de absorção).*

Exemplo 2.0.6. *São reticulados as estruturas seguintes:*

(1) $(P; \wedge, \vee)$*, onde P representa o conjunto das proposições, $\wedge$ representa o conetivo conjunção e $\vee$ representa o conetivo disjunção.*

(2) $(\mathbb{N}; \text{m.d.c.}, \text{m.m.c.})$*, onde* m.d.c. *representa a operação máximo divisor comum em $\mathbb{N}$ e* m.m.c. *representa a operação mínimo múltiplo comum.*

(3) $(\mathcal{P}(A); \cap, \cup)$, onde A é um conjunto e $\cap$ e $\cup$ são, respetivamente, as operações de interseção e união.

As duas definições de reticulado apresentadas anteriormente são equivalentes.

Teorema 2.0.7. *(1) Se $\mathcal{R} = (R; \wedge, \vee)$ é um reticulado, então a relação $\leq$ definida em R por*

$$x \leq y \ \text{ se } \ x = x \wedge y$$

é uma relação de ordem parcial tal que, para quaisquer $x, y \in R$, existem $\inf\{x, y\}$ *e* $\sup\{x, y\}$ *e tem-se*

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

(2) Se $(R, \leq)$ é um conjunto parcialmente ordenado tal que, para quaisquer $x, y \in R$, existem $\inf\{x, y\}$ *e* $\sup\{x, y\}$*, então $\mathcal{R} = (R; \wedge, \vee)$, onde*

$$x \wedge y = \inf\{x, y\} \ \text{ e } \ x \vee y = \sup\{x, y\},$$

é um reticulado e, para quaisquer $x, y \in R$,

$$x \leq y \Leftrightarrow x = x \wedge y \Leftrightarrow y = x \vee y.$$

Demonstração. (1) Suponhamos que $\mathcal{R} = (R; \wedge, \vee)$ é um reticulado. Seja $\leq$ a relação definida por

$$x \leq y \text{ se } x = x \wedge y.$$

De $x \wedge x = x$ segue que $x \leq x$. Se $x \leq y$ e $y \leq x$, então $x = x \wedge y$ e $y = y \wedge x$ e, portanto, $x = y$. Se $x \leq y$ e $y \leq z$, então $x = x \wedge y$ e $y = y \wedge z$, donde temos $x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$ e, por conseguinte, $x \leq z$. Logo a relação $\leq$ é uma ordem parcial em R.
De $x = x \wedge (x \vee y)$ e $y = y \wedge (x \vee y)$, temos $x \leq x \vee y$ e $y \leq x \vee y$, pelo que $x \vee y$ é um majorante de $\{x, y\}$. Além disso, se $x \leq u$ e $y \leq u$, tem-se $x \vee u = (x \wedge u) \vee u = u$ e $y \vee u = (y \wedge u) \vee u = u$, donde $(x \vee u) \vee (y \vee u) = u$. Assim, $(x \vee y) \vee u = u$, pelo que $(x \vee y) \wedge u = (x \vee y) \wedge [(x \vee y) \vee u] = x \vee y$ e, portanto, $x \vee y \leq u$. Logo $\sup\{x, y\} = x \vee y$. De forma análoga prova-se que $\inf\{x, y\} = x \wedge y$.

(2) Reciprocamente, se $(R, \leq)$ é um conjunto parcialmente ordenado tal que, para quaisquer $x, y \in R$, existem $\inf\{x, y\}$ e $\sup\{x, y\}$, é simples verificar que as operações $\wedge$ e $\vee$ definidas por $x \wedge y = \inf\{x, y\}$ e $x \vee y = \sup\{x, y\}$ satisfazem as condições R1 a R4 e que

$$x \leq y \Leftrightarrow x = x \wedge y \Leftrightarrow y = x \vee y.$$

□

Do resultado anterior segue que os reticulados, considerados como estruturas algébricas, podem ser completamente caracterizados em termos das operações supremo e ínfimo. Assim, se Φ é uma afirmação sobre reticulados expressa em termos de $\wedge$ e $\vee$, a afirmação dual de Φ é obtida trocando as ocorrências de $\wedge$ e $\vee$, respetivamente, por $\vee$ e $\wedge$. Se $\mathcal{R} = (R; \wedge, \vee)$ é um reticulado, o seu reticulado dual é $\mathcal{R}^d = (R; \vee, \wedge)$.

Descrição de reticulados

Para ilustrar certos resultados ou para refutar conjeturas a respeito de reticulados pode ser conveniente descrever exemplos de reticulados. Atendendo a que os reticulados são casos particulares de conjuntos parcialmente ordenados, a descrição de reticulados finitos pode ser feita por meio de diagramas de Hasse. Alternativamente, considerando um reticulado como uma estrutura algébrica $(R; \wedge, \vee)$, um reticulado pode ser descrito recorrendo às tabelas das operações $\wedge$ e $\vee$.

Exemplo 2.0.8. *As duas tabelas seguintes*

$\wedge$	*0*	*a*	*b*	*1*
0	*0*	*0*	*0*	*0*
a	*0*	*a*	*0*	*a*
b	*0*	*0*	*b*	*b*
1	*0*	*a*	*b*	*1*

$\vee$	*0*	*a*	*b*	*1*
0	*0*	*a*	*b*	*1*
a	*a*	*a*	*1*	*1*
b	*b*	*1*	*b*	*1*
1	*1*	*1*	*1*	*1*

descrevem o reticulado representado pelo diagrama de Hasse

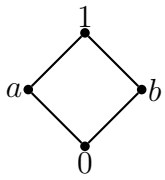


Figura 2.1

Subrreticulados

De entre os subconjuntos de um reticulado têm particular interesse aqueles que são fechados para as operações do reticulado - a estes subconjuntos dá-se a designação de subrreticulados.

Definição 2.0.9. *Sejam $\mathcal{R} = (R; \wedge, \vee)$ um reticulado, R' um subconjunto não vazio de R e $\wedge'$ e $\vee'$ operações binárias em R'. Diz-se que $\mathcal{R}' = (R'; \wedge', \vee')$ é um* ***subrreticulado*** *de $\mathcal{R}$ se, para quaisquer $a, b \in R'$, $a \wedge b \in R'$, $a \vee b \in R'$ e*

$$a \wedge' b = a \wedge b \quad e \quad a \vee' b = a \vee b.$$

Note-se que se $\leq$ é a relação de ordem parcial associada a um reticulado $\mathcal{R} = (R; \wedge, \vee)$ e R' é um subconjunto não vazio de R, não é suficiente que $(R', \leq_{|_{R'}})$ seja um reticulado para que seja um subrreticulado de $(R, \leq)$. De facto, é possivel encontrar reticulados $(R, \leq)$ e subconjuntos R' de R tais que $(R', \leq_{|_{R'}})$ é um reticulado mas não é um subrreticulado de $(R, \leq)$. O exemplo seguinte ilustra este tipo de situação. Considerando o reticulado $(\{a, b, c, d, e\}, \leq)$ a seguir representado e sendo $R' = \{a, c, d, e\}$, verifica-se que $(R', \leq_{|_{R'}})$ é um reticulado mas não é subrreticulado do reticulado indicado.

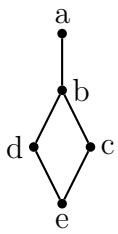


Figura 2.2

Dados um reticulado $(R, \leq)$ e um subconjunto não vazio R' de R, um c.p.o. $(R', \leq')$ diz-se um subrreticulado de $(R, \leq)$ se $\leq' = \leq_{|_{R'}}$ e, para quaisquer $a, b \in R'$, o supremo e o infímo de $\{a, b\}$ (determinados em $(R, \leq)$) pertencem a R'.

Produtos

A partir de reticulados $\mathcal{R}_1 = (R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$ e $\mathcal{R}_2 = (R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$ define-se naturalmente um reticulado que tem $R_1 \times R_2$ como conjunto suporte.

Teorema 2.0.10. *Sejam $\mathcal{R}_1 = (R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$, $\mathcal{R}_2 = (R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$ reticulados e $\wedge_{\mathcal{R}_1 \times \mathcal{R}_2}$ e $\vee_{\mathcal{R}_1 \times \mathcal{R}_2}$ as operações binárias em $R_1 \times R_2$ definidas por*

$$(a_1, a_2) \wedge_{\mathcal{R}_1 \times \mathcal{R}_2} (b_1, b_2) = (a_1 \wedge_{\mathcal{R}_1} b_1, a_2 \wedge_{\mathcal{R}_2} b_2),$$
$$(a_1, a_2) \vee_{\mathcal{R}_1 \times \mathcal{R}_2} (b_1, b_2) = (a_1 \vee_{\mathcal{R}_1} b_1, a_2 \vee_{\mathcal{R}_2} b_2).$$

Então $(R_1 \times R_2; \wedge_{\mathcal{R}_1 \times \mathcal{R}_2}, \vee_{\mathcal{R}_1 \times \mathcal{R}_2})$ é um reticulado.

A prova do teorema anterior é um exercício simples que fica ao cuidado do leitor.

Definição 2.0.11. *Sejam $\mathcal{R}_1 = (R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$, $\mathcal{R}_2 = (R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$ reticulados e $\wedge_{\mathcal{R}_1 \times \mathcal{R}_2}$ e $\vee_{\mathcal{R}_1 \times \mathcal{R}_2}$ as operações binárias em $R_1 \times R_2$ definidas por*

$$(a_1, a_2) \wedge_{\mathcal{R}_1 \times \mathcal{R}_2} (b_1, b_2) = (a_1 \wedge_{\mathcal{R}_1} b_1, a_2 \wedge_{\mathcal{R}_2} b_2),$$
$$(a_1, a_2) \vee_{\mathcal{R}_1 \times \mathcal{R}_2} (b_1, b_2) = (a_1 \vee_{\mathcal{R}_1} b_1, a_2 \vee_{\mathcal{R}_2} b_2).$$

*Designa-se por **reticulado produto de** $\mathcal{R}_1$ e $\mathcal{R}_2$, e representa-se por $\mathcal{R}_1 \times \mathcal{R}_2$, o reticulado $(R_1 \times R_2; \wedge_{\mathcal{R}_1 \times \mathcal{R}_2}, \vee_{\mathcal{R}_1 \times \mathcal{R}_2})$.*

Sejam $\mathcal{R}_1 = (R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$ e $\mathcal{R}_2 = (R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$ reticulados, $\leq_1$ e $\leq_2$ as relações de ordem associadas, respetivamente, a $\mathcal{R}_1$ e $\mathcal{R}_2$ e seja $\leq$ a relação de ordem definida em $R_1 \times R_2$ por

$$(a_1, a_2) \leq (b_1, b_2) \text{ se e só se } a_1 \leq_1 b_1 \text{ e } a_2 \leq_2 b_2.$$

Então $(R_1 \times R_2, \leq)$ é um reticulado. Além disso,

$$\begin{aligned} (a_1, a_2) \wedge_{\mathcal{R}_1 \times \mathcal{R}_2} (b_1, b_2) = (a_1, a_2) &\Leftrightarrow a_1 \wedge_{\mathcal{R}_1} b_1 = a_1 \text{ e } a_2 \wedge_{\mathcal{R}_2} b_2 = a_2 \\ &\Leftrightarrow a_1 \leq_1 b_1 \text{ e } a_2 \leq_2 b_2 \\ &\Leftrightarrow (a_1, a_2) \leq (b_1, b_2). \end{aligned}$$

Por conseguinte, o reticulado produto $\mathcal{R}_1 \times \mathcal{R}_2 = (R_1 \times R_2; \wedge_{\mathcal{R}_1 \times \mathcal{R}_2}, \vee_{\mathcal{R}_1 \times \mathcal{R}_2})$ coincide com o reticulado $(R_1 \times R_2, \leq)$.

Homomorfismos, isomorfismos

Quando se consideram reticulados como estruturas algébricas tem interesse considerar aplicações que preservem as operações dos reticulados - os *homomorfismos*.

Definição 2.0.12. *Sejam $\mathcal{R}_1 = (R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$ e $\mathcal{R}_2 = (R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$ reticulados e $\alpha : R_1 \to R_2$ uma aplicação. Diz-se que:*

- *α é um **homomorfismo de** $\mathcal{R}_1$ em $\mathcal{R}_2$ se, para quaisquer $a, b \in R_1$,*

$$\alpha(a \wedge_{\mathcal{R}_1} b) = \alpha(a) \wedge_{\mathcal{R}_2} \alpha(b) \text{ e } \alpha(a \vee_{\mathcal{R}_1} b) = \alpha(a) \vee_{\mathcal{R}_2} \alpha(b);$$

- *α é um **isomorfismo de** $\mathcal{R}_1$ em $\mathcal{R}_2$ se α é bijetiva e é um homomorfismo.*

Caso exista um isomorfismo de reticulados de $\mathcal{R}_1$ em $\mathcal{R}_2$, o reticulado $\mathcal{R}_1$ diz-se ***isomorfo*** *ao reticulado $\mathcal{R}_2$.*

Note-se que se α é um isomorfismo de um reticulado $\mathcal{R}_1$ para um reticulado $\mathcal{R}_2$, então α^{-1} é um isomorfismo de $\mathcal{R}_2$ para $\mathcal{R}_1$. Assim, caso exista um isomorfismo de um reticulado noutro, diz-se somente que os reticulados são isomorfos.

Uma vez que os reticulados também são estruturas ordenadas, importa perceber qual a relação existente entre os homomorfismos e as aplicações que preservam a ordem. A noção de isomorfismo entre reticulados pode ser estabelecida recorrendo às relações de ordem associadas aos mesmos reticulados.

Teorema 2.0.13. *Sejam $\mathcal{R}_1 = (R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$ e $\mathcal{R}_2 = (R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$ reticulados e $\leq_1$ e $\leq_2$ as relações de ordem definidas, respetivamente, em R_1 e R_2 por*

$$a \leq_1 b \text{ sse } a = a \wedge_{\mathcal{R}_1} b, \text{ para quaisquer } a, b \in R_1,$$

$$a \leq_2 b \text{ sse } a = a \wedge_{\mathcal{R}_2} b, \text{ para quaisquer } a, b \in R_2.$$

Então os reticulados $\mathcal{R}_1 = (R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$ e $\mathcal{R}_2 = (R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$ são isomorfos se e só se os c.p.o.s $(R_1, \leq_1)$ e $(R_2, \leq_2)$ são isomorfos.

Demonstração. Suponhamos que $(R_1; \wedge_1, \vee_1)$ e $(R_2; \wedge_2, \vee_2)$ são reticulados isomorfos. Então existe uma aplicação bijetiva $\alpha : R_1 \to R_2$ tal que, para quaisquer $a, b \in R_1$,

$$\alpha(a \vee_1 b) = \alpha(a) \vee_2 \alpha(b) \text{ e } \alpha(a \wedge_1 b) = \alpha(a) \wedge_2 \alpha(b). \tag{1}$$

Mostremos que α é um isomorfismo de c.p.o.s., ou seja, mostremos que a aplicação α é sobrejetiva e que, para quaisquer $a, b \in R_1$,

$$a \leq_1 b \Leftrightarrow \alpha(a) \leq_2 \alpha(b). \tag{2}$$

Atendendo a que α é bijetiva, é imediato que α é sobrejetiva. Considerando (1), a prova de (2) também é simples. De facto, dados $a, b \in R_1$, se $a \leq_1 b$, então $a = a \wedge_1 b$, donde $\alpha(a) = \alpha(a \wedge_1 b) = \alpha(a) \wedge_2 \alpha(b)$. Logo $\alpha(a) \leq_2 \alpha(b)$. Reciprocamente, se $\alpha(a) \leq_2 \alpha(b)$ tem-se $\alpha(a) \vee_2 \alpha(b) = \alpha(b)$, pelo que $\alpha(a \vee_1 b) = \alpha(b)$. Uma vez que α é invertível segue que $\alpha^{-1}(\alpha(a \vee_1 b)) = \alpha^{-1}(\alpha(b))$ e, portanto, $a \vee_1 b = b$. Logo $a \leq_1 b$. Assim, provámos que α é uma aplicação sobrejetiva e um mergulho de ordem, isto é, α é um isomorfismo de c.p.o.s.

Reciprocamente, admitamos que $(R_1, \leq_1)$ e $(R_2, \leq_2)$ são c.p.o.s isomorfos. Então existe uma aplicação sobrejetiva $\alpha : R_1 \to R_2$ que satisfaz a condição (2). Pretendemos mostrar que α é um isomorfismo de $(R_1; \wedge_{\mathcal{R}_1}, \vee_{\mathcal{R}_1})$ em $(R_2; \wedge_{\mathcal{R}_2}, \vee_{\mathcal{R}_2})$, isto é, que α é um homomorfismo bijetivo. Para provar que α é bijetiva, resta mostrar que α é injetiva. Se a, b são elementos de R_1 tais que $\alpha(a) = \alpha(b)$, então $\alpha(a) \leq_2 \alpha(b)$ e $\alpha(b) \leq_2 \alpha(a)$. Logo, atendendo a (2), segue que $a \leq b$ e $b \leq a$ e, por conseguinte, $a = b$. Assim, α é injetiva. Facilmente também se prova que α é um homomorfismo. De facto, dados $a, b \in R_1$, tem-se $a \leq_1 a \vee_1 b$ e $b \leq_1 a \vee_1 b$. Então, por

(2), $\alpha(a) \leq_2 \alpha(a \vee_1 b)$ e $\alpha(b) \leq_2 \alpha(a \vee_1 b)$. Assim, $\alpha(a \vee_1 b)$ é um majorante de $\{\alpha(a), \alpha(b)\}$ e, atendendo a que $\alpha(a) \vee_2 \alpha(b)$ é o supremo de $\{\alpha(a), \alpha(b)\}$, resulta que $\alpha(a) \vee_2 \alpha(b) \leq \alpha(a \vee_1 b)$. Provemos, agora, que $\alpha(a \vee_1 b) \leq \alpha(a) \vee_2 \alpha(b)$. Por hipótese, a aplicação α é sobrejetiva, pelo que $\alpha(a) \vee_2 \alpha(b) = \alpha(c)$, para algum $c \in R_1$. Logo $\alpha(a) \leq_2 \alpha(c)$ e $\alpha(b) \leq_2 \alpha(c)$ e por (2) segue que $a \leq_1 c$ e $b \leq_1 c$. Assim, $a \vee_1 b \leq_1 c$ e de (2) resulta $\alpha(a \vee_1 b) \leq_2 \alpha(c)$. Consequentemente, $\alpha(a \vee_1 b) \leq_2 \alpha(a) \vee_2 \alpha(b)$. Desta forma, provámos que $\alpha(a \vee_1 b) = \alpha(a) \vee_2 \alpha(b)$, para quaisquer $a, b \in R_1$ e, portanto, α é um homomorfismo. □

Reticulados completos, reticulados algébricos

Apresentam-se seguidamente duas classes de reticulados que desempenham um papel relevante no estudo de álgebra universal.

Definição 2.0.14. *Um reticulado $(R, \leq)$ diz-se um* ***reticulado completo*** *se, para qualquer subconjunto S de R, existem $\bigwedge S$ e $\bigvee S$.*

Exemplo 2.0.15.
(1) *O reticulado $(\mathbb{R}, \leq)$ não é completo.*
(2) *O reticulado $(\mathbb{R} \cup \{-\infty, \infty\}, \leq)$ é completo.*
(3) *O reticulado $(\{x \in \mathbb{R} : |x| < 1\} \cup \{-2, 2\}, \leq)$ é completo.*
(4) *Dado um conjunto A, $(\mathcal{P}(A), \subseteq)$ é um reticulado completo.*

Se $(R, \leq)$ é um reticulado, então, para qualquer suconjunto F de R que seja finito, existem $\bigvee F$ e $\bigwedge F$. Por conseguinte, é imediato o resultado seguinte.

Teorema 2.0.16. *Todo o reticulado finito é completo.*

Na definição anterior é possível prescindir de uma das condições que caracterizam os reticulados completos, uma vez que é válido o resultado seguinte.

Teorema 2.0.17. *Seja $(R, \leq)$ um reticulado tal que existe $\bigvee S$ para qualquer subconjunto S de R ou tal que existe $\bigwedge S$ para qualquer subconjunto S de R. Então $(R, \leq)$ é um reticulado completo.*

Demonstração. Suponhamos que existe $\bigvee S$ para qualquer subconjunto S de R. Seja M_S o conjunto dos minorantes de S. É um exercício simples verificar que $\bigvee M_S$ é o ínfimo de S. Analogamente, caso exista $\bigwedge S$ para qualquer subconjunto S de R, prova-se que também existe $\bigvee S$. □

Observe-se que se $(R, \leq)$ é um reticulado completo, então R tem elemento máximo 1 e elemento mínimo 0 e tem-se $\bigvee \emptyset = 0$ e $\bigwedge \emptyset = 1$. Note-se também que o teorema anterior pode ser formulado de forma equivalente dos seguintes modos: (i) um reticulado $(R, \leq)$ é completo se R tem elemento máximo e existe ínfimo

de qualquer subconjunto não vazio de R; (ii) um reticulado $(R, \leq)$ é completo se R tem elemento mínimo e existe supremo de qualquer subconjunto não vazio de R.

Um reticulado completo pode ter subrreticulados que não são completos; por exemplo, $(\mathbb{R}, \leq)$ é um subrreticulado de $(\mathbb{R} \cup \{-\infty, \infty\}, \leq)$. Pode também acontecer que o subrreticulado de um reticulado completo seja um reticulado completo, mas os supremos e ínfimos de certos subconjuntos quando determinados no subrreticulado não coincidam com os supremos e os ínfimos no reticulado; é o caso do reticulado $(\{x \in \mathbb{R} : |x| < 1\} \cup \{-2, 2\}, \leq)$ que é um subrreticulado de $(\mathbb{R} \cup \{-\infty, \infty\}, \leq)$.

Definição 2.0.18. *Um subrreticulado $(R', \leq_{|_{R'}})$ de um reticulado $(R, \leq)$ diz-se um* ***subrreticulado completo de*** *$(R, \leq)$ se, para qualquer subconjunto S de R', $\bigvee S$ e $\bigwedge S$, como definidos em $(R, \leq)$, pertencem a R'.*

Definição 2.0.19. *Seja $(R, \leq)$ um reticulado. Um elemento $a \in R$ diz-se* ***compacto*** *se sempre que existe $\bigvee A$ e $a \leq \bigvee A$, para algum $A \subseteq R$, então $a \leq \bigvee B$, para algum conjunto finito $B \subseteq A$. Um reticulado $(R, \leq)$ diz-se* ***compactamente gerado*** *se, para todo $a \in R$, $a = \bigvee S$, para algum subconjunto S de R formado por elementos compactos de R. Um reticulado $(R, \leq)$ diz-se um* ***reticulado algébrico*** *se é um reticulado completo e compactamente gerado.*

Exemplo 2.0.20.
(1) *Todos os elementos de um reticulado finito são compactos.*
(2) *Dado um conjunto A, o reticulado $(\mathcal{P}(A), \subseteq)$ é algébrico; os elementos compactos deste reticulado são os subconjuntos finitos de A.*
(3) *O reticulado* $(\mathrm{Subg}(G), \subseteq)$*, dos subgrupos de um grupo G, é algébrico; os elementos compactos deste reticulado são os subgrupos de G finitamente gerados.*

Dados um conjunto A e um operador fecho f em $(\mathcal{P}(A), \subseteq)$, facilmente se verifica que o conjunto parcialmente ordenado dos subconjuntos de A fechados para f é um reticulado completo.

Teorema 2.0.21. *Sejam A um conjunto e f um operador de fecho em $(\mathcal{P}(A), \subseteq)$. Então $(Fc_f(\mathcal{P}(A)), \subseteq)$ é um reticulado completo e, para qualquer família $(A_i)_{i \in I}$ de subconjuntos fechados de A, tem-se*

$$\bigwedge_{i \in I} f(A_i) = \bigcap_{i \in I} f(A_i) \quad e \quad \bigvee_{i \in I} f(A_i) = f\left(\bigcup_{i \in I} A_i\right).$$

Demonstração. Seja $(A_i)_{i \in I}$ uma família de subconjuntos fechados de A. Uma vez que, para cada $i \in I$,

$$\bigcap_{i \in I} A_i \subseteq A_i,$$

tem-se

$$f\left(\bigcap_{i\in I} A_i\right) \subseteq f(A_i) = A_i.$$

Assim,

$$f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} A_i,$$

e, por conseguinte,

$$f\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} A_i.$$

Logo, $\bigcap_{i\in I} A_i$ é um elemento de $Fc_f(\mathcal{P}(A))$. Atendendo a que A também é um elemento de $Fc_f(\mathcal{P}(A))$, conclui-se que $(Fc_f(\mathcal{P}(A)), \subseteq)$ é um reticulado completo. A prova das igualdades indicadas no enunciado é simples. □

Reciprocamente, todo o reticulado completo pode ser visto como o reticulado dos subconjuntos fechados de algum conjunto com um operador de fecho.

Teorema 2.0.22. *Seja $(R, \leq)$ um reticulado completo. Então $(R, \leq)$ é isomorfo ao reticulado dos subconjuntos fechados de algum conjunto A com um operador de fecho f.*

Demonstração. Seja $(R, \leq)$ um reticulado completo. Facilmente prova-se que a aplicação $f : \mathcal{P}(R) \to \mathcal{P}(R)$ definida por

$$f(X) = \{a \in R : a \leq \sup X\}$$

é um operador de fecho em $(\mathcal{P}(R), \subseteq)$ e que a aplicação $a \mapsto \{b \in R : b \leq a\}$ é um isomorfismo entre $(R, \leq)$ e $(Fc_f(\mathcal{P}(R)), \subseteq)$. □

Teorema 2.0.23. *Seja A um conjunto. Se f é um operador de fecho algébrico em $(\mathcal{P}(A), \subseteq)$, então $(Fc_f(\mathcal{P}(A)), \subseteq)$ é um reticulado algébrico e os elementos compactos de $(Fc_f(\mathcal{P}(A)), \subseteq)$ são os conjuntos fechados $f(X)$, onde X é um subconjunto finito de A.*

Demonstração. Comecemos por mostrar que se X é um subconjunto finito de A, então $f(X)$ é compacto. Seja $X = \{a_1, \ldots, a_k\}$ e admitamos que

$$f(X) \subseteq \bigvee_{i\in I} f(A_i) = f\left(\bigcup_{i\in I} A_i\right).$$

Atendendo a que $X \subseteq f(X)$ e uma vez que o operador de fecho f é algébrico, segue que, para cada $a_j \in X$, existe um conjunto finito $X_j \subseteq \bigcup_{i\in I} A_i$ tal que $a_j \in f(X_j)$. Então, uma vez que existe um número finito de conjuntos A_i, digamos $A_{j1}, \ldots, A_{jn_j}$, tais que

$$X_j \subseteq A_{j1} \cup \ldots \cup A_{jn_j},$$

tem-se

$$a_j \in f(A_{j1} \cup \ldots \cup A_{jn_j}).$$

Assim,

$$X \subseteq \bigcup_{1 \leq j \leq k} f\left(A_{j1} \cup \ldots \cup A_{jn_j}\right),$$

pelo que

$$X \subseteq f\left(\bigcup_{\substack{1 \leq j \leq k, \\ 1 \leq i \leq n_j}} A_{ji}\right)$$

e, portanto,

$$f(X) \subseteq f\left(\bigcup_{\substack{1 \leq j \leq k, \\ 1 \leq i \leq n_j}} A_{ji}\right) = \bigvee_{\substack{1 \leq j \leq k, \\ 1 \leq i \leq n_j}} f\left(A_{ji}\right).$$

Logo, $f(X)$ é compacto.

Além disso, prova-se que os elementos $f(X)$, onde X é um subconjunto finito de A, são os únicos elementos compactos de $(Fc_f(\mathcal{P}(A)), \subseteq)$. De facto, admitindo que $f(Y)$ é diferente de $f(X)$ para todo o subconjunto finito X de A, e atendendo a que

$$f(Y) \subseteq \bigcup \{f(X) : X \subseteq Y \text{ e } X \text{ é finito}\},$$

é simples concluir que $f(Y)$ não pode estar contido em qualquer união finita de conjuntos $f(X)$ e, portanto, $f(Y)$ não é compacto.
Assim, considerando o Teorema 2.0.21, tendo em conta que o operador de fecho f é algébrico e que, para todo $X \subseteq A$ tal que X é finito, $f(X)$ é compacto, concluímos que $(Fc_f(\mathcal{P}(A)), \subseteq)$ é um reticulado algébrico. □

Corolário 2.0.24. *Seja f um operador de fecho algébrico em $(\mathcal{P}(A), \subseteq)$, para algum conjunto A. Então os subconjuntos de A finitamente gerados são precisamente os elementos compactos de $(Fc_f(\mathcal{P}(A)), \subseteq)$.*

Teorema 2.0.25. *Todo o reticulado algébrico é isomorfo ao reticulado dos subconjuntos fechados de algum conjunto A com um operador de fecho algébrico.*

Demonstração. Sejam $(R, \leq)$ um reticulado algébrico e A o conjunto dos elementos compactos de $(R, \leq)$. Considere-se a correspondência $f : \mathcal{P}(A) \to \mathcal{P}(A)$ tal que, para cada $X \subseteq A$,

$$f(X) = \{a \in A : a \leq \sup X\}.$$

Então f é um operador de fecho em $(\mathcal{P}(A), \subseteq)$ e da definição de elemento compacto resulta que f é algébrico. Atendendo a que $(R, \leq)$ é compactamente gerado, a aplicação $a \mapsto \{b \in A : b \leq a\}$ é um isomorfismo entre $(R, \leq)$ e $(Fc_f(\mathcal{P}(A)), \subseteq)$. □

Reticulados distributivos e reticulados modulares

Nesta secção estudam-se classes de reticulados que satisfazem identidades adicionais que relacionam as duas operações do reticulado: os *reticulados distributivos* e os *reticulados modulares*

Definição 2.0.26. *Um reticulado $\mathcal{R} = (R; \wedge, \vee,)$ diz-se um* ***reticulado distributivo*** *se satisfaz uma das seguintes condições:*

D1: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, $\forall\, x, y, z \in R$,

D2: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $\forall\, x, y, z \in R$.

Exemplo 2.0.27. *Os reticulados seguintes são distributivos:*
(1) $(P; \wedge, \vee)$*, onde P representa o conjunto das proposições, $\wedge$ representa o conetivo conjunção e $\vee$ representa o conetivo disjunção.*

(2) $(\mathbb{N}; \text{m.d.c.}, \text{m.m.c.})$*, onde* m.d.c. *representa a operação máximo divisor comum em $\mathbb{N}$ e* m.m.c. *representa a operação mínimo múltiplo comum.*

(3) $(\mathcal{P}(A); \cap, \cup)$, onde A é um conjunto e $\cap$ e $\cup$ são, respetivamente, as operações de interseção e união.

As condições D1 e D2 referidas na definição anterior, designadas por ***leis distributivas***, são equivalentes.

Teorema 2.0.28. *Seja $\mathcal{R} = (R; \wedge, \vee)$ um reticulado. Então $\mathcal{R}$ satisfaz* D1 se e só se $\mathcal{R}$ satisfaz D2.

Demonstração. Admitamos que $\mathcal{R}$ satisfaz D1. Então

$$\begin{array}{rcll} x \vee (y \wedge z) & = & (x \vee (x \wedge z)) \vee (y \wedge z) & (\text{por R4}) \\ & = & x \vee ((x \wedge z) \vee (y \wedge z)) & (\text{por R2}) \\ & = & x \vee ((z \wedge x) \vee (z \wedge y)) & (\text{por R1}) \\ & = & x \vee (z \wedge (x \vee y)) & (\text{por D1}) \\ & = & x \vee ((x \vee y) \wedge z) & (\text{por R1}) \\ & = & (x \wedge (x \vee y)) \vee ((x \vee y) \wedge z) & (\text{por R4}) \\ & = & ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) & (\text{por R1}) \\ & = & (x \vee y) \wedge (x \vee z). & (\text{por D1}) \end{array}$$

A prova de que D2 implica D1 é análoga. □

Note-se que qualquer reticulado satisfaz as desigualdades

$$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z) \text{ e } x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z).$$

Assim, para mostrar que um determinado reticulado é distributivo basta verificar uma das desigualdades

$$x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z) \text{ ou } (x \vee y) \wedge (x \vee z) \leq x \vee (y \wedge z).$$

Definição 2.0.29. *Um reticulado $\mathcal{R} = (R; \wedge, \vee)$ diz-se um* ***reticulado modular*** *se, para quaisquer $x, y, z \in R$,*

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

A condição da definição anterior, designada por ***lei modular***, é equivalente a

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

uma vez que $x \leq y$ se e só se $x = x \wedge y$. Também é simples verificar que todo o reticulado satisfaz a condição

$$x \leq y \Rightarrow x \vee (y \wedge z) \leq y \wedge (x \vee z),$$

pelo que, para mostrar que um reticulado é modular basta verificar que, para quaisquer $x, y, z \in R$,

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

Teorema 2.0.30. *Todo o reticulado distributivo é um reticulado modular.*

Demonstração. Basta considerar D2 e ter em atenção que $x \vee y = y$ se e só se $x \leq y$. □

Os dois próximos teoremas caracterizam os reticulados modulares e os reticulados distributivos e permitem identificar de uma forma mais eficiente estes reticulados. Tal caracterização é estabelecida recorrendo aos reticulados M_5 e N_5 a seguir apresentados

Figura 2.3

Observe-se que nenhum dos reticulados anteriores é distributivo, pois em nenhum dos casos se tem $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. No que respeita à modularidade, o reticulado M_5 é modular, mas no reticulado N_5 tem-se $a \leq b$ e $a \vee (b \wedge c) \neq b \wedge (a \vee c)$, pelo que N_5 não é modular.

Teorema 2.0.31. *Seja $\mathcal{R} = (R; \wedge, \vee)$ um reticulado. Então $\mathcal{R}$ é modular se e só se não tem qualquer subrreticulado isomorfo a N_5.*

Demonstração. Tendo em conta o que foi observado anteriormente, é imediato que se $\mathcal{R}$ tem um subrreticulado isomorfo a N_5, então $\mathcal{R}$ não é modular. Reciprocamente, se admitirmos que $\mathcal{R}$ não é modular, então existem $a, b, c \in R$ tais que $a \leq b$ e $a \vee (b \wedge c) < b \wedge (a \vee c)$. Sejam $a_1 = a \vee (b \wedge c)$ e $b_1 = b \wedge (a \vee c)$.

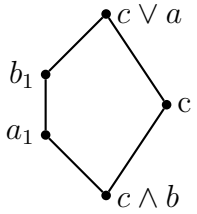
Então

$$\begin{aligned} c \wedge b_1 &= c \wedge (b \wedge (a \vee c)) \\ &= [c \wedge (c \vee a)] \wedge b \quad \text{(por R1 e R2)} \\ &= c \wedge b \quad \text{(por R4)} \end{aligned}$$

e

$$\begin{aligned} c \vee a_1 &= c \vee (a \vee (b \wedge c)) \\ &= [c \vee (b \wedge c)] \vee a \quad \text{(por R1 e R2)} \\ &= c \vee a \quad \text{(por R4).} \end{aligned}$$

Agora, atendendo a que $c \wedge b \leq a_1 \leq b_1$, temos $c \wedge b \leq c \wedge a_1 \leq c \wedge b_1 = c \wedge b$, donde $c \wedge a_1 = c \wedge b_1 = c \wedge b$. De modo análogo, tem-se $c \vee b_1 = c \vee a_1 = c \vee a$. Logo o reticulado a seguir apresentado



é um subrreticulado de $\mathcal{R}$ e é isomorfo a N_5. □

Teorema 2.0.32. *Seja $\mathcal{R} = (R; \wedge, \vee)$ um reticulado. Então $\mathcal{R}$ é distributivo se e só se não tem qualquer subrreticulado isomorfo a N_5 ou a M_5.*

Demonstração. Se $\mathcal{R}$ é um reticulado que tem um subrreticulado isomorfo a M_5 ou a N_5, então é imediato que $\mathcal{R}$ não é distributivo. Reciprocamente, se $\mathcal{R}$ é um reticulado não distributivo, prova-se que $\mathcal{R}$ tem um subrreticulado isomorfo a M_5 ou a N_5. De facto, se $\mathcal{R}$ não é modular, do teorema anterior segue que $\mathcal{R}$ tem um subrreticulado isomorfo a N_5. Caso $\mathcal{R}$ seja modular prova-se que $\mathcal{R}$ tem um subrreticulado isomorfo a M_5. Com efeito, se $\mathcal{R}$ não é distributivo, existem elementos $d, e, f \in R$ tais que $(d \wedge e) \vee (d \wedge f) < d \wedge (e \vee f)$. A partir destes elementos definem-se

$$\begin{aligned} p &= (d \wedge e) \vee (e \wedge f) \vee (f \wedge d), \\ q &= (d \vee e) \wedge (e \vee f) \wedge (f \vee d), \\ u &= (d \wedge q) \vee p, \\ v &= (e \wedge q) \vee p, \\ w &= (f \wedge q) \vee p. \end{aligned}$$

Claramente, $p \leq u$, $p \leq v$ e $p \leq w$. Também é imediato que $p \leq q$. Assim, $u \leq (d \wedge q) \vee q = q$. De forma análoga, tem-se $v \leq q$ e $w \leq q$. Atendendo às leis associativa, comutativa e de absorção, segue que

$$d \wedge q = d \wedge (e \vee f)$$

e

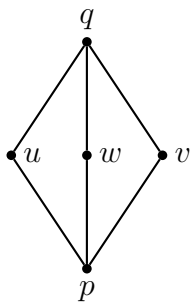
$$\begin{aligned} d \wedge p &= d \wedge ((d \wedge e) \vee (e \wedge f) \vee (f \wedge d)) \\ &= (d \wedge (e \wedge f)) \vee ((d \wedge e) \vee (f \wedge d)) \\ &= (d \wedge e) \vee (f \wedge d). \end{aligned}$$

Logo $p = q$ é impossível. Por conseguinte $p < q$.

Seguidamente, prova-se que $u \wedge v = p$. De facto,

$$\begin{array}{rcll}
u \wedge v & = & ((d \wedge q) \vee p) \wedge ((e \wedge q) \vee p) & \\
& = & (((e \wedge q) \vee p) \wedge (d \wedge q)) \vee p & \text{(R1 e lei modular)} \\
& = & (((q \wedge (e \vee p)) \wedge (d \wedge q)) \vee p & \text{(R1 e lei modular)} \\
& = & ((e \vee p) \wedge (d \wedge q)) \vee p & \text{(por R1, R2 e R3)} \\
& = & ((d \wedge (e \vee f)) \wedge (e \vee (f \wedge d))) \vee p & \text{(por R1 e R4)} \\
& = & (d \wedge ((e \vee f) \wedge (e \vee (f \wedge d)))) \vee p & \text{(por R3)} \\
& = & (d \wedge (((e \vee f) \wedge (f \wedge d)) \vee e)) \vee p & \text{(lei modular)} \\
& = & (d \wedge ((f \wedge d) \vee e)) \vee p & \text{(pois } f \wedge d \leq f \leq e \vee f\text{)} \\
& = & ((d \wedge e) \vee (f \wedge d)) \vee p & \text{(lei modular)} \\
& = & p &
\end{array}$$

De forma análoga mostra-se que $v \wedge w = p$ e $w \wedge u = p$. Argumentos semelhantes permitem mostrar que $u \vee v = q$, $v \vee w = q$ e $w \vee u = q$.
Finalmente, é simples verificar que se dois dos elementos u, v, w, p, q são iguais, então $p = q$, o que é impossível.
Logo, o reticulado



□

é um subrreticulado de $\mathcal{R}$ isomorfo a M_5.

3. Elementos de álgebra Universal

O desenvolvimento do estudo na área da matemática levou ao aparecimento de diversas estruturas algébricas, tais como grupos, anéis, reticulados, álgebras de Boole, etc. Tais estruturas, embora distintas, têm propriedades análogas, o que levou ao surgir de uma área da matemática, a Álgebra Universal, que tem por objetivo o estudo de propriedades que são comuns a estas estruturas.

3.1 Álgebras

Um dos conceitos básicos em álgebra universal, suficientemente abrangente para englobar muitas das estruturas algébricas que nos são familiares, é a noção de álgebra, a qual é definida como um conjunto não vazio equipado com uma família de operações.

No sentido de formalizar o conceito de álgebra, começamos por considerar a noção de *tipo algébrico*.

Definição 3.1.1. *Dá-se a designação de* ***tipo algébrico****, ou simplesmente* ***tipo****, a um par* (O, τ)*, onde* O *é um conjunto e* τ *é uma função de* O *em* $\mathbb{N}_0$*. Cada elemento* f *de* O *é designado por* ***símbolo de operação*** *e* $\tau(f)$ *diz-se a sua* ***aridade****. O conjunto de todos os símbolos de* O *de aridade* n*,* $n \in \mathbb{N}_0$*, é representado por* O_n*.*

Definição 3.1.2. *Chama-se* ***álgebra*** *a um par* $\mathcal{A} = (A; F)$ *onde* A *é um conjunto não vazio e* F *é uma família* $(f^{\mathcal{A}})_{f \in O}$ *de operações finitárias em* A *indexada por um conjunto* O*. Ao conjunto* A *dá-se a designação de* ***universo*** *ou* ***conjunto suporte de*** $\mathcal{A}$*, cada operação* $f^{\mathcal{A}}$ *é designada por* ***operação fundamental de*** $\mathcal{A}$ *ou* ***operação básica*** *de* $\mathcal{A}$ *e ao conjunto* O *dá-se a designação de* ***conjunto de símbolos operacionais de*** $\mathcal{A}$*.*
Uma álgebra $\mathcal{A}$ *diz-se uma* ***álgebra de tipo*** (O, τ) *se* O *é o conjunto de símbolos operacionais de* $\mathcal{A}$ *e* τ *é a função de* O *em* $\mathbb{N}_0$ *que a cada símbolo operacional* $f \in O$ *associa a aridade* n_f *da operação básica* $f^{\mathcal{A}}$*.*

Ao longo do texto as álgebras são representadas por letras maiúsculas caligráficas, eventualmente com índices, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, ..., $\mathcal{A}_1$, $\mathcal{A}_2$, ..., e o conjunto suporte das álgebras é representado pelas letras maiúsculas respetivas, A, B, C, ..., A_1, A_2, ...

Uma álgebra $\mathcal{A} = (A; F)$ diz-se ***trivial*** se $|A| = 1$ e diz-se ***finita*** ou ***infinita*** caso o seu conjunto suporte A seja finito ou infinito, respetivamente.

Note-se que na definição de álgebra é importante fazer a distinção entre símbolos operacionais e operações, uma vez que em diferentes álgebras o mesmo símbolo operacional pode estar associado a operações distintas. Assim, dada uma álgebra $\mathcal{A} = (A; (f^{\mathcal{A}})_{f\in O})$, usa-se a notação $f^{\mathcal{A}}$ para representar a operação fundamental de $\mathcal{A}$ indexada por f; à operação $f^{\mathcal{A}}$ dá-se a designação de ***interpretação de*** f ***em*** $\mathcal{A}$. Caso o contexto seja claro pode escrever-se apenas f em vez de $f^{\mathcal{A}}$.
A indexação das operações básicas de uma álgebra $\mathcal{A}$ com o conjunto de símbolos operacionais O permite ter uma sequência ordenada das operações básicas da álgebra, associando a cada símbolo operacional em O uma operação finitária em A. Esta indexação tem a vantagem de permitir diferenciar operações que tenham a mesma aridade. O conjunto de símbolos operacionais O de uma álgebra $\mathcal{A}$ pode ser finito ou infinito. Caso O seja finito e não vazio, digamos $O = \{f_1, f_2, \ldots, f_k\}$, é usual escrever $\mathcal{A} = (A; {f_1}^{\mathcal{A}}, {f_2}^{\mathcal{A}}, \ldots, {f_k}^{\mathcal{A}})$ ou apenas $\mathcal{A} = (A; f_1, f_2, \ldots, f_k)$ e representa-se o tipo de $\mathcal{A}$ por $(O, n_{f_1}, n_{f_2}, \ldots, n_{f_k})$ ou por $(n_{f_1}, n_{f_2}, \ldots, n_{f_k})$, onde n_{f_i}, $i \in \{1, \ldots, k\}$, representa a aridade da operação ${f_i}^{\mathcal{A}}$.
Uma álgebra $\mathcal{A}$ diz-se ***unária*** se $\mathcal{A}$ é uma álgebra de tipo (O, τ) onde $\tau(f) = 1$, para todo $f \in O$, ou seja, $\mathcal{A}$ é uma álgebra em que todas as operações fundamentais são unárias. A uma álgebra $\mathcal{A}$ com uma única operação binária, ou seja, a uma álgebra de tipo $(\{f\}, \tau)$ onde $\tau(f) = 2$, dá-se a designação de ***grupóide***.

Definição 3.1.3. *Sejam $\mathcal{A}$ e $\mathcal{B}$ álgebras de tipos (O_1, τ_1) e (O_2, τ_2), respetivamente. Diz-se que a álgebra $\mathcal{B}$ é um* **reduto** *da álgebra $\mathcal{A}$ se: $\mathcal{A}$ e $\mathcal{B}$ têm o mesmo universo, $O_2 \subseteq O_1$ e, para todo $f \in O_2$, $\tau_1(f) = \tau_2(f)$ e $f^{\mathcal{A}} = f^{\mathcal{B}}$.*

Terminamos esta secção com a apresentação de alguns exemplos de álgebras.

(i) Para qualquer conjunto não vazio A, $\mathcal{A} = (A; \emptyset)$ é uma álgebra.

(ii) Um ***semigrupo*** é um grupóide $\mathcal{S} = (S; \cdot)$ tal que, para quaisquer $x, y, z \in S$,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z, \tag{1.1}$$

ou seja, um semigrupo é uma álgebra definida por um conjunto não vazio munido de uma operação binária associativa.

(iii) Um ***monóide*** é um semigrupo $(M; \cdot)$ com um elemento $1 \in M$ tal que, para todo $x \in M$,

$$x \cdot 1 = x = 1 \cdot x. \tag{1.2}$$

A um elemento 1 que satisfaça as condições anteriores dá-se a designação de *elemento neutro* ou *identidade* e é simples verificar que num dado semigrupo não existe mais do que um elemento destes. Assim, o elemento neutro pode ser interpretado como uma função constante e um monóide pode ser definido como uma álgebra $\mathcal{M} = (M; \cdot, 1)$ de tipo $(2, 0)$ que satisfaz as condições (1.1) e (1.2).

(iv) Um ***grupo*** pode ser descrito como um tipo especial de semigrupo, ou seja, como uma álgebra $(G;\cdot)$ de tipo (2) que satisfaz as identidades (1.1), (1.2) e tal que, para cada $x \in G$, existe $x^{-1} \in G$ que satisfaz as condições seguintes

$$x \cdot x^{-1} = 1 = x^{-1} \cdot x. \tag{1.3}$$

Atendendo a que um grupo é um monóide, um grupo pode também ser definido como uma álgebra $(G;\cdot,1)$ de tipo $(2,0)$ que satisfaz as condições (1.1), (1.2) e (1.3).
Num grupo $(G;\cdot)$, para cada $x \in G$, existe um único elemento $x^{-1} \in G$ que satisfaz (1.3), pelo que faz sentido considerar uma operação unária que a cada elemento $x \in G$ associa o elemento x^{-1}. Por conseguinte, um grupo pode ser descrito como uma álgebra $\mathcal{G} = (G;\cdot,^{-1},1)$ de tipo $(2,1,0)$ que satisfaz (1.1), (1.2) e (1.3).
Um **grupo abeliano** é um grupo $\mathcal{G} = (G;\cdot,^{-1},1)$ tal que, para quaisquer $x, y \in G$,

$$x \cdot y = y \cdot x. \tag{1.4}$$

(v) Um ***anel*** é uma álgebra $\mathcal{A} = (A;+,\cdot,-,0)$ de tipo $(2,2,1,0)$ tal que $(A;+,-,0)$ é um grupo abeliano, $(A;\cdot)$ é um semigrupo e, para quaisquer $x, y, z \in A$,

$$x \cdot (y+z) = x \cdot y + x \cdot z \quad \text{e} \quad (y+z) \cdot x = y \cdot x + z \cdot x.$$

Um **anel com identidade** é uma álgebra $\mathcal{A} = (A;+,\cdot,-,0,1)$ de tipo $(2,2,1,0,0)$ tal que $(A;+,\cdot,-,0)$ é um anel e $(A;\cdot,1)$ é um monóide.

(vi) Um ***semirreticulado*** é um semigrupo comutativo $\mathcal{S} = (S;\cdot)$ tal que, para todo $x \in S$,

$$x \cdot x = x.$$

(vii) Um ***reticulado*** é uma álgebra $\mathcal{R} = (R;\wedge,\vee)$ de tipo $(2,2)$ tal que, para quaisquer $x, y, z \in R$,

R1:	$x \wedge y = y \wedge x$,	$x \vee y = y \vee x$	(leis comutativas);
R2:	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$,	$x \vee (y \vee z) = (x \vee y) \vee z$	(leis associativas);
R3:	$x \wedge x = x$,	$x \vee x = x$	(leis de idempotência);
R4:	$x \wedge (x \vee y) = x$,	$x \vee (x \wedge y) = x$	(leis de absorção).

(viii) Um ***reticulado limitado*** é uma álgebra $\mathcal{R} = (R;\wedge,\vee,0,1)$ de tipo $(2,2,0,0)$ tal que $(R;\wedge,\vee)$ é um reticulado e, para qualquer $x \in R$,

$$x \wedge 0 = 0 \quad \text{e} \quad x \vee 1 = 1.$$

(ix) Um ***reticulado distributivo*** é um reticulado $\mathcal{R} = (R;\wedge,\vee)$ tal que, para quaisquer $x, y, z \in R$,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \text{e} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

(x) Uma ***álgebra de Boole*** é uma álgebra $\mathcal{B} = (B;\wedge,\vee,',0,1)$ de tipo $(2,2,1,0,0)$ tal que $(B;\wedge,\vee)$ é um reticulado distributivo e, para todo $x \in B$,

$$x \wedge 0 = 0, \quad x \vee 1 = 1,$$

$$x \wedge x' = 0, \quad x \vee x' = 1.$$

3.2 Subálgebras

Em certos casos o estudo de uma álgebra pode ser simplificado recorrendo ao estudo de outras álgebras que estejam relacionadas com a álgebra dada. Por este motivo, é importante considerar processos que permitam construir novas álgebras a partir de uma determinada álgebra. Alguns desses processos de construção são abordados ao longo deste texto. Começamos por referir a formação de subálgebras.

Definição 3.2.1. *Sejam A um conjunto, $n \in \mathbb{N}_0$, f uma operação n-ária em A e $X \subseteq A$. Diz-se que o* ***conjunto X é fechado para a operação*** *f se*

$$f(a_1, \ldots, a_n) \in X, \text{ para todo } (a_1, \ldots, a_n) \in X^n.$$

Nas condições da definição anterior, se f é uma operação nulária, então o conjunto X é fechado para a operação f se e só se $f \in X$. Por conseguinte, se $X = \emptyset$, o conjunto X não é fechado para qualquer operação nulária. Note-se, no entanto, que $X = \emptyset$ é fechado para toda toda a operação n-ária sempre que $n \geq 1$.

Definição 3.2.2. *Sejam $\mathcal{A} = (A; F)$ uma álgebra. Um subconjunto B de A diz-se um* ***subuniverso*** *de $\mathcal{A}$ se B é fechado para toda a operação de F.*
Representa-se por $\mathrm{Sub}\mathcal{A}$ *o conjunto de todos os subuniversos de $\mathcal{A}$.*

Observe-se que o conjunto vazio é subuniverso de uma álgebra $\mathcal{A}$ se e só se $\mathcal{A}$ não tem operações nulárias.

Exemplo 3.2.3.
(1) Os conjuntos $\{0\}$, $\{2n \mid n \in \mathbb{Z}\}$ e $\mathbb{Z}$ são subuniversos do semigrupo $(\mathbb{Z}; +)$ e do anel $(\mathbb{Z}; +, \cdot, -, 0)$.
(2) O conjunto $\{2n+1 \mid n \in \mathbb{Z}\}$ não é subuniverso do semigrupo $(\mathbb{Z}; +)$ nem do anel $(\mathbb{Z}; +, \cdot, -, 0)$.
(3) O conjunto $\emptyset$ é um subuniverso do semigrupo $(\mathbb{Z}; +)$, mas não é subuniverso do anel $(\mathbb{Z}; +, \cdot, -, 0)$.

Teorema 3.2.4. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $(S_i \mid i \in I)$ uma família de subuniversos de $\mathcal{A}$. Então $\bigcap_{i \in I} S_i$ é um subuniverso de $\mathcal{A}$.*

Demonstração. Para cada $i \in I$, S_i é um subuniverso de $\mathcal{A}$, pelo que $S_i \subseteq A$. Assim, $\bigcap_{i \in I} S_i \subseteq A$. Além disso, para qualquer $n \in \mathbb{N}_0$, para qualquer f operação n-ária de $\mathcal{A}$ e para qualquer $(a_1, \ldots, a_n) \in (\bigcap_{i \in I} S_i)^n$, tem-se $f(a_1, \ldots, a_n) \in S_i$, para cada $i \in I$, uma vez que $(a_1, \ldots, a_n) \in (S_i)^n$ e cada um dos conjuntos S_i é um subuniverso de $\mathcal{A}$. Então $f(a_1, \ldots, a_n) \in \bigcap_{i \in I} S_i$ e, portanto, $\bigcap_{i \in I} S_i$ é fechado para a operação f. □

Teorema 3.2.5. *Sejam $\mathcal{A} = (A; F)$ uma álgebra, $X \subseteq A$ e*

$$S = \bigcap \{B \mid B \text{ é subuniverso de } \mathcal{A} \text{ e } X \subseteq B\}.$$

Então S é um subuniverso de $\mathcal{A}$ e é o menor subuniverso de $\mathcal{A}$ que contém X.

Demonstração. Do Teorema 3.2.4 segue que S é um subniverso de $\mathcal{A}$ e da definição de S é imediato que $X \subseteq S$ e que S está contido em qualquer subuniverso de $\mathcal{A}$ que contenha X. □

Definição 3.2.6. *Sejam $\mathcal{A} = (A; F)$ uma álgebra, $X \subseteq A$ e S um subuniverso de $\mathcal{A}$. Designa-se por **subuniverso de $\mathcal{A}$ gerado por** X, e representa-se por $Sg^{\mathcal{A}}(X)$, o menor subuniverso de $\mathcal{A}$ que contém X, i.e., o conjunto*

$$Sg^{\mathcal{A}}(X) = \bigcap \{B \mid B \text{ é subuniverso de } \mathcal{A} \text{ e } X \subseteq B\}.$$

*Diz-se que S é **finitamente gerado** se $S = Sg^{\mathcal{A}}(X)$, para algum conjunto finito $X \subseteq A$.*

Teorema 3.2.7. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $X \subseteq A$. Para $i \in \mathbb{N}_0$, define-se*

$$\begin{array}{lcl} X_0 & = & X; \\ X_{i+1} & = & X_i \cup \{f(x) \mid f \text{ é operação } n\text{-ária em } \mathcal{A} \text{ e } x \in (X_i)^n, n \in \mathbb{N}_0\}. \end{array}$$

Então $Sg^{\mathcal{A}}(X) = \bigcup_{i \in \mathbb{N}_0} X_i$.

Demonstração. É imediato que $X \subseteq \bigcup_{i \in \mathbb{N}_0} X_i \subseteq A$. Facilmente também se verifica que $\bigcup_{i \in \mathbb{N}_0} X_i$ é fechado para toda a operação de $\mathcal{A}$: se f é uma operação n-ária em $\mathcal{A}$ e $a_1, \ldots, a_n$ são elementos de $\bigcup_{i \in \mathbb{N}_0} X_i$, então $(a_1, \ldots, a_n) \in (X_k)^n$, para algum $k \in \mathbb{N}_0$, donde $f(a_1, \ldots, a_n) \in X_{k+1} \subseteq \bigcup_{i \in \mathbb{N}_0} X_i$. Logo $\bigcup_{i \in \mathbb{N}_0} X_i$ é um subuniverso de $\mathcal{A}$ e contém X. Além disso, $\bigcup_{i \in \mathbb{N}_0} X_i$ é o menor subuniverso de $\mathcal{A}$ que contém X. De facto, se B é um subuniverso de $\mathcal{A}$ que contém X, mostra-se, por indução em i, que $X_i \subseteq B$, para todo $i \in \mathbb{N}_0$, e, portanto, $\bigcup_{i \in \mathbb{N}_0} X_i \subseteq B$. Assim, $Sg^{\mathcal{A}}(X) = \bigcup_{i \in \mathbb{N}_0} X_i$. □

Corolário 3.2.8. *Sejam $\mathcal{A}$ uma álgebra, $X \subseteq A$ e $a \in Sg^{\mathcal{A}}(X)$. Então $a \in Sg^{\mathcal{A}}(Y)$, para algum subconjunto finito Y de X.*

Demonstração. Do teorema anterior sabe-se que $Sg^{\mathcal{A}}(X) = \bigcup_{i \in \mathbb{N}_0} X_i$, onde X_i são os conjuntos descritos nesse mesmo teorema. Por indução em i, prova-se que se $a \in X_i$, então $a \in Sg^{\mathcal{A}}(Y)$, para algum subconjunto finito Y de X. □

Corolário 3.2.9. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $X, Y \subseteq A$. Então*

(i) $X \subseteq Sg^{\mathcal{A}}(X)$.

(ii) $X \subseteq Y \Rightarrow Sg^{\mathcal{A}}(X) \subseteq Sg^{\mathcal{A}}(Y)$.

(iii) $Sg^{\mathcal{A}}(Sg^{\mathcal{A}}(X)) = Sg^{\mathcal{A}}(X)$.

(iv) $Sg^{\mathcal{A}}(X) = \bigcup \{Sg^{\mathcal{A}}(Z) \mid Z \text{ é subconjunto finito de } X\}$. □

Corolário 3.2.10. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $Sg^{\mathcal{A}} : \mathcal{P}(A) \to \mathcal{P}(A)$ a aplicação definida por $X \mapsto Sg^{\mathcal{A}}(X)$, para todo $X \in \mathcal{P}(A)$. Então $Sg^{\mathcal{A}}$ é um operador de fecho algébrico em $(\mathcal{P}(A), \subseteq)$.*

Observe-se que os subuniversos de uma álgebra $\mathcal{A}$ são exatamente os subconjuntos X de A para os quais se tem $X = Sg^{\mathcal{A}}(X)$, ou seja, são os subconjuntos de A fechados para o operador de fecho $Sg^{\mathcal{A}}$.

Teorema 3.2.11. *Seja $\mathcal{A}$ uma álgebra. Então* $(\mathrm{Sub}\mathcal{A}, \subseteq)$ *é um reticulado algébrico e, para quaisquer $B, C \in \mathrm{Sub}\mathcal{A}$,*

$$B \wedge C = B \cap C, \;\; B \vee C = Sg^{\mathcal{A}}(B \cup C), \;\; \forall B, C \in \mathrm{Sub}\mathcal{A}.$$

Demonstração. A prova de

$$B \wedge C = B \cap C, \;\; B \vee C = Sg^{\mathcal{A}}(B \cup C), \;\; \forall B, C \in \mathrm{Sub}\mathcal{A}$$

é um exercício simples e do que foi observado anteriormente segue que

$$(Fc_{Sg^{\mathcal{A}}}, \subseteq) = (\mathrm{Sub}\mathcal{A}, \subseteq).$$

Logo o resultado é imediato atendendo ao Teorema 2.0.23. □

Definição 3.2.12. *Sejam $\mathcal{A}$ uma álgebra e* $\mathrm{Sub}\mathcal{A}$ *o conjunto dos subuniversos de $\mathcal{A}$. O reticulado* $(\mathrm{Sub}\mathcal{A}, \subseteq)$ *designa-se por* ***reticulado dos subuniversos de*** *$\mathcal{A}$ e representa-se por $\mathcal{S}ub\mathcal{A}$.*

Definição 3.2.13. *Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo (O, τ). Diz-se que $\mathcal{B}$ é uma* ***subálgebra*** *de $\mathcal{A}$, e escreve-se $\mathcal{B} \leq \mathcal{A}$, se B é um subuniverso de $\mathcal{A}$ e, para todo $n \in \mathbb{N}_0$ e para todo o simbolo de operação $f \in O_n$,*

$$f^{\mathcal{A}}(b_1, \ldots, b_n) = f^{\mathcal{B}}(b_1, \ldots, b_n),$$

para qualquer $(b_1, \ldots, b_n) \in B^n$.

Se $\mathcal{B} = (B; G)$ é subálgebra de uma álgebra $\mathcal{A} = (A; F)$, então B é um subuniverso de $\mathcal{A}$. No entanto, um subuniverso de $\mathcal{A}$ não é necessariamente o universo de uma subálgebra de $\mathcal{A}$. Observe-se, por exemplo, que o conjunto vazio pode ser subuniverso de uma álgebra $\mathcal{A}$, mas não é universo de qualquer subálgebra de $\mathcal{A}$.

Exemplo 3.2.14.
(1) O anel $(\mathbb{R}; +, \cdot, -, 0)$ é uma subálgebra do anel $(\mathbb{C}; +, \cdot, -, 0)$.
(2) Se $(G; \cdot)$ é um grupo, as suas subálgebras são os subsemigrupos de G.
(3) Se $(G; \cdot, ^{-1}, 1)$ é um grupo, as suas subálgebras são os subgrupos de G.

Definição 3.2.15. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $X \subseteq A$ tal que $X \neq \emptyset$. Chama-se* ***subálgebra de $\mathcal{A}$ gerada por*** *X, e representa-se por $\mathcal{S}g^{\mathcal{A}}(X)$, a subálgebra de $\mathcal{A}$ cujo universo é $Sg^{\mathcal{A}}(X)$.*
Se na álgebra $\mathcal{A}$ há, pelo menos, uma operação nulária, define-se a ***subálgebra de $\mathcal{A}$ gerada por*** $\emptyset$ *como sendo a subálgebra de $\mathcal{A}$ cujo universo é $Sg^{\mathcal{A}}(\emptyset)$.*
Diz-se que a álgebra $\mathcal{A}$ ***é gerada por*** *X ou que X* ***é um conjunto de geradores de $\mathcal{A}$*** *se $\mathcal{S}g^{\mathcal{A}}(X) = \mathcal{A}$. A álgebra $\mathcal{A}$ diz-se* ***finitamente gerada*** *se $\mathcal{A}$ admite um conjunto de geradores finito.*

Exemplo 3.2.16. *O anel $\mathcal{Z} = (\mathbb{Z}; +, \cdot, -, 0)$ é finitamente gerado: $\mathcal{S}g^{\mathcal{Z}}(\{1\}) = \mathcal{Z}$.*

3.3 Congruências e álgebras quociente

Uma congruência numa álgebra é uma relação de equivalência que é compatível com as operações da álgebra. A noção de congruência desempenha um papel relevante no estudo de álgebra universal.

Definição 3.3.1. *Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo (O, τ) e θ uma relação de equivalência em A. Diz-se que θ* ***é uma congruência*** *em $\mathcal{A}$ se θ satisfaz a* ***propriedade de substituição****, i.e., se, para quaisquer $n \in \mathbb{N}_0$, $f \in O_n$ e $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in A^n$,*

$$(a_i \,\theta\, b_i, \forall i \in \{1, \ldots, n\}) \Rightarrow f^{\mathcal{A}}(a_1, \ldots, a_n) \,\theta\, f^{\mathcal{A}}(b_1, \ldots, b_n).$$

Exemplo 3.3.2.
(1) Considere o anel $(\mathbb{Z}; +, \cdot, -, 0)$. Para cada $q \in \mathbb{Z}$, seja $\equiv_q$ a relação de equivalência definida em $\mathbb{Z}$ por

$$r \equiv_q s \text{ sse } r - s = qk, \text{ para algum } k \in \mathbb{Z}.$$

Facilmente se verifica que: para todo $q \in \mathbb{Z}$, $\equiv_q$ é uma congruência no anel $(\mathbb{Z}; +, \cdot, -, 0)$; $\equiv_0$ é a congruência identidade; $\equiv_1$ é a congruência universal.

(2) Dado um grupo $\mathcal{G} = (G; \cdot, ^{-1}, 1)$, é possível estabelecer uma relação entre as congruências de $\mathcal{G}$ e os subgrupos invariantes de $\mathcal{G}$:

(a) se θ é uma congruência em $\mathcal{G}$, então $[1]_\theta$ é o universo de um subgrupo invariante de $\mathcal{G}$ e, dados $a, b \in G$, tem-se $a \,\theta\, b$ se e só se $a \cdot b^{-1} \in [1]_\theta$;

(b) se $\mathcal{N} = (N; \cdot, ^{-1}, 1)$ é um subgrupo invariante de $\mathcal{G}$, a relação binária θ definida em N por

$$a \,\theta\, b \text{ sse } a \cdot b^{-1} \in N$$

é uma congruência em $\mathcal{G}$ e tem-se $[1]_\theta = N$.

A aplicação $\theta \mapsto [1]_\theta$ é uma bijeção entre o conjunto das congruências de $\mathcal{G}$ e o conjunto dos subgrupos invariantes de $\mathcal{G}$.

(3) Sendo $\mathcal{A} = (A; +, \cdot, -, 0)$ um anel, também é possível relacionar as congruências e os ideais do anel:

(a) se θ é uma congruêcia em $\mathcal{A}$, então $[0]_\theta$ é o universo de um ideal de $\mathcal{A}$ e, dados $a, b \in A$, tem-se $a\,\theta\,b$ se e só se $a - b \in [0]_\theta$;

(b) se $\mathcal{I} = (I; \cdot, ^{-1}, 1)$ é um ideal de $\mathcal{A}$, a relação binária θ definida em I por

$$a\,\theta\,b \text{ sse } a - b \in I$$

é uma congruência em $\mathcal{A}$ e tem-se $[0]_\theta = I$.

A aplicação $\theta \mapsto [0]_\theta$ é uma bijeção entre o conjunto das congruências de $\mathcal{A}$ e o conjunto dos ideais de $\mathcal{A}$.

(4) Se $\mathcal{R} = (R; \wedge, \vee)$ é um reticulado, então $\theta \in \mathrm{Eq}(R)$ é uma congruência em $\mathcal{R}$ se e só se:

(a) cada classe de θ é um subrreticulado de $\mathcal{R}$;

(b) cada classe de θ é um subconjunto convexo de R;

(c) as classes de equivalência de θ são fechadas para quadriláteros (i.e. sempre que a, b, c, d são elementos de R distintos tais que $a < b$, $c < d$ e

$$(a \vee d = b \text{ e } a \wedge d = c) \text{ ou } (b \vee c = d \text{ e } b \wedge c = a),$$

então $a\,\theta\,b$ sse $c\,\theta\,d$).

(5) Seja $\mathcal{R} = (R; \wedge, \vee)$ um reticulado que é uma cadeia (enquanto c.p.o.) e seja $\theta \in \mathrm{Eq}(R)$. Então θ é uma congruência em $\mathcal{R}$ se e só se as suas classes de equivalência são conjuntos convexos.

O conjunto de todas as congruências de uma álgebra $\mathcal{A}$ é denotado por $\mathrm{Con}\,\mathcal{A}$. A relação identidade $\triangle_A = \{(a, a) \in A^2 \mid a \in A\}$ e a relação universal $\nabla_A = A^2$ são elementos de $\mathrm{Con}\mathcal{A}$. O conjunto de congruências de uma álgebra, quando ordenado pela relação de inclusão de conjuntos, define um reticulado.

Lema 3.3.3. *Sejam $\mathcal{A}$ uma álgebra. Se θ_1, θ_2 são congruências em $\mathcal{A}$, então:*

(1) $\theta_1 \cap \theta_2 \in \mathrm{Con}\mathcal{A}$.

(2) $\{(x, y) \in A^2 \mid \exists\, n \in \mathbb{N}, \exists\, z_0, z_1, \ldots, z_n \in A : x = z_0, y = z_n$
$e\ \forall 1 \leq k \leq n, z_{k-1}\,\theta_1\,z_k \text{ ou } z_{k-1}\,\theta_2\,z_k\} \in \mathrm{Con}\mathcal{A}$. □

Teorema 3.3.4. *Sejam $\mathcal{A}$ uma álgebra. Então $(\mathrm{Con}\mathcal{A}, \subseteq)$ é um reticulado, tendo-se, para quaisquer $\theta_1, \theta_2 \in \mathrm{Con}\mathcal{A}$,*

$$\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2,$$

$$\theta_1 \vee \theta_2 = \{(x,y) \in A^2 \mid \exists\, n \in \mathbb{N}, \exists\, z_0, z_1, \ldots, z_n \in A : x = z_0, y = z_n \\ e\ \forall 1 \leq k \leq n, z_{k-1}\,\theta_1\, z_k \text{ ou } z_{k-1}\,\theta_2\, z_k\}.$$

Demonstração. Imediato a partir do Teorema 1.4.1 e do Lema 3.3.3. □

Definição 3.3.5. *Sejam $\mathcal{A}$ uma álgebra. Ao reticulado $\mathcal{C}on\mathcal{A} = (\mathrm{Con}\mathcal{A}, \subseteq)$ dá-se a designação de* ***reticulado das congruências de*** *$\mathcal{A}$.*

O resultado estabelecido na alínea (1) do Lema 3.3.3 pode ser generalizado.

Lema 3.3.6. *Sejam $\mathcal{A}$ uma álgebra e $(\theta_i)_{i\in I}$ uma família de congruências em $\mathcal{A}$. Então $\bigcap_{i\in I}\theta_i$ é uma congruência em $\mathcal{A}$.* □

Como consequência do lema anterior, pode estabelecer-se o seguinte.

Teorema 3.3.7. *Seja $\mathcal{A}$ uma álgebra. Então $\mathcal{C}on\mathcal{A}$ é um reticulado completo, tendo-se, para cada família $(\theta_i)_{i\in I}$ de congruências em $\mathcal{A}$,*

$$\bigwedge_{i\in I}\theta_i = \bigcap_{i\in I}\theta_i \quad e \quad \bigvee_{i\in I}\theta_i = \bigcap\{\theta \in \mathrm{Con}\mathcal{A} \mid \bigcup_{i\in I}\theta_i \subseteq \theta\}.$$ □

Teorema 3.3.8. *Para qualquer álgebra $\mathcal{A} = (A; F)$ de tipo (O, τ), existe um operador de fecho algébrico em $A \times A$ tal que os subconjuntos fechados de $A \times A$ são precisamente as congruências de $\mathcal{A}$. Assim, $\mathcal{C}on\mathcal{A}$ é um reticulado algébrico.*

Demonstração. Consideremos a álgebra

$$\mathcal{B} = (A \times A; \{f^{\mathcal{B}}\}_{f\in O} \cup \{c_a : a \in A\} \cup \{s^{\mathcal{B}}, t^{\mathcal{B}}\}),$$

onde

- para cada $f \in O_n$, $f^{\mathcal{B}} : (A \times A)^n \to A \times A$ é a aplicação definida por

$$f^{\mathcal{B}}((a_1,b_1),(a_2,b_2),\ldots,(a_n,b_n)) = (f^{\mathcal{A}}(a_1,a_2,\ldots,a_n), f^{\mathcal{A}}(b_1,b_2,\ldots,b_n));$$

- para cada $a \in A$, $c_a : (A \times A)^0 \to A \times A$ é a operação nulária definida por

$$c_a = (a,a);$$

- $s^{\mathcal{B}} : A \times A \to A \times A$ é a operação unária definida por

$$s^{\mathcal{B}}((a,b)) = (b,a);$$

- $t^{\mathcal{B}} : (A \times A)^2 \to A \times A$ é a operação binária definida por

$$s((a,b),(c,d)) = \begin{cases} (a,d) & \text{se } b = c \\ (a,b) & \text{se } b \neq c \end{cases}$$

Relativamente a esta álgebra verifica-se o seguinte: um subconjunto S de $A \times A$ é um subuniverso de $\mathcal{B}$ se e só se S é uma congruência em $\mathcal{B}$. Além disso, do Corolário 3.2.10 sabe-se que a aplicação $Sg^{\mathcal{B}}(\,) : \mathcal{P}(A \times A) \to \mathcal{P}(A \times A)$ definida por $S \mapsto Sg^{\mathcal{B}}(S)$ é um operador de fecho algébrico e que $(Fc_{Sg^{\mathcal{B}}(\,)}, \subseteq)$ é o reticulado algébrico dos subuniversos de $\mathcal{B}$. Assim, do que foi observado anteriormente e do Teorema 2.0.23 segue que $(\mathrm{Con}\mathcal{A}, \subseteq)$ é um reticulado algébrico. □

Dada uma álgebra $\mathcal{A} = (A; F)$ e dado $X \subseteq A \times A$, existe pelo menos uma congruência em $\mathcal{A}$ que contém X, mais precisamente, a congruência universal ∇_A. Assim, a família de congruências $(\theta \in \mathrm{Con}\mathcal{A} \,|\, X \subseteq \theta)$ é não vazia. Recorrendo a esta família constroi-se a menor congruência em $\mathcal{A}$ que contém X.

Teorema 3.3.9. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $X \subseteq A \times A$. Então*

$$\bigcap \{\theta \in \mathrm{Con}\mathcal{A} \,|\, X \subseteq \theta\}$$

é a menor congruência em $\mathcal{A}$ que contém X. □

Definição 3.3.10. *Sejam $\mathcal{A} = (A; F)$ uma álgebra, $X \subseteq A \times A$ e $a, b \in A$. Designa-se por **congruência gerada por** X **em** $\mathcal{A}$, e representa-se por $\Theta(X)$, a congruência*

$$\Theta(X) = \bigcap \{\theta \in \mathrm{Con}\mathcal{A} \,|\, X \subseteq \theta\}.$$

*Se $X = \{(a_i, a_j) \in A \times A \,|\, 1 \leq i, j \leq n\}$, representa-se $\Theta(X)$ por $\Theta(a_1, \ldots, a_n)$. Em particular, se $X = \{(a, b)\}$, designa-se por **congruência principal gerada por** a, b **em** $\mathcal{A}$, e representa-se por $\Theta(a, b)$, a congruência $\bigcap \{\theta \in \mathrm{Con}\mathcal{A} \,|\, a\, \theta\, b\}$.*

Dada uma álgebra $\mathcal{A} = (A; F)$, os elementos compactos do reticulado $\mathcal{C}on\mathcal{A}$ são as congruências finitamente geradas $\Theta((a_1, b_1), \ldots, (a_n, b_n))$.

Alguns factos úteis a respeito de congruências são estabelecidos no resultado seguinte.

Teorema 3.3.11. *Sejam $\mathcal{A}$ uma álgebra, $a_1, b_1, \ldots, a_n, b_n \in A$ e $\theta \in \mathrm{Con}\mathcal{A}$. Então*

(a) $\Theta(a_1, b_1) = \Theta(b_1, a_1)$.

(b) $\Theta((a_1, b_1), \ldots (a_n, b_n)) = \Theta(a_1, b_1) \vee \ldots \vee \Theta(a_n, b_n)$.

(c) $\Theta(a_1, \ldots, a_n) = \Theta(a_1, a_2) \vee \Theta(a_2, a_3) \vee \ldots \vee \Theta(a_{n-1}, a_n)$.

(d) $\theta = \bigcup \{\Theta(a, b) \,|\, (a, b) \in \theta\} = \bigvee \{\Theta(a, b) \,|\, (a, b) \in \theta\}$.

(e) $\theta = \bigcup \{\Theta((a_1, b_1), \ldots, (a_n, b_n)) \,|\, (a_i, b_i) \in \theta, n \geq 1\}$.

Demonstração. (a) Uma vez que $(b_1, a_1) \in \Theta(a_1, b_1)$, então $\Theta(b_1, a_1) \subseteq \Theta(a_1, b_1)$. Por simetria, também se tem $\Theta(a_1, b_1) \subseteq \Theta(b_1, a_1)$. Logo $\Theta(a_1, b_1) = \Theta(b_1, a_1)$.

(b) Por um lado, tem-se $(a_i, b_i) \in \Theta((a_1, b_1), \ldots, (a_n, b_n))$, para todo $i \in \{1, \ldots, n\}$, pelo que

$$\Theta(a_1, b_1) \vee \ldots \vee \Theta(a_n, b_n) \subseteq \Theta((a_1, b_1), \ldots, (a_n, b_n)).$$

Por outro lado, para todo $i \in \{1, \ldots n\}$,

$$(a_i, b_i) \in \Theta(a_i, b_i) \subseteq \Theta(a_1, b_1) \vee \ldots \vee \Theta(a_n, b_n),$$

donde $\{(a_1, b_1), \ldots, (a_n, b_n)\} \subseteq \Theta(a_1, b_1) \vee \ldots \vee \Theta(a_n, b_n)$ e, portanto,

$$\Theta((a_1, b_1), \ldots, (a_n, b_n)) \subseteq \Theta(a_1, b_1) \vee \ldots \vee \Theta(a_n, b_n).$$

(c) Para todo $i \in \{1, \ldots, n\}$, $\Theta(a_i, a_{i+1}) \subseteq \Theta(a_1, \ldots, a_n)$, donde

$$\Theta(a_1, a_2) \vee \ldots \vee \Theta(a_{n-1}, a_n) \subseteq \Theta(a_1, \ldots, a_n).$$

Reciprocamente, para $1 \leq i \leq j \leq n$, tem-se

$$(a_i, a_j) \in \Theta(a_i, a_{i+1}) \circ \ldots \circ \Theta(a_{j-1}, a_j),$$

donde, pelo Teorema 1.4.2, segue que

$$(a_i, a_j) \in \Theta(a_i, a_{i+1}) \vee \ldots \vee \Theta(a_{j-1}, a_j);$$

logo

$$(a_i, a_j) \in \Theta(a_1, a_2) \vee \ldots \vee \Theta(a_{n-1}, a_n).$$

Assim,

$$\Theta(a_1, \ldots, a_n) \subseteq \Theta(a_1, a_2) \vee \ldots \vee \Theta(a_{n-1}, a_n)$$

e, portanto,

$$\Theta(a_1, \ldots, a_n) = \Theta(a_1, a_2) \vee \ldots \vee \Theta(a_{n-1}, a_n).$$

(d) Para cada $(a, b) \in \theta$, tem-se

$$(a, b) \in \Theta(a, b) \subseteq \theta.$$

Logo,

$$\theta \subseteq \bigcup\{\Theta(a, b) \mid (a, b) \in \theta\} \subseteq \bigvee\{\Theta(a, b) \mid (a, b) \in \theta\} \subseteq \theta$$

e, portanto,

$$\theta = \bigcup\{\Theta(a, b) \mid (a, b) \in \theta\} = \bigvee\{\Theta(a, b) \mid (a, b) \in \theta\}.$$

□

Os reticulados de congruências de certas classes de álgebras satisfazem propriedades adicionais que se relacionam com as propriedades das respetivas álgebras.

Definição 3.3.12. *Sejam $\mathcal{A}$ uma álgebra e $\theta_1, \theta_2 \in \mathrm{Con}\mathcal{A}$. Diz-se que θ_1 e θ_2 são* ***permutáveis*** *se $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$. Diz-se que a álgebra $\mathcal{A}$ é:*

- ***congruente-permutável*** *se qualquer par de congruências em $\mathcal{A}$ é permutável;*
- ***congruente-distributiva*** *(**congruente-modular**) se $\mathcal{C}on\mathcal{A}$ é distributivo (modular).*

Uma classe $\mathbf{K}$ *de álgebras diz-se* ***congruente-permutavel***, ***congruente-distributiva***, ***congruente-modular*** *se cada álgebra da classe satisfaz a respetiva propriedade.*

Exemplo 3.3.13. *Todos os grupos e todos os anéis são congruente-permutáveis e todos os reticulados são congruente-distributivos.*

Nos resultados seguintes apresentam-se algumas propriedades a respeito de álgebras congruente-permutáveis.

Teorema 3.3.14. *Sejam $\mathcal{A}$ uma álgebra e $\theta_1, \theta_2 \in \mathrm{Con}\mathcal{A}$. Então as afirmações seguintes são equivalentes:*

(a) $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$,

(b) $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2$,

(c) $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1$.

Demonstração. (a) $\Rightarrow$ (b) Para quaisquer relações de equivalência θ e σ tem-se $\theta \circ \theta = \theta$ e $\theta \subseteq \theta \circ \sigma$. Então, admitindo que θ_1 e θ_2 são congruências de $\mathcal{A}$ tais que $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$ e tendo em atenção a observação que se segue ao Teorema 1.4.1, tem-se $\theta_1 \vee \theta_2 = \theta_1 \cup \theta_1 \circ \theta_2 = \theta_1 \circ \theta_2$.

(b) $\Rightarrow$ (c) Uma vez que $\theta_2 \circ \theta_1 \subseteq \theta_1 \vee \theta_2$, de (b) segue que $\theta_2 \circ \theta_1 \subseteq \theta_1 \circ \theta_2$. Então $(\theta_2 \circ \theta_1)^I \subseteq (\theta_1 \circ \theta_2)^I$, donde resulta ${\theta_1}^I \circ {\theta_2}^I \subseteq {\theta_2}^I \circ {\theta_1}^I$. Uma vez que, para cada relação de equivalência θ, se tem $\theta^I = \theta$, conclui-se que $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1$.

(c) $\Rightarrow$ (a) Suponhamos que $\theta_2 \circ \theta_1 \subseteq \theta_1 \circ \theta_2$. Então, considerando as respetivas relações inversas, temos $(\theta_2 \circ \theta_1)^I \subseteq (\theta_1 \circ \theta_2)^I$, donde ${\theta_1}^I \circ {\theta_2}^I \subseteq {\theta_2}^I \circ {\theta_1}^I$. Por conseguinte, $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1$. Logo $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$. □

Teorema 3.3.15. *Seja $\mathcal{A}$ uma álgebra. Se $\mathcal{A}$ é congruente-permutável, então $\mathcal{A}$ é congruente-modular.*

Demonstração. Sejam $\mathcal{A} = (A; F)$ uma álgebra congruente-permutável e $\theta_1, \theta_2, \theta_3$ congruências de $\mathcal{A}$ tais que $\theta_1 \subseteq \theta_2$. Pretendemos mostrar que $\theta_2 \wedge (\theta_1 \vee \theta_3) \subseteq \theta_1 \vee (\theta_2 \wedge \theta_3)$. Seja $(a, b) \in \theta_2 \wedge (\theta_1 \vee \theta_3)$. Uma vez que $(a, b) \in \theta_1 \vee \theta_3$ e $\theta_1 \vee \theta_3 = \theta_3 \circ \theta_1$, existe um elemento $c \in A$ tal que $(a, c) \in \theta_1$ e $(c, b) \in \theta_3$. Como $(a, c) \in \theta_1$ e θ_1 é simétrica, então $(c, a) \in \theta_1$. Logo $(c, a) \in \theta_2$, pois $\theta_1 \subseteq \theta_2$. Dado que $(c, a) \in \theta_2$ e $(a, b) \in \theta_2$, tem-se $(c, b) \in \theta_2$. Assim, atendendo a que $(a, c) \in \theta_1$ e $(c, b) \in \theta_2 \wedge \theta_3$, resulta que $(a, b) \in (\theta_2 \wedge \theta_3) \circ \theta_1 = \theta_1 \vee (\theta_2 \wedge \theta_3)$. □

Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo (O, τ) e θ uma congruência em $\mathcal{A}$. Atendendo à propriedade de substituição satisfeita pela congruência θ, é simples verificar que, para cada $n \in \mathbb{N}_0$ e para cada $f \in O_n$, a correspondência de $(A/\theta)^n$ em A/θ que a cada elemento $([a_1]_\theta, \ldots, [a_n]_\theta)$ de $(A/\theta)^n$ associa o elemento $[f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta$ é independente dos representantes $a_1, \ldots, a_n$ que se escolhem para as classes $[a_1]_\theta$, ..., $[a_n]_\theta$, pelo que esta correspondência é uma operação n-ária em A/θ. Assim, é possível associar ao conjunto quociente A/θ a estrutura de uma álgebra do mesmo tipo da álgebra $\mathcal{A}$.

Definição 3.3.16. *Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo (O, τ) e θ uma congruência em $\mathcal{A}$. Chama-se* ***álgebra quociente de*** $\mathcal{A}$*, e representa-se por $\mathcal{A}/\theta$, a álgebra $(A/\theta; (f^{A/\theta})_{f\in O})$ do mesmo tipo da álgebra $\mathcal{A}$ e tal que, para qualquer $n \in \mathbb{N}_0$ e para qualquer símbolo operacional $f \in O_n$,*

$$f^{\mathcal{A}/\theta}([a_1]_\theta, \ldots, [a_n]_\theta) = [f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta, \ \forall a_1, \ldots, a_n \in A.$$

3.4 Homomorfismos

No estudo de aplicações entre álgebras do mesmo tipo são particularmente relevantes as que são compatíveis com as operações das álgebras: os homomorfismos.

Definição 3.4.1. *Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo (O, τ) e $\alpha : A \to B$ uma função. Diz-se que α* ***é um homomorfismo*** *de $\mathcal{A}$ em $\mathcal{B}$, e escreve-se $\alpha : \mathcal{A} \to \mathcal{B}$, se, para cada $n \in \mathbb{N}_0$ e para cada $f \in O_n$, α* ***é compatível com*** *f, i.e., se*

$$\alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)),$$

para quaisquer $a_1, \ldots, a_n \in A$.

Exemplo 3.4.2. *Os homomorfismos de grupos, de anéis e de reticulados são casos particulares da definição anterior.*

Dadas álgebras $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ do mesmo tipo, representa-se por $\mathrm{Hom}(\mathcal{A}, \mathcal{B})$ o conjunto dos homomorfismos de $\mathcal{A}$ em $\mathcal{B}$. Dado $\alpha \in \mathrm{Hom}(\mathcal{A}, \mathcal{B})$, diz-se que: α é um ***epimorfismo*** se α é uma aplicação sobrejetiva; α é um ***monomorfismo*** ou um ***mergulho*** de $\mathcal{A}$ em $\mathcal{B}$ se α é injetiva. Caso exista um mergulho de $\mathcal{A}$ em $\mathcal{B}$ diz-se que ***a álgebra $\mathcal{A}$ pode ser mergulhada na álgebra $\mathcal{B}$***. A um homomorfismo que seja bijetivo dá-se a designação de ***isomorfismo***. Diz-se que a álgebra $\mathcal{A}$ ***é isomorfa à álgebra $\mathcal{B}$*** se existe um isomorfismo de $\mathcal{A}$ em $\mathcal{B}$. Caso exista um isomorfismo de $\mathcal{A}$ em $\mathcal{B}$, também existe um isomorfismo de $\mathcal{B}$ em $\mathcal{A}$, pelo que, caso exista um isomorfismo de uma álgebra na outra, diz-se apenas que as álgebras $\mathcal{A}$ e $\mathcal{B}$ são isomorfas e escreve-se $\mathcal{A} \cong \mathcal{B}$. A um homomorfismo de $\mathcal{A}$ em $\mathcal{A}$ dá-se a designação de ***endomorfismo***. Um endomorfismo que seja bijetivo diz-se um ***automorfismo***. Os conjuntos dos endomorfismos e dos automorfismos de $\mathcal{A}$ representam-se, respetivamente, por $\mathrm{End}\mathcal{A}$ e por $\mathrm{Aut}\mathcal{A}$. A aplicação identidade id_A pertence quer a $\mathrm{End}\mathcal{A}$ quer a $\mathrm{Aut}\mathcal{A}$.

É simples a verificação de que cada um dos conjuntos $\mathrm{End}\mathcal{A}$ e $\mathrm{Aut}\mathcal{A}$ é fechado para a composição de aplicações, tal como é estabelecido no resultado seguinte.

Teorema 3.4.3. *Sejam $\mathcal{A}, \mathcal{B}$ e $\mathcal{C}$ álgebras do mesmo tipo. Se $\alpha : \mathcal{A} \to \mathcal{B}$ e $\beta : \mathcal{B} \to \mathcal{C}$ são homomorfismos (respetivamente, isomorfismos), então $\beta \circ \alpha$ é um homomorfismo (respetivamente, isomorfismo) de $\mathcal{A}$ em $\mathcal{C}$.* □

Do resultado anterior segue que, para cada álgebra $\mathcal{A}$, $\mathcal{E}nd\mathcal{A} = (\mathrm{End}\mathcal{A}; \circ, \mathrm{id}_A)$ é um monóide e a estrutura algébrica $\mathcal{A}ut\mathcal{A} = (\mathrm{Aut}\mathcal{A}; \circ, ^{-1}, \mathrm{id}_A)$, onde $^{-1}$ representa a operação unária que a cada automorfismo de $\mathrm{Aut}\mathcal{A}$ associa a sua aplicação inversa, é um grupo.

Um isomorfismo é uma correspondência bijetiva entre os elementos de duas álgebras do mesmo tipo que respeita a interpretação de cada símbolo operacional. Assim, há certas propriedades, ditas "propriedades algébricas", que sendo satisfeitas por uma dada álgebra são satisfeitas por qualquer álgebra que lhe seja isomorfa, o que torna as álgebras indistinguíveis a respeito destas propriedades. Embora duas álgebras isomorfas possam ser completamente diferentes, em particular no que respeita aos seus elementos, é usual dizer que "as álgebras são a mesma, a menos de isomorfismo".

Seguidamente apresentam-se algumas propriedades a respeito de homomorfismos.

Teorema 3.4.4. *Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo. Se a álgebra $\mathcal{A}$ é gerada por um conjunto X ($X \subseteq A$) e $\alpha, \beta : \mathcal{A} \to \mathcal{B}$ são homomorfismos tais que, para todo $x \in X$, $\alpha(x) = \beta(x)$, então $\alpha = \beta$.*

Demonstração. Se a álgebra $\mathcal{A}$ é gerada pelo conjunto X, então do Teorema 3.2.7 segue que $A = \bigcup_{i\in\mathbb{N}_0} X_i$, onde

$$\begin{array}{lcl} X_0 & = & X; \\ X_{i+1} & = & X_i \cup \{f(x) \mid f \text{ é operação } n\text{-ária em } \mathcal{A} \text{ e } x \in (X_i)^n, n \in \mathbb{N}_0\}. \end{array}$$

Por indução em i prova-se que, para todo $i \in \mathbb{N}_0$, tem-se $\alpha(x) = \beta(x)$, para qualquer $x \in X_i$. Por conseguinte, para todo $x \in A$, $\alpha(x) = \beta(x)$ e, portanto, $\alpha = \beta$. □

Teorema 3.4.5. *Sejam $\mathcal{A} = (A; F)$, $\mathcal{B} = (B; G)$ álgebras do mesmo tipo e $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo.*

(i) Se A_1 é um subuniverso de $\mathcal{A}$, então $\alpha(A_1)$ é um subuniverso de $\mathcal{B}$.

(ii) Se B_1 é um subuniverso de $\mathcal{B}$, então $\alpha^{\leftarrow}(B_1)$ é um subuniverso de $\mathcal{A}$.

(iii) Para qualquer $X \subseteq A$, $Sg^{\mathcal{B}}(\alpha(X)) = \alpha(Sg^{\mathcal{A}}(X))$.

Demonstração. A prova de (i) e de (ii) é um exercício simples que fica ao cuidado do leitor.

(iii) Dado $X \subseteq A$, sejam

- $X_0 = X$;
- $X_{k+1} = X_k \cup \{f(x) \mid f \text{ é operação } n\text{-ária em } \mathcal{A} \text{ e } x \in (X_k)^n, n \in \mathbb{N}_0\}$;
- $(\alpha(X))_0 = \alpha(X)$;

- $(\alpha(X))_{k+1} = (\alpha(X))_k \cup \{f(x) \mid f$ é operação n-ária em $\mathcal{B}$ e $x \in ((\alpha(X))_k)^n, n \in \mathbb{N}_0\}$.

Por indução em k, prova-se que, para todo $k \in \mathbb{N}_0$, $(\alpha(X))_k = \alpha(X_k)$. Então

$$Sg^{\mathcal{B}}(\alpha(X)) = \bigcup_{k\in\mathbb{N}_0}(\alpha(X))_k = \bigcup_{k\in\mathbb{N}_0}\alpha(X_k) = \alpha(\bigcup_{k\in\mathbb{N}_0}X_k) = \alpha(Sg^{\mathcal{A}}(\alpha(X))).$$

□

Do teorema anterior é imediato o resultado seguinte.

Corolário 3.4.6. *Sejam $\mathcal{A} = (A; F)$, $\mathcal{B} = (B; G)$ álgebras de tipo (O, τ) e $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo.*

(i) Se $\mathcal{A}_1 = (A_1; F_1)$ é uma subálgebra de $\mathcal{A}$, então o par $(\alpha(A_1); (f^{\alpha(\mathcal{A}_1)})_{f\in O})$, onde, para cada $n \in \mathbb{N}_0$ e para cada $f \in O_n$, $f^{\alpha(\mathcal{A}_1)}$ é a função de $(\alpha(A_1))^n$ em $\alpha(A_1)$ definida por

$$f^{\alpha(\mathcal{A}_1)}(\alpha(a_1), \ldots, \alpha(a_n)) = f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)),$$

para quaisquer $a_1, \ldots, a_n \in A_1$, é uma subálgebra de $\mathcal{B}$.

(ii) Se $\mathcal{B}_1 = (B_1, G_1)$ é uma subálgebra de $\mathcal{B}$ e $\alpha^{\leftarrow}(B_1) \neq \emptyset$, então o par $(\alpha^{\leftarrow}(B_1); (f^{\alpha^{\leftarrow}(\mathcal{B}_1)})_{f\in O})$, onde, para cada $n \in \mathbb{N}_0$ e para cada $f \in O_n$, $f^{\alpha^{\leftarrow}(\mathcal{B}_1)}$ é a função de $(\alpha^{\leftarrow}(B_1))^n$ em $\alpha^{\leftarrow}(B_1)$ definida por

$$f^{\alpha^{\leftarrow}(\mathcal{B}_1)}(a_1, \ldots, a_n) = f^{\mathcal{A}}(a_1, \ldots, a_n),$$

para quaisquer $a_1, \ldots, a_n \in \alpha^{\leftarrow}(B_1)$, é uma subálgebra de $\mathcal{A}$. □

Sendo $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo (O, τ), $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo, $\mathcal{A}_1 = (A_1; F_1)$ uma subálgebra de $\mathcal{A}$ e $\mathcal{B}_1 = (B_1; G_1)$ uma subálgebra de $\mathcal{B}$ nas condições do teorema anterior: designa-se por ***imagem homomorfa de*** $\mathcal{A}_1$, e representa-se por $\alpha(\mathcal{A}_1)$, a álgebra $(\alpha(A_1); (f^{\alpha(\mathcal{A}_1)})_{f\in O})$; dá-se a designação de ***pré-imagem de*** $\mathcal{B}_1$, e representa-se por $\alpha^{\leftarrow}(\mathcal{B}_1)$, à álgebra $(\alpha^{\leftarrow}(B_1); (f^{\alpha^{\leftarrow}(\mathcal{B}_1)})_{f\in O})$. Observe-se que a álgebra $\mathcal{B}$ é uma imagem homomorfa de $\mathcal{A}$ se e só se existe um epimorfismo de $\mathcal{A}$ em $\mathcal{B}$.

Dado um homomorfismo α entre álgebras $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$, a aplicação $\alpha : A \to B$ não é, em geral, injetiva. Sendo assim, tem interesse estudar a relação binária induzida por α, ou seja, a que relaciona elementos de A que tenham a mesma imagem através da aplicação α.

Definição 3.4.7. *Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo e $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo. Designa-se por* ***kernel de*** *α, e representa-se por* $\ker \alpha$*, a relação binária em A definida por*

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

Teorema 3.4.8. *Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo e $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo. Então a relação* $\ker \alpha$ *é uma congruência em $\mathcal{A}$.*

Demonstração. É imediato que $\ker \alpha$ é uma relação de equivalência em A. Além disso, para cada $n \in \mathbb{N}_0$ e para cada $f \in O_n$, se $(a_i, b_i) \in \ker \alpha$, para todo $i \in \{1, \ldots, n\}$, então

$$\begin{aligned} \alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)) &= f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)) \\ &= f^{\mathcal{B}}(\alpha(b_1), \ldots, \alpha(b_n)) \\ &= \alpha(f^{\mathcal{A}}(b_1, \ldots, b_n)) \end{aligned}$$

e, portanto, $(f^{\mathcal{A}}(a_1, \ldots, a_n), f^{\mathcal{A}}(b_1, \ldots, b_n)) \in \ker \alpha$. Logo $\ker \alpha$ é uma congruência em $\mathcal{A}$. □

Do teorema anterior segue que a cada homomorfismo é possivel associar uma congruência. Reciprocamente, a cada congruência também é possível associar um homomorfismo.

Dada uma álgebra $\mathcal{A} = (A; F)$ e dada uma congruência θ em $\mathcal{A}$, é imediato que a correspondência π_θ de A em A/θ, definida por $\pi_\theta(a) = [a]_\theta$, para todo $a \in A$, é uma aplicação.

Definição 3.4.9. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e θ uma congruência em $\mathcal{A}$. A aplicação $\pi_\theta : A \to A/\theta$, definida por $\pi_\theta(a) = [a]_\theta$, é designada por* ***aplicação natural de*** *A* ***em*** *A/θ.*

Teorema 3.4.10. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e θ uma congruência em $\mathcal{A}$. Então a aplicação $\pi_\theta : A \to A/\theta$, definida por $\pi_\theta(a) = [a]_\theta$, para todo $a \in A$, é um epimorfismo de $\mathcal{A}$ em $\mathcal{A}/\theta$.*

Demonstração. Sejam $\theta \in \mathrm{Con}\mathcal{A}$ e $\pi_\theta : A \to A/\theta$ a aplicação definida por $\pi_\theta(a) = [a]_\theta$, para todo $a \in A$. Então, para cada $n \in \mathbb{N}_0$, para cada $f \in O_n$ e para quaisquer $a_1, \ldots, a_n \in A$, tem-se

$$\begin{aligned} \pi_\theta(f^{\mathcal{A}}(a_1, \ldots, a_n)) &= [f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta \\ &= f^{\mathcal{A}/\theta}([a_1]_\theta, \ldots, [a_n]_\theta) \\ &= f^{\mathcal{A}/\theta}(\pi_\theta(a_1), \ldots, \pi_\theta(a_n)), \end{aligned}$$

pelo que π_θ é um homomorfismo. Claramente, π_θ é sobrejetiva. □

Definição 3.4.11. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e θ uma congruência em $\mathcal{A}$. Ao epimorfismo $\pi_\theta : \mathcal{A} \to \mathcal{A}/\theta$ dá-se a designação de* ***homomorfismo natural de*** *$\mathcal{A}$* ***em*** *$\mathcal{A}/\theta$.*

Dos teoremas 3.4.8 e 3.4.10 resulta que as congruências de uma álgebra $\mathcal{A}$ são exatamente os kernels dos homomorfismos com domínio $\mathcal{A}$.

Teorema 3.4.12 (Teorema do Homomorfismo)**.** *Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo, $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo, $\theta = \ker \alpha$ e $\pi_\theta : \mathcal{A} \to \mathcal{A}/\theta$ o homomorfismo natural. Então a correspondência β de A/θ para B, definida por $\beta([a]_\theta) = \alpha(a)$, para todo $[a]_\theta \in A/\theta$, é um monomorfismo de $\mathcal{A}/\theta$ em $\mathcal{B}$ e tem-se $\beta \circ \pi_\theta = \alpha$. Caso α seja um epimorfismo, então β é um isomorfismo.*

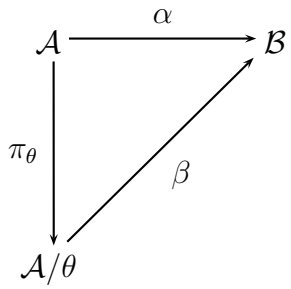


Figura 3.1

Demonstração. A correspondência β é uma aplicação. Com efeito, para todo $[a]_\theta \in A/\theta$, tem-se $\beta([a]_\theta) \in B$ e, para quaisquer $[a]_\theta, [b]_\theta \in A/\theta$,

$$[a]_\theta = [b]_\theta \Rightarrow a\,\theta\,b \Rightarrow \alpha(a) = \alpha(b) \Rightarrow \beta([a]_\theta) = \beta([b]_\theta).$$

Facilmente também se prova que β é injetiva, pois, para quaisquer $[a]_\theta, [b]_\theta \in A/\theta$,

$$\beta([a]_\theta) = \beta([b]_\theta) \Rightarrow \alpha(a) = \alpha(b) \Rightarrow a\,\theta\,b \Rightarrow [a]_\theta = [b]_\theta.$$

A aplicação β é um homomorfismo, uma vez que, para qualquer $n \in \mathbb{N}_0$, para qualquer símbolo de operação n-ário f e para quaisquer $a_1, \ldots, a_n \in A$,

$$\begin{aligned} \beta(f^{\mathcal{A}/\theta}([a_1]_\theta, \ldots, [a_n]_\theta)) &= \beta([f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta) \\ &= \alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)) \\ &= f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)) \\ &= f^{\mathcal{B}}(\beta([a_1]_\theta), \ldots, \beta([a_n]_\theta)). \end{aligned}$$

Assim, β é um monomorfismo.
A prova da igualdade $\beta \circ \pi_\theta = \alpha$ é imediata, pois $\beta \circ \pi_\theta$ e α são ambas aplicações de A em B e, para qualquer $a \in A$,

$$(\beta \circ \pi_\theta)(a) = \beta(\pi_\theta(a)) = \beta([a]_\theta) = \alpha(a).$$

Caso α seja um epimorfismo é simples concluir que β é um isomorfismo. De facto, se α é sobrejetiva, então, para todo $b \in B$, existe $a \in A$ tal que $b = \alpha(a)$ e, por conseguinte, $b = \beta([a]_\theta)$; logo β também é sobrejetiva. □

O Teorema do Homomorfismo é também conhecido por Primeiro Teorema do Isomorfismo.

Do Teorema 3.4.3 e do Teorema do Homomorfismo segue que uma álgebra é imagem homomorfa de uma álgebra $\mathcal{A}$ se e só se é isomorfa a uma álgebra quociente de $\mathcal{A}$. Assim, o problema da determinação das imagens homomorfas de $\mathcal{A}$ reduz-se ao problema da determinação das congruências de $\mathcal{A}$.

Definição 3.4.13. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $\theta, \phi \in \mathrm{Con}\mathcal{A}$ tais que $\theta \subseteq \phi$. Define-se a relação ϕ/θ em A/θ por*

$$\phi/\theta = \{([a]_\theta, [b]_\theta) \in (A/\theta)^2 \mid (a, b) \in \phi\}.$$

Lema 3.4.14. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $\theta, \phi \in \mathrm{Con}\mathcal{A}$ tais que $\theta \subseteq \phi$. Então ϕ/θ é uma congruência em $\mathcal{A}/\theta$.*

Demonstração. Atendendo a que ϕ é uma relação de equivalência em A, é imediato que ϕ/θ é uma relação de equivalência em A/θ. A propriedade de substituição para ϕ/θ resulta da propriedade de substituição para ϕ. Seja f um símbolo operacional n-ário de $\mathcal{A}$, $n \in \mathbb{N}_0$, e suponhamos que $([a_i]_\theta, [b_i]_\theta) \in \phi/\theta$, para todo $1 \leq i \leq n$. Então $(a_i, b_i) \in \phi$, para todo $1 \leq i \leq n$, pelo que

$$(f^{\mathcal{A}}(a_1, \ldots, a_n), f^{\mathcal{A}}(b_1, \ldots, b_n)) \in \phi.$$

Logo

$$([f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta, [f^{\mathcal{A}}(b_1, \ldots, b_n)]_\theta) \in \phi/\theta$$

e, portanto,

$$(f^{\mathcal{A}/\theta}([a_1]_\theta, \ldots, [a_n]_\theta), f^{\mathcal{A}/\theta}([b_1]_\theta, \ldots, [b_n]_\theta)) \in \phi/\theta.$$

□

Teorema 3.4.15 (Segundo Teorema do Isomorfismo)**.** *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $\theta, \phi \in \mathrm{Con}\mathcal{A}$ tais que $\theta \subseteq \phi$. Então a correspondência α de $(A/\theta)/(\phi/\theta)$ para A/ϕ, dada por $\alpha([[a]_\theta]_{\phi/\theta}) = [a]_\phi$, é um isomorfismo.*

Demonstração. Para todo $a \in A$, tem-se $\alpha([[a]_\theta]_{\phi/\theta}) \in A/\phi$ e, para todos $a, b \in A$,

$$[[a]_\theta]_{\phi/\theta} = [[b]_\theta]_{\phi/\theta} \text{ sse } [a]_\phi = [b]_\phi,$$

pelo que α é uma aplicação e é injetiva. Claramente, a aplicação α também é sobrejetiva. Além disso, para todo $n \in \mathbb{N}_0$, para todo o símbolo operacional n-ário f e para quaisquer $a_1, \ldots, a_n \in A$, tem-se

$$\begin{aligned}
&\alpha(f^{(\mathcal{A}/\theta)/(\phi/\theta)}([[a_1]_\theta]_{\phi/\theta}, \ldots, [[a_n]_\theta]_{\phi/\theta})) \\
&\quad = \alpha([f^{\mathcal{A}/\theta}([a_1]_\theta, \ldots, [a_n]_\theta)]_{\phi/\theta}) \\
&\quad = \alpha([[f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta]_{\phi/\theta}) \\
&\quad = [f^{\mathcal{A}}(a_1, \ldots, a_n)]_\phi \\
&\quad = f^{\mathcal{A}/\phi}([a_1]_\phi, \ldots, [a_n]_\phi) \\
&\quad = f^{\mathcal{A}/\phi}(\alpha([[a_1]_\theta]_{\phi/\theta}), \ldots, \alpha([[a_n]_\theta]_{\phi/\theta}))
\end{aligned}$$

e, portanto, α é um isomorfismo. □

Definição 3.4.16. *Sejam $\mathcal{A} = (A; F)$ uma álgebra, $\theta \in \mathrm{Con}\mathcal{A}$ e $B \subseteq A$. Define-se*

$$B^\theta = \{a \in A \mid [a]_\theta \cap B \neq \emptyset\}$$

e representa-se por:

- *$\mathcal{B}^\theta$ a subálgebra de $\mathcal{A}$ gerada por B^θ.*
- *$\theta_{|B}$ a restriçao de θ a B (i.e., $\theta_{|B} = \theta \cap B^2$).*

Lema 3.4.17. *Sejam $\mathcal{A} = (A; F)$ uma álgebra, $\mathcal{B} = (B; G)$ uma subálgebra de $\mathcal{A}$ e $\theta \in \operatorname{Con}\mathcal{A}$. Então*

(i) O universo de $\mathcal{B}^\theta$ é B^θ.

(ii) $\theta_{|B}$ é uma congruência em $\mathcal{B}$.

Demonstração. (i) Seja f um símbolo operacional n-ário. Dados $a_1, \ldots, a_n \in B^\theta$, existem $b_1, \ldots, b_n \in B$ tais que $(a_i, b_i) \in \theta$, para todo $1 \leq i \leq n$. Logo

$$(f^{\mathcal{A}}(a_1, \ldots, a_n), f^{\mathcal{A}}(b_1, \ldots, b_n)) \in \theta$$

e, atendendo a que $f^{\mathcal{A}}(b_1, \ldots, b_n) \in B$, segue que $f^{\mathcal{A}}(a_1, \ldots, a_n) \in B^\theta$. Assim, B^θ é um subuniverso de $\mathcal{A}$.

(ii) É claro que $\theta_{|B}$ é uma relação de equivalência em B. Além disso, para todo o símbolo operacional n-ário f e para quaisquer $a_1, \ldots, a_n$, $b_1, \ldots, b_n \in B$ tais que $(a_i, b_i) \in \theta$, para todo $1 \leq i \leq n$, tem-se $f^{\mathcal{B}}(a_1, \ldots, a_n), f^{\mathcal{B}}(b_1, \ldots, b_n) \in B$ e

$$(f^{\mathcal{B}}(a_1, \ldots, a_n), f^{\mathcal{B}}(b_1, \ldots, b_n)) \in \theta,$$

pelo que

$$(f^{\mathcal{B}}(a_1, \ldots, a_n), f^{\mathcal{B}}(b_1, \ldots, b_n)) \in \theta_{|B}.$$

□

Teorema 3.4.18 (Terceiro Teorema do Isomorfismo)**.** *Sejam $\mathcal{A} = (A; F)$ uma álgebra, $\mathcal{B} = (B; G)$ uma subálgebra de $\mathcal{A}$ e $\theta \in \operatorname{Con}\mathcal{A}$. Então a correspondência α de $B/\theta_{|B}$ para $B^\theta/\theta_{|B^\theta}$, definida por $\alpha([b]_{\theta_{|B}}) = [b]_{\theta_{|B^\theta}}$, é um isomorfismo.*

Demonstração. A prova deste resultado é deixada ao cuidado do leitor. □

Terminamos esta secção com o enunciado e a prova do Teorema da Correspondência, o qual é relevante no estudo de álgebras subdiretamente irredutíveis.

Teorema 3.4.19 (Teorema da Correspondência)**.** *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $\theta \in \operatorname{Con}\mathcal{A}$. Então o subrreticulado $([\theta, \nabla_A], \subseteq)$ de $\operatorname{Con}\mathcal{A}$ e o reticulado $\mathcal{C}on\mathcal{A}/\theta$ são isomorfos. Mais precisamente, a correspondência α de $[\theta, \nabla_A]$ para $\operatorname{Con} A/\theta$, definida por $\alpha(\phi) = \phi/\theta$, é um isomorfismo de reticulados de $[\theta, \nabla_A]$ em $\operatorname{Con}\mathcal{A}/\theta$.*

Demonstração. Atendendo ao Lema 3.4.14, a correspondência α é uma aplicação. No sentido de verificar que α é injetiva, consideremos $\phi, \psi \in [\theta, \nabla_A]$ tais que $\phi \neq \psi$. Então, sem perda de generalidade, podemos assumir que existem elementos $a, b \in A$ tais que $(a, b) \in \phi \setminus \psi$. Assim, $([a]_\theta, [b]_\theta) \in (\phi/\theta) \setminus (\psi/\theta)$ e, portanto, $\alpha(\phi) \neq \alpha(\psi)$. Para provar que α é sobrejetiva, consideremos $\psi \in \operatorname{Con}\mathcal{A}/\theta$ e $\phi = \ker(\pi_\psi \circ \pi_\theta)$. Então, para quaisquer $a, b \in A$,

$$\begin{array}{lll} ([a]_\theta, [b]_\theta) \in \phi/\theta & \text{sse} & (a, b) \in \phi \\ & \text{sse} & ([a]_\theta, [b]_\theta) \in \psi, \end{array}$$

pelo que

$$\phi/\theta = \psi.$$

Por último, prova-se que α é um mergulho de ordem. De facto, dados $\phi, \psi \in [\theta, \nabla_A]$, tem-se

$$\begin{array}{lll} \phi \subseteq \psi & \text{sse} & \phi/\theta \subseteq \psi/\theta \\ & \text{sse} & \alpha(\phi) \subseteq \alpha(\psi). \end{array}$$

□

3.5 Produtos diretos e álgebras diretamente indecomponíveis

Com os processos de construção de álgebras apresentados anteriormente, nomeadamente formação de subálgebras, álgebras quociente e imagens homomorfas, não é possível obter álgebras com uma cardinalidade superior à cardinalidade da álgebra inicial, mas com o processo de construção a seguir descrito, que consiste na formação de produtos diretos, torna-se possível obter álgebras de maior complexidade.

Definição 3.5.1. *Sejam I um conjunto e $(\mathcal{A}_i)_{i\in I} = ((A_i; F_i))_{i\in I}$ uma família de álgebras de tipo (O, τ). Designa-se por* ***produto direto*** *da família $(\mathcal{A}_i)_{i\in I}$, e representa-se por $\prod_{i\in I} \mathcal{A}_i$, a álgebra $(\prod_{i\in I} A_i, (f^{\prod_{i\in I}\mathcal{A}_i})_{f\in O})$ de tipo (O, τ) tal que, para todo $n \in \mathbb{N}_0$, para todo o símbolo de operação $f \in O_n$ e para quaisquer $f_1, \ldots, f_n \in \prod_{i\in I} A_i$,*

$$f^{\prod_{i\in I}\mathcal{A}_i}(f_1, \ldots, f_n)(i) = f^{\mathcal{A}_i}(f_1(i), \ldots, f_n(i)), \text{ para todo } i \in I.$$

Sejam $(A_i)_{i\in I}$ uma família de álgebras do mesmo tipo. Se $I = \{i_1, \ldots, i_k\}$, o produto direto $\prod_{i\in I} \mathcal{A}_i$ é representado por $\mathcal{A}_{i_1} \times \ldots \times \mathcal{A}_{i_k}$. No caso em que $\mathcal{A}_i = \mathcal{A}$, para todo $i \in I$, $\prod_{i\in I} \mathcal{A}_i$ é representado por $\mathcal{A}^I$ e diz-se uma potência direta de $\mathcal{A}$. Se $I = \emptyset$, $\prod_{i\in I} \mathcal{A}_i$ é a álgebra trivial com universo $\{\emptyset\}$.
Para todo $j \in I$, a projeção $p_j : \prod_{i\in I} A_i \to A_j$ é um epimorfismo de $\prod_{i\in I} \mathcal{A}_i$ em $\mathcal{A}_j$. Assim, cada uma das álgebras $\mathcal{A}_j$, $j \in I$, é imagem homomorfa de $\prod_{i\in I} \mathcal{A}_i$.

A prova do resultado seguinte é um exercício de rotina.

Teorema 3.5.2. *Se $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$ são álgebras do mesmo tipo, então:*

(i) $\mathcal{A}_1 \times \mathcal{A}_2 \cong \mathcal{A}_2 \times \mathcal{A}_1$.

(ii) $\mathcal{A}_1 \times (\mathcal{A}_2 \times \mathcal{A}_3) \cong (\mathcal{A}_1 \times \mathcal{A}_2) \times \mathcal{A}_3$.

Demonstração. Exercício. □

Teorema 3.5.3. *Sejam $(\mathcal{A}_i)_{i\in I} = ((A_i; F_i))_{i\in I}$ uma família de álgebras do mesmo tipo e $\mathcal{A} = (A; F)$ uma subálgebra de $\prod_{i\in I} \mathcal{A}_i$. Então $\bigcap_{i\in I} (\ker p_i)_{|A} = \triangle_A$.*

Demonstração. Seja $(a, b) \in \bigcap_{i\in I} (\ker p_i)_{|A}$. Então $a, b \in A \subseteq \prod_{i\in I} A_i$ e, para todo $i \in I$, $p_i(a) = p_i(b)$. Logo $a = b$ e, portanto, $(a, b) \in \triangle_A$. Reciprocamente, é óbvio que $\triangle_A \subseteq (\ker p_i)_{|A}$, para todo $i \in I$. □

Lema 3.5.4. *Sejam $\mathcal{A}_1 = (A_1; F_1)$ e $\mathcal{A}_2 = (A_2; F_2)$ álgebras do mesmo tipo, $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ e $p_i : A_1 \times A_2 \to A_i$ a projeção-i, $i \in \{1, 2\}$. Em $\operatorname{Con}\mathcal{A}$, tem-se*

(i) $\ker\ p_1 \cap \ker p_2 = \triangle_{A_1 \times A_2}$.

(ii) $\ker\ p_1 \circ \ker p_2 = \ker\ p_2 \circ \ker p_1$.

(iii) $\ker\ p_1 \vee \ker p_2 = \nabla_{A_1 \times A_2}$.

Demonstração. (i) Imediato a partir da proposição anterior.

(ii), (iii) Dados $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$, tem-se

$$((a_1, a_2), (b_1, a_2)) \in \ker p_2 \text{ e } ((b_1, a_2), (b_1, b_2)) \in \ker p_1.$$

Logo $\ker p_1 \circ \ker p_2 = \nabla_{A_1 \times A_2}$. De modo análogo prova-se que $\ker p_2 \circ \ker p_1 = \nabla_{A_1 \times A_2}$. Assim, $\ker p_1$ e $\ker p_2$ são permutáveis e do Teorema 3.3.14 segue que $\ker p_1 \vee \ker p_2 = \nabla_{A_1 \times A_2}$. □

O resultado anterior motiva a definição seguinte.

Definição 3.5.5. *Sejam $\mathcal{A} = (A; F)$ uma álgebra. Uma congruência θ_1 em $\mathcal{A}$ diz-se uma* ***congruência fator*** *se existe uma congruência θ_2 em $\mathcal{A}$ tal que θ_1 e θ_2 são permutáveis, $\theta_1 \cap \theta_2 = \triangle_A$ e $\theta_1 \vee \theta_2 = \nabla_A$. Se θ_1 e θ_2 são congruências em $\mathcal{A}$ que satisfazem estas condições, o par (θ_1, θ_2) diz-se um* ***par de congruências fator em*** *$\mathcal{A}$.*

Do Lema 3.5.4 sabe-se que a álgebra resultante do produto direto de duas álgebras tem sempre duas congruências fator. Reciprocamente, se uma álgebra tem um par de congruências fator, então esta álgebra é isomorfa a um produto direto de duas álgebras.

Teorema 3.5.6. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e (θ_1, θ_2) um par de congruências fator em $\mathcal{A}$. Então a correspondência $\alpha : A \to A/\theta_1 \times A/\theta_2$, definida por $\alpha(a) = ([a]_{\theta_1}, [a]_{\theta_2})$, para todo $a \in A$, é um isomorfismo de $\mathcal{A}$ em $\mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$.*

Demonstração. Claramente, α é uma aplicação.
De forma simples verifica-se que a aplicação α é injetiva: dados $a, b \in A$ tais que $\alpha(a) = \alpha(b)$, tem-se $[a]_{\theta_1} = [b]_{\theta_1}$ e $[a]_{\theta_2} = [b]_{\theta_2}$. Logo $(a, b) \in \theta_1$ e $(a, b) \in \theta_2$, donde $a = b$.
A aplicação α também é sobrejetiva. De facto, dados $a, b \in A$, existe $c \in A$ tal que $(a, c) \in \theta_1$ e $(c, b) \in \theta_2$. Então $([a]_{\theta_1}, [b]_{\theta_2}) = ([c]_{\theta_1}, [c]_{\theta_2}) = \alpha(c)$.
Por último, prova-se que α é um homomorfismo, uma vez que, para todo o símbolo operacional f que seja n-ário e para quaisquer $a_1, \ldots, a_n \in A$, tem-se

$$\begin{aligned}
\alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)) &= ([f^{\mathcal{A}}(a_1, \ldots, a_n)]_{\theta_1}, [f^{\mathcal{A}}(a_1, \ldots, a_n)]_{\theta_2}) \\
&= (f^{\mathcal{A}/\theta_1}([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1}), f^{\mathcal{A}/\theta_2}([a_1]_{\theta_2}, \ldots, [a_n]_{\theta_2})) \\
&= f^{\mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2}(([a_1]_{\theta_1}, [a_1]_{\theta_2}), \ldots, ([a_n]_{\theta_1}, [a_n]_{\theta_2})) \\
&= f^{\mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2}(\alpha(a_1), \ldots, \alpha(a_n)).
\end{aligned}$$

□

O resultado anterior mostra que é possível recorrer a certas congruências de uma álgebra para expressá-la como um produto direto de álgebras possívelmente mais pequenas. Porém, em certos casos só é possível expressar uma álgebra como um produto direto de álgebras se um dos fatores do produto direto for uma álgebra isomorfa à álgebra dada.

Definição 3.5.7. *Seja $\mathcal{A}$ uma álgebra. Diz-se que $\mathcal{A}$ é **diretamente indecomponível** se sempre que $\mathcal{A} \cong \mathcal{A}_1 \times \mathcal{A}_2$, então $\mathcal{A}_1$ é a álgebra trivial ou $\mathcal{A}_2$ é a álgebra trivial.*

Exemplo 3.5.8. *Toda a álgebra finita com um número primo de elementos é diretamente indecomponível.*

Corolário 3.5.9. *Seja $\mathcal{A}$ uma álgebra. Então $\mathcal{A}$ é diretamente indecomponível se e só se as únicas congruências fator de $\mathcal{A}$ são $\triangle_A$ e ∇_A.*

Demonstração. Imediato a partir do Lema 3.5.4 e do Teorema 3.5.6. □

O resultado seguinte estabelece que as álgebras diretamente indecomponíveis funcionam como "blocos de construção" de certas álgebras.

Teorema 3.5.10. *Toda a álgebra finita é isomorfa a um produto direto de álgebras diretamente indecomponíveis.*

Demonstração. Seja $\mathcal{A} = (A; F)$ uma álgebra finita. A prova segue por indução forte no número de elementos de A. Se $|A| = 1$, ou seja, se $\mathcal{A}$ é trivial, o resultado é imediato, uma vez que $\mathcal{A}$ é diretamente indecomponível. Se $\mathcal{A}$ não é trivial, admita-se, por hipótese de indução, que toda álgebra $\mathcal{B} = (B; G)$ tal que $|B| < |A|$ é isomorfa a um produto direto de álgebras diretamente indecomponíveis. Caso $\mathcal{A}$ seja diretamente indecomponível, a prova termina. Se $\mathcal{A}$ não é diretamente indecomponível, então existem álgebras não triviais $\mathcal{A}_1$ e $\mathcal{A}_2$ tais que $\mathcal{A} \cong \mathcal{A}_1 \times \mathcal{A}_2$. Uma vez que $|A_1|, |A_2| < |A|$ segue, por hipótese de indução, que

$$\begin{array}{rcl} \mathcal{A}_1 & \cong & \mathcal{B}_1 \times \ldots \times \mathcal{B}_m \\ \mathcal{A}_2 & \cong & \mathcal{C}_1 \times \ldots \times \mathcal{C}_n, \end{array}$$

onde $\mathcal{B}_1, \ldots, \mathcal{B}_m, \mathcal{C}_1, \ldots, \mathcal{C}_n$ são álgebras diretamente indecomponíveis. Consequentemente,

$$\mathcal{A} \cong \mathcal{B}_1 \times \ldots \times \mathcal{B}_m \times \mathcal{C}_1 \times \ldots \times \mathcal{C}_n.$$

□

Seguidamente estabelecem-se dois processos de obter um homomorfismo a partir de uma família de homomorfismos.

Teorema 3.5.11. *Sejam $\mathcal{A}$ uma álgebra, $(\mathcal{A}_i)_{i\in I}$ e $(\mathcal{B}_i)_{i\in I}$ famílias de álgebras do mesmo tipo de $\mathcal{A}$ e $(h_i : \mathcal{A} \to \mathcal{B}_i)_{i\in I}$ e $(g_i : \mathcal{A}_i \to \mathcal{B}_i)_{i\in I}$ famílias de homomorfismos. Então*

(i) A aplicação $h : A \to \prod_{i\in I} B_i$, definida por $(h(a))(i) = h_i(a)$, para todo $a \in A$ e para todo $i \in I$, é um homomorfismo de $\mathcal{A}$ em $\prod_{i\in I} \mathcal{B}_i$.

(ii) A aplicação $g : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$, definida por $(g(a))(i) = g_i(a(i))$, para todo $a \in \prod_{i\in I} A_i$ e para todo $i \in I$, é um homomorfismo de $\prod_{i\in I} \mathcal{A}_i$ em $\prod_{i\in I} \mathcal{B}_i$.

Demonstração. (i) Para cada $i \in I$, h_i é um homomorfismo. Sejam f um símbolo operacional n-ário e $a_1, \ldots, a_n \in A$. Então, para cada $i \in I$, tem-se

$$\begin{aligned}(h(f^{\mathcal{A}}(a_1,\ldots,a_n)))(i) &= h_i(f^{\mathcal{A}}(a_1,\ldots,a_n))\\ &= f^{\mathcal{B}_i}(h_i(a_1),\ldots,h_i(a_n))\\ &= f^{\mathcal{B}_i}((h(a_1))(i),\ldots,(h(a_n))(i))\\ &= (f^{\prod_{i\in I}\mathcal{B}_i}(h(a_1),\ldots,h(a_n)))(i).\end{aligned}$$

Logo $h(f^{\mathcal{A}}(a_1,\ldots,a_n)) = f^{\prod_{i\in I}\mathcal{B}_i}(h(a_1),\ldots,h(a_n))$ e $h : \mathcal{A} \to \prod_{i\in I} \mathcal{B}_i$ é um homomorfismo.

(ii) Considerando em (i) $\mathcal{A} = \prod_{i\in I} \mathcal{A}_i$ e $h_i = g_i \circ p_i$, para todo $i \in I$, conclui-se que $g = h : \mathcal{A} \to \prod_{i\in I} \mathcal{B}_i$ é um homomorfismo. □

3.6 Produtos subdiretos e álgebras subdiretamente irredutíveis

Embora toda a álgebra finita seja isomorfa a um produto direto de álgebras diretamente indecomponíveis, o mesmo não acontece para álgebras infinitas em geral; por exemplo, as álgebras de Boole numeráveis infinitas não são isomorfas a produtos diretos de álgebras de Boole diretamente indecomponíveis. Assim, as álgebras diretamente indecomponíveis não podem ser consideradas como "blocos de construção" de toda a álgebra. A necessidade de obter "blocos de construção" gerais, levou Birkhoff a considerar um tipo de produto de álgebras diferente do produto direto.

Definição 3.6.1. *Sejam $\mathcal{A}$ uma álgebra e $(\mathcal{A}_i)_{i\in I}$ uma família de álgebras do mesmo tipo. Diz-se que a álgebra $\mathcal{A}$ é um* ***produto subdireto da família*** *$(\mathcal{A}_i)_{i\in I}$ se $\mathcal{A}$ é uma subálgebra de $\prod_{i\in I} \mathcal{A}_i$ e, para cada $i \in I$, $p_i(\mathcal{A}) = \mathcal{A}_i$.*

Note-se que se $I = \emptyset$, então $\mathcal{A}$ é produto subdireto de $(\mathcal{A}_i)_{i\in I}$ se e só se $\mathcal{A}$ é a álgebra trivial.

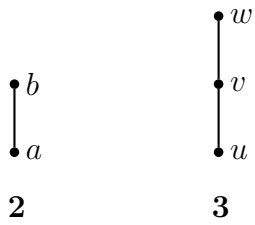
Exemplo 3.6.2.

(1) Sejam $(\mathcal{A}_i)_{i\in I}$ uma família de álgebras do mesmo tipo. O produto direto $\prod_{i\in I} \mathcal{A}_i$ é um produto subdireto de $(\mathcal{A}_i)_{i\in I}$.

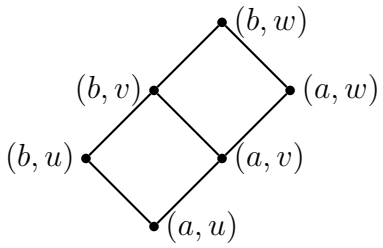
(2) Para qualquer álgebra $\mathcal{A} = (A; F)$ que não tenha operações nulárias, verifica-se facilmente que o conjunto $\triangle_A = \{(a, a) \mid a \in A\}$ é um subuniverso de $\mathcal{A} \times \mathcal{A}$;

representemos por $\triangle_{\mathcal{A}}$ *a subálgebra de* $\mathcal{A} \times \mathcal{A}$ *com universo* $\triangle_A$. *Uma vez que* $p_1(\triangle_A) = p_2(\triangle_A) = A$, *então* $\triangle_{\mathcal{A}}$ *é um produto subdireto de* $(\mathcal{A}_i)_{i\in\{1,2\}}$, *onde* $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A}$.

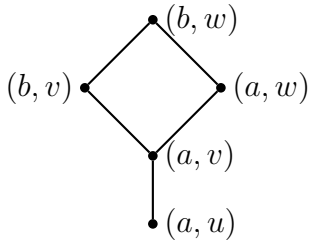
(3) Considerando os reticulados **2** *e* **3**, *i.e., as cadeias com dois e três elementos,*



o seu produto direto é o reticulado representado pelo diagrama



e o subrreticulado de $\mathbf{2} \times \mathbf{3}$ *representado por*



é um produto subdireto de **2** *e* **3**.

Definição 3.6.3. *Sejam* $\mathcal{A}$ *uma álgebra e* $(\mathcal{A}_i)_{i\in I}$ *uma família de álgebras do mesmo tipo. A um monomorfismo* $\alpha : \mathcal{A} \to \prod_{i\in I} \mathcal{A}_i$ *tal que* $\alpha(\mathcal{A})$ *é um produto subdireto de* $(\mathcal{A}_i)_{i\in I}$ *dá-se a designação de* ***mergulho subdireto****.*

Teorema 3.6.4. *Sejam* $\mathcal{A} = (A; F)$ *uma álgebra e* $(\theta_i)_{i\in I}$ *uma família de congruências em* $\mathcal{A}$ *tal que* $\bigcap_{i\in I} \theta_i = \triangle_A$. *Então a correspondência* $\alpha : A \to \prod_{i\in I} A/\theta_i$, *definida por* $(\alpha(a))(i) = [a]_{\theta_i}$, *para todo* $a \in A$, *é um mergulho subdireto.*

Demonstração. Pelo Teorema 3.5.11 sabe-se que a correspondência α é um homomorfismo de $\mathcal{A}$ em $\prod_{i\in I} \mathcal{A}/\theta_i$. A aplicação α também é injetiva, pois, para quaisquer $a, b \in A$,

$$\begin{aligned} \alpha(a) = \alpha(b) &\Rightarrow (\forall i \in I, [a]_{\theta_i} = [b]_{\theta_i}) \\ &\Rightarrow (\forall i \in I, (a, b) \in \theta_i) \\ &\Rightarrow (a, b) \in \textstyle\bigcap_{i\in I} \theta_i = \triangle_A \\ &\Rightarrow a = b. \end{aligned}$$

Então α é um monomorfismo.
A respeito de $\alpha(\mathcal{A})$ verifica-se facilmente que esta álgebra é um produto subdireto de $(\mathcal{A}/\theta_i)_{i\in I}$, uma vez que pelo Teorema 3.4.6 tem-se $\alpha(\mathcal{A}) \leq \prod_{i\in I}(\mathcal{A}/\theta_i)_{i\in I}$ e é óbvio que $p_i(\alpha(A)) = A/\theta_i$, para todo $i \in I$. □

Do teorema anterior é imediato o resultado seguinte.

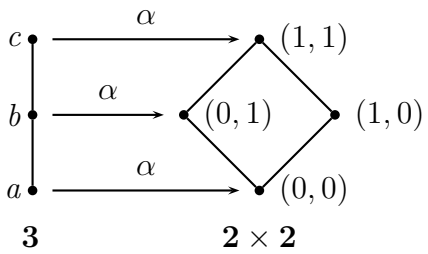
Teorema 3.6.5. *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $(\theta_i)_{i\in I}$ uma família de congruências em $\mathcal{A}$ tal que $\bigcap_{i\in I}\theta_i = \triangle_A$. Então $\mathcal{A}$ é isomorfa a um produto subdireto da família de álgebras $(\mathcal{A}/\theta_i)_{i\in I}$.*

Demonstração. Pelo teorema anterior sabe-se que a aplicação $\alpha : A \to \prod_{i\in I} A/\theta_i$, definida por $(\alpha(a))(i) = [a]_{\theta_i}$, para todo $a \in A$, é um monomorfismo. Logo $\mathcal{A} \cong \alpha(\mathcal{A})$. Pelo mesmo teorema sabe-se que $\alpha(\mathcal{A})$ é um produto subdireto da família de álgebras $(\mathcal{A}/\theta_i)_{i\in I}$. □

Em analogia com a definição de álgebras diretamente indecomponíveis, pretendemos considerar álgebras que não possam ser expressas como produto subdireto de álgebras mais pequenas, com excepção dos casos triviais.

Definição 3.6.6. *Uma álgebra $\mathcal{A}$ diz-se **subdiretamente irredutível** se, para qualquer família $(\mathcal{A})_{i\in I}$ de álgebras do mesmo tipo de $\mathcal{A}$ e para qualquer mergulho subdireto $\alpha : \mathcal{A} \to \prod_{i\in I}\mathcal{A}_i$, existe $i \in I$ tal que $p_i \circ \alpha$ é um isomorfismo.*

Exemplo 3.6.7. *A cadeia com três elementos $\mathbf{3}$ não é subdiretamente irredutível. De facto, considerando o monomorfismo α de $\mathbf{3}$ em $\mathbf{2}\times\mathbf{2}$ definido da forma seguinte*



verifica-se que este monomorfismo é um mergulho subdireto, pois a sua imagem é um produto subdireto de $(\mathcal{A}_i)_{i\in\{1,2\}}$, onde $\mathcal{A}_1 = \mathcal{A}_2 = \mathbf{2}$, mas nem $p_1 \circ \alpha$ nem $p_2 \circ \alpha$ é um monomorfismo.

Uma caracterização útil das álgebras subdiretamente irredutíveis, e que é geralmente usada para identificar estas álgebras, é dada pelo resultado seguinte.

Teorema 3.6.8. *Uma álgebra $\mathcal{A}$ é subdiretamente irredutível se e só se $\mathcal{A}$ é trivial ou $\mathrm{Con}\mathcal{A} \setminus \{\triangle_{\mathcal{A}}\}$ tem elemento mínimo. No segundo caso, o elemento mínimo de $\mathrm{Con}\mathcal{A} \setminus \{\triangle_{\mathcal{A}}\}$ é $\bigcap(\mathrm{Con}\mathcal{A} \setminus \{\triangle_{\mathcal{A}}\})$ e é uma congruência principal.*

Demonstração. ($\Rightarrow$) Seja $\mathcal{A} = (A; F)$ uma álgebra não trivial tal que $\mathrm{Con}\mathcal{A} \setminus \{\triangle_A\}$ não tem elemento mínimo. Então $I = \mathrm{Con}\mathcal{A} \setminus \{\triangle_\mathcal{A}\} \neq \emptyset$ e $\bigcap(\mathrm{Con}\mathcal{A} \setminus \{\triangle_A\}) = \triangle_A$. Pelo Teorema 3.6.4 segue que a aplicação $\alpha : A \to \prod_{\theta \in I} A/\theta$, definida por $(\alpha(a))(\theta) = [a]_\theta$, para todo $a \in A$, é um mergulho subdireto. No entanto, para cada $\theta \in I$, o epimorfismo canónico $\pi_\theta : A \to A/\theta$ não é injetivo, pelo que, para todo $\theta \in I$, $p_\theta \circ \alpha$ não é um isomorfismo, pois $p_\theta \circ \alpha = \pi_\theta$. Por conseguinte, $\mathcal{A}$ não é subdiretamente irredutível.
($\Leftarrow$) Sejam $\mathcal{A}$ uma álgebra, $(A_i)_{i \in I}$ uma família de álgebras do mesmo tipo de $\mathcal{A}$ e $\alpha : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$ um mergulho subdireto. Se $\mathcal{A}$ é trivial, então, para cada $i \in I$, $\mathcal{A}_i$ é trivial. Logo $p_i \circ \alpha : A \to A_i$ é um isomorfismo de $\mathcal{A}$ em $\mathcal{A}_i$, para cada $i \in I$. Caso $\mathcal{A}$ não seja trivial, admitamos que $\mathrm{Con}\mathcal{A} \setminus \{\triangle_A\}$ tem elemento mínimo θ. Neste caso tem-se $\theta = \bigcap(\mathrm{Con}\mathcal{A} \setminus \{\triangle_A\}) \neq \triangle_A$. Seja $(a, b) \in \theta$ tal que $a \neq b$. Então se $\alpha : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$ é um mergulho subdireto, tem-se $(\alpha(a))(i) \neq (\alpha(b))(i)$, para algum $i \in I$, donde $(p_i \circ \alpha)(a) \neq (p_i \circ \alpha)(b)$ e, por conseguinte, $(a, b) \notin \ker(p_i \circ \alpha)$. Assim, $\theta \nsubseteq \ker(p_i \circ \alpha)$ e, atendendo a que θ é o mínimo de $\mathrm{Con}\mathcal{A} \setminus \{\triangle_A\}$, segue que $\ker(p_i \circ \alpha) = \triangle_A$. Então $p_i \circ \alpha$ é um monomorfismo e, uma vez que $p_i \circ \alpha$ também é um epimorfismo, tem-se que $p_i \circ \alpha$ é um isomorfismo. Logo, se $\mathcal{A}$ é trivial ou $\mathrm{Con}\mathcal{A} \setminus \{\triangle_A\}$ tem elemento mínimo, a álgebra $\mathcal{A}$ é subdiretamente irredutível.

Se $\mathrm{Con}\mathcal{A} \setminus \{\triangle_A\}$ tem elemento mínimo θ, então θ é uma congruência principal. De facto, como $\theta \neq \triangle_A$, existem $a, b \in A$ tais que $a \neq b$ e $(a, b) \in \theta$, donde $\theta(a, b) \subseteq \theta$ e, por conseguinte, $\theta = \theta(a, b)$. □

Uma álgebra diretamente indecomponível nem sempre é uma álgebra subdiretamente irredutivel (basta considerar como exemplo as cadeias com exatamente três elementos), mas o recíproco verifica-se necessariamente.

Teorema 3.6.9. *Toda a álgebra subdiretamente irredutível é diretamente indecomponível.*

Demonstração. Do Teorema 3.6.8 segue que as únicas congruências fator de uma álgebra subdiretamente irredutível $\mathcal{A} = (A; F)$ são as congruências $\triangle_A$ e ∇_A. Logo, pelo Corolário 3.5.9, $\mathcal{A}$ é diretamente indecomponível. □

Teorema 3.6.10 (Birkhoff)**.** *Toda a álgebra é isomorfa a um produto subdireto de álgebras subdiretamente irredutíveis.*

Demonstração. Uma vez que as álgebras triviais são subdiretamente irredutíveis, apenas necessitamos de considerar o caso de álgebras não triviais $\mathcal{A} = (A; F)$. Dados $a, b \in A$ tais que $a \neq b$, sabe-se, pelo Lema de Zorn, que existe uma congruência $\theta_{a,b} \in \mathrm{Con}\mathcal{A}$ que é maximal no que respeita à propriedade $(a, b) \notin \theta_{a,b}$. Então $\theta(a, b) \vee \theta_{a,b}$ é a menor congruência de $[\theta_{a,b}, \nabla_A] \setminus \{\theta_{a,b}\}$ e pelos teoremas 3.4.19 e 3.6.8 segue que a álgebra $\mathcal{A}/\theta_{a,b}$ é subdiretamente irredutível. Uma vez que $\bigcap\{\theta_{a,b} \mid a, b \in A, a \neq b\} = \triangle_A$, resulta do Lema 3.6.4 que $\mathcal{A}$ é produto subdireto da família de álgebras subdiretamente irredutíveis $(A/\theta_{a,b})_{a \neq b}$. □

Como consequência imediata do teorema anterior tem-se o resultado seguinte.

Corolário 3.6.11. *Toda a álgebra finita é produto subdireto de um número finito de álgebras subdiretamente irredutíveis.*

Na definição seguinte consideramos um tipo especial de álgebras subdiretamente irredutíveis.

Definição 3.6.12. *Uma álgebra $\mathcal{A}$ diz-se* ***simples*** *se* $\mathrm{Con}\mathcal{A} = \{\triangle_A, \nabla_A\}$. *Uma congruência θ numa álgebra $\mathcal{A}$ diz-se* ***maximal*** *se o intervalo $[\theta, \nabla_A]$ tem exatamente dois elementos.*

Teorema 3.6.13. *Sejam $\mathcal{A}$ uma álgebra e $\theta \in \mathrm{Con}\mathcal{A}$. Então a álgebra $\mathcal{A}/\theta$ é simples se e só se θ é uma congruência maximal em $\mathcal{A}$ ou $\theta = \nabla_A$.*

Demonstração. O resultado é imediato das definições anteriores, uma vez que pelo Teorema 3.4.19 se tem $\mathrm{Con}\,\mathcal{A}/\theta \cong [\theta, \nabla_A]$. □

3.7 Operadores e variedades

A formação de subálgebras, imagens homomorfas, produtos diretos e produtos subdiretos são as principais ferramentas que usamos na construção de álgebras. Um tema importante em álgebra universal é o estudo de classes de álgebras do mesmo tipo que sejam fechadas para estas construções.

A uma função que associa a uma classe de álgebras (todas do mesmo tipo) uma classe de álgebras (do mesmo tipo) damos a designação de ***operador***.

Dados operadores O_1 e O_2, escreve-se $O_1 \leq O_2$ se $O_1(\mathbf{K}) \subseteq O_2(\mathbf{K})$, para qualquer classe $\mathbf{K}$ de álgebras. Os operadores podem ser compostos dando origem a novos operadores. Dados operadores O_1 e O_2 e uma classe $\mathbf{K}$ de álgebras, escreve-se $O_1O_2(\mathbf{K})$ em vez de $O_1(O_2(\mathbf{K}))$ e ${O_1}^2(\mathbf{K})$ em vez de $O_1(O_1(\mathbf{K}))$. Um operador O diz-se ***idempotente*** se $O^2 = O$.

Nesta secção o estudo é dedicado a operadores que estão relacionados com as construções de álgebras referidas anteriormente. Dada uma classe $\mathbf{K}$ de álgebras do mesmo tipo, representamos por:

- $S(\mathbf{K})$ a classe de todas as subálgebras de elementos de $\mathbf{K}$;
- $H(\mathbf{K})$ a classe de todas as imagens homomorfas de elementos de $\mathbf{K}$;
- $I(\mathbf{K})$ a classe de todas as imagens isomorfas de elementos de $\mathbf{K}$;
- $P(\mathbf{K})$ a classe de todos os produtos diretos de famílias de elementos de $\mathbf{K}$;
- $P_S(\mathbf{K})$ a classe de todos os produtos subdiretos de famílias de elementos de $\mathbf{K}$.

Para cada um dos operadores O definidos anteriormente, assumimos que $O(\emptyset) = \emptyset$ e verifica-se o seguinte:

- $\mathbf{K} \subseteq O(\mathbf{K})$, para qualquer classe $\mathbf{K}$ de álgebras do mesmo tipo;
- se $\mathbf{K}_1$ e $\mathbf{K}_2$ são classes de álgebras do mesmo tipo tais que $\mathbf{K}_1 \subseteq \mathbf{K}_2$, então $O(\mathbf{K}_1) \subseteq O(\mathbf{K}_2)$.

O resultado seguinte estabelece mais algumas propriedades a respeito destes operadores.

Teorema 3.7.1. *Seja* $\mathbf{K}$ *uma classe de álgebras. Então:*

(i) $SH(\mathbf{K}) \subseteq HS(\mathbf{K})$; *(ii)* $PS(\mathbf{K}) \subseteq SP(\mathbf{K})$; *(iii)* $PH(\mathbf{K}) \subseteq HP(\mathbf{K})$;
(iv) $IS(\mathbf{K}) = SI(\mathbf{K})$; *(v)* $IH(\mathbf{K}) = HI(\mathbf{K})$; *(vi)* $H^2(\mathbf{K}) = H(\mathbf{K})$;
(vii) $I^2(\mathbf{K}) = I(\mathbf{K})$; *(viii)* $S^2(\mathbf{K}) = S(\mathbf{K})$; *(ix)* $(IP)^2(\mathbf{K}) = IP(\mathbf{K})$.

Demonstração. Mostramos as alíneas *(i), (ii) e (iii)*, ficando a prova das restantes alíneas ao cuidado do leitor.

(i) Seja $\mathcal{A} = (A; F) \in SH(\mathbf{K})$. Então existe $\mathcal{B} \in \mathbf{K}$ e um epimorfimo $\alpha : \mathcal{B} \to \mathcal{C}$ tal que $\mathcal{A} \leq \mathcal{C}$. Como α é sobrejetiva, então $\alpha^{\leftarrow}(A)$ é um conjunto não vazio. Seja $\alpha^{\leftarrow}(\mathcal{A})$ a álgebra pré-imagem de $\mathcal{A}$. Uma vez que $\alpha^{\leftarrow}(\mathcal{A}) \leq \mathcal{B}$ e $\alpha(\alpha^{\leftarrow}(\mathcal{A})) = \mathcal{A}$, então $\mathcal{A} \in HS(\mathbf{K})$.

(ii) Seja $\mathcal{A} = (A; F) \in PS(\mathbf{K})$. Então $\mathcal{A} = \prod_{i\in I} \mathcal{A}_i$, onde $\mathcal{A}_i \leq \mathcal{B}_i$, para algum $\mathcal{B}_i \in \mathbf{K}$. Uma vez que $\prod_{i\in I} \mathcal{A}_i \leq \prod_{i\in I} \mathcal{B}_i$, então $\mathcal{A} \in SP(\mathbf{K})$.

(iii) Seja $\mathcal{A} = (A; F) \in PH(\mathbf{K})$. Então existem álgebras $\mathcal{B}_i \in \mathbf{K}$ e epimorfismos $\alpha_i : \mathcal{B}_i \to \mathcal{A}_i$ tais que $\mathcal{A} = \prod_{i\in I} \mathcal{A}_i$. Facilmente se verifica que a aplicação $\alpha : \prod_{i\in I} \mathcal{B}_i \to \prod_{i\in I} \mathcal{A}_i$ definida por $(\alpha(a))(i) = \alpha_i(b(i))$ é um epimorfismo. Logo $\mathcal{A} \in HP(\mathbf{K})$. □

Uma classe $\mathbf{K}$ de álgebras do mesmo tipo diz-se ***fechada*** para um operador O se $O(\mathbf{K}) \subseteq \mathbf{K}$.

Teorema 3.7.2. *Seja* $\mathbf{K}$ *uma classe de álgebras. Se a classe* $\mathbf{K}$ *é fechada para um dos operadores* $O \in \{H, I, S, P, P_S\}$*, então* $O(\mathbf{K}) = \mathbf{K}$.

Demonstração. Imediato. □

Definição 3.7.3. *Seja* $\mathbf{K}$ *uma classe não vazia de álgebras do mesmo tipo. Diz-se que* $\mathbf{K}$ *é uma* ***variedade*** *se é fechada para a formação de imagens homomorfas, subálgebras e produtos diretos.*

Atendendo a que a interseção de uma familia não vazia de variedades de álgebras do mesmo tipo é uma variedade e que a classe formada por todas as álgebras do mesmo tipo é uma variedade, conclui-se que, para qualquer classe $\mathbf{K}$ de álgebras do mesmo tipo, existe a menor variedade que contém $\mathbf{K}$.

Definição 3.7.4. *Seja* $\mathbf{K}$ *uma classe de álgebras do mesmo tipo. Designa-se por* ***variedade gerada por*** $\mathbf{K}$*, e representa-se por* $V(\mathbf{K})$*, a menor variedade que contém* $\mathbf{K}$.

Teorema 3.7.5 (Teorema de Tarski)**.** *Seja* $\mathbf{K}$ *uma classe de álgebras do mesmo tipo. Então* $V(\mathbf{K}) = HSP(\mathbf{K})$.

Demonstração. Por um lado, como $\mathbf{K} \subseteq V(\mathbf{K})$ e $V(\mathbf{K})$ é uma variedade, tem-se

$$HSP(\mathbf{K}) \subseteq HSP(V(\mathbf{K})) = HS(V(\mathbf{K})) = HV(\mathbf{K}) = V(\mathbf{K}).$$

Por outro lado, atendendo ao Teorema 3.7.1, verifica-se que $HHSP(\mathbf{K}) = HSP(\mathbf{K})$; $SHSP(\mathbf{K}) \subseteq HSSP(\mathbf{K}) = HSP(\mathbf{K})$; $PHSP(\mathbf{K}) \subseteq HPSP(\mathbf{K}) \subseteq HSPP(\mathbf{K}) \subseteq HSIPIP(\mathbf{K}) = HSIP(\mathbf{K}) \leq HSHP(\mathbf{K}) \leq HHSP(\mathbf{K}) = HSP(\mathbf{K})$. Logo $HSP(\mathbf{K})$ é uma variedade. Por conseguinte, como $\mathbf{K} \subseteq HSP(\mathbf{K})$, conclui-se que $V(\mathbf{K}) \subseteq HSP(\mathbf{K})$. □

O resultado seguinte, que se trata de uma variante do Teorema de Birkhoff (Teorema 3.6.10), é bastante útil no estudo de variedades.

Teorema 3.7.6. *Seja* $\mathbf{K}$ *uma variedade. Então toda a álgebra de* $\mathbf{K}$ *é isomorfa a um produto subdireto de álgebras subdiretamente irredutíveis de* $\mathbf{K}$.

Corolário 3.7.7. *Toda a variedade é gerada pelas suas álgebras subdiretamente irredutíveis.*

3.8 Termos, álgebras livres

Nas secções anteriores foram abordados alguns processos algébricos para a construção de álgebras e foi dada especial atenção ao estudo de classes de álgebras que são fechadas para alguns desses processos de construção, em particular, estudaram-se classes de álgebras fechadas para a formação de subálgebras, para a formação de imagens homomorfas e para a formação de produtos diretos. Atendendo a que a maioria das álgebras que se estudam são definidas por operações que satisfazem determinadas identidades, torna-se importante averiguar se os processos de construção referidos anteriormente também preservam as identidades que são satisfeitas pelas álgebras de uma determinada classe. No sentido de se fazer tal estudo, começamos por introduzir os conceitos de termo e de álgebras livres, conceitos estes que serão posteriormente utilizados para definir identidades e estabelecer a ligação existente entre a abordagem algébrica e a abordagem equacional adotada no estudo das álgebras.

Definição 3.8.1. *Sejam* (O, τ) *um tipo algébrico e* X *um conjunto de objetos designados por* ***variáveis****. O* ***conjunto*** $T(X)$ ***dos termos de tipo*** (O, τ) ***sobre*** X *é o menor conjunto tal que:*

(i) $X \cup O_0 \subseteq T(X)$.

(ii) Se $(t_1, \ldots, t_n) \in (T(X))^n$ *e* $f \in O_n$*, então* $f(t_1, \ldots, t_n) \in T(X)$.

Note-se que $T(X) \neq \emptyset$ se e só se $X \cup O_0 \neq \emptyset$. Para um símbolo de operação binário $\cdot$ é usual adotar a notação $t_1 \cdot t_2$, em vez de $\cdot(t_1, t_2)$. Dado $t \in T(X)$, escreve-se $t(x_1, \ldots, x_n)$ para indicar que as variáveis que ocorrem no termo t pertencem a $\{x_1, \ldots, x_n\}$. Um termo t diz-se n-ário se o número de variáveis que ocorrem em t é menor ou igual a n.

Exemplo 3.8.2.
(1) Sejam $X = \{x, y, z\}$ e (O, τ) o tipo algébrico tal que O é constituído por um único símbolo de operação binário $\cdot$. Então

$$x,\ y,\ z,\ x \cdot y,\ y \cdot z,\ x \cdot (y \cdot z),\ (x \cdot y) \cdot z$$

são exemplos de alguns termos sobre X.

(2) Sejam $X = \{x, y, z\}$ e (O, τ) o tipo algébrico tal que O é constituído por dois símbolos de operação binários $\cdot$ e $+$. Então

$$x,\ y,\ z,\ x \cdot (y + z),\ (x \cdot y) + (x \cdot z)$$

são alguns dos termos sobre X.

(3) Os polinómios reais são termos de tipo (O, τ), onde O é constituído por três símbolos de operação binários, $+$, $\cdot$, $-$, e por um símbolo de operação nulário r, para cada $r \in \mathbb{R}$.

Os polinómios reais de grau n, $n \in \mathbb{N}_0$, são usualmente associados a funções de $\mathbb{R}^n$ em $\mathbb{R}$. A associação de termos a funções pode ser generalizada a qualquer termo.

Definição 3.8.3. *Dado um termo $t(x_1, \ldots, x_n)$ de tipo (O, τ) sobre um conjunto X e dada uma álgebra $\mathcal{A} = (A; F)$ de tipo (O, τ), define-se a função $t^{\mathcal{A}} : A^n \to A$ da seguinte forma:*

(1) se t é uma variável x_i, então

$$t^{\mathcal{A}}(a_1, \ldots, a_n) = a_i,$$

para $(a_1, \ldots, a_n) \in A^n$.

(2) se t é da forma $f(t_1(x_1, \ldots, x_n), \ldots, t_k(x_1, \ldots, x_n))$, onde $f \in O_k$, então

$$t^{\mathcal{A}}(a_1, \ldots, a_n) = f^{\mathcal{A}}({t_1}^{\mathcal{A}}(a_1, \ldots, a_n), \ldots, {t_k}^{\mathcal{A}}(a_1, \ldots, a_n)),$$

para quaisquer $(a_1, \ldots, a_n) \in A^n$.

A função $t^{\mathcal{A}}$ designa-se por ***função termo em $\mathcal{A}$ induzida por*** *t.*

O resultado seguinte, cuja prova fica como exercício, estabelece algumas propriedades importantes relativas a funções termo; em particular, estabelece que as funções termo se comportam de forma análoga às operações fundamentais de uma álgebra no que respeita a congruências e a homomorfismos.

Teorema 3.8.4. *Para qualquer tipo algébrico (O,τ) e para quaisquer álgebras $\mathcal{A}=(A;F)$ e $\mathcal{B}=(B;G)$ de tipo (O,τ), tem-se o seguinte:*

(i) Se t é um termo n-ário de tipo (O,τ), $\theta \in \operatorname{Con}\mathcal{A}$ e $(a_i,b_i)\in\theta$, para qualquer $i\in\{1,\ldots,n\}$, então

$$t^{\mathcal{A}}(a_1,\ldots,a_n)\,\theta\, t^{\mathcal{A}}(b_1,\ldots,b_n).$$

(ii) Se t é um termo n-ário de tipo (O,τ) e $\alpha:\mathcal{A}\to\mathcal{B}$ é um homomorfismo, então

$$\alpha(t^{\mathcal{A}}(a_1,\ldots,a_n)) = t^{\mathcal{B}}(\alpha(a_1),\ldots,\alpha(a_n)),$$

para quaisquer $(a_1,\ldots,a_n)\in A^n$.

(iii) Seja S um subconjunto de A. Então

$$Sg^{\mathcal{A}}(S) = \{t^{\mathcal{A}}(a_1,\ldots,a_n) : t \text{ é um termo } n\text{-ário de tipo } (O,\tau),\ n\in\mathbb{N}_0, (a_1,\ldots,a_n)\in S^n\}.$$

Dado um tipo algébrico (O,τ) e um conjunto X, define-se de forma natural uma álgebra de tipo (O,τ) que tem como universo o conjunto de termos $T(X)$.

Definição 3.8.5. *Sejam (O,τ) um tipo algébrico e X um conjunto tal que $X\cup O_0\neq\emptyset$. Designa-se por* ***álgebra dos termos de tipo*** *(O,τ)* ***sobre*** *X, e representa-se por $\mathcal{T}(X)$, a álgebra $\mathcal{T}(X)=(T(X);(f^{\mathcal{T}(X)})_{f\in O})$ tal que, para quaisquer $n\in\tau(O)$ e $f\in O_n$, $f^{\mathcal{T}(X)}:T(X)^n\to T(X)$ é a operação definida por*

$$f^{\mathcal{T}(X)}(t_1,\ldots,t_n) = f(t_1,\ldots,t_n),$$

para quaisquer $(t_1,\ldots,t_n)\in(T(X))^n$.

Claramente, a álgebra $\mathcal{T}(X)$ é gerada por X. Além disso, a álgebra $\mathcal{T}(X)$ é, a menos de isomorfismo, determinada por $|X|$.

Teorema 3.8.6. *Sejam (O,τ) um tipo algébrico e X e Y conjuntos tais que $X\cup O_0\neq\emptyset$ e $|X|=|Y|$. Então $\mathcal{T}(X)\cong\mathcal{T}(Y)$.*

Demonstração. Sejam X e Y são conjuntos tais que $X\cup O_0\neq\emptyset$ e $|X|=|Y|$. Uma vez que existe uma bijeção $\alpha:X\to Y$, é simples verificar que a aplicação $\overline{\alpha}:T(X)\to T(Y)$ definida por

(i) $\overline{\alpha}(x)=\alpha(x)$, para todo $x\in X$,

(ii) $\overline{\alpha}(f(t_1,\ldots,t_n)) = f^{\mathcal{T}(Y)}(\overline{\alpha}(t_1),\ldots,\overline{\alpha}(t_n))$, para quaisquer $n\in\tau(O)$, $f\in O_n$ e $(t_1,\ldots,t_n)\in(T(X))^n$,

é um isomorfismo de $\mathcal{T}(X)$ em $\mathcal{T}(Y)$. □

Definição 3.8.7. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O,τ), $\mathcal{U}=(U;F)$ *uma álgebra de tipo* (O,τ) *e* X *um subconjunto de* U. *Diz-se que a álgebra* $\mathcal{U}$ *é* ***livre para*** $\mathbf{K}$ ***sobre*** X *se:*

(i) $\mathcal{U}$ *é gerada por* X*;*

(ii) para cada álgebra $\mathcal{A}\in\mathbf{K}$ *e para cada aplicação* $\alpha: X\to A$, *existe um homomorfismo* $\overline{\alpha}:\mathcal{U}\to\mathcal{A}$ *que estende* α *(i.e.,* $\overline{\alpha}(x)=\alpha(x)$, *para todo* $x\in X$*).*

O conjunto X *diz-se um conjunto de* ***geradores livres*** *de* U *e a álgebra* U *diz-se* ***livremente gerada por*** X**.**

Lema 3.8.8. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O,τ), $\mathcal{U}=(U;F)$ *uma álgebra de tipo* (O,τ) *e* X *um subconjunto de* U. *Se a álgebra* $\mathcal{U}$ *é livre para* $\mathbf{K}$ *sobre* X, *então, para qualquer álgebra* $\mathcal{A}=(A;G)\in\mathbf{K}$ *e para qualquer aplicação* $\alpha: X\to A$, *existe um único homomorfismo* $\overline{\alpha}:\mathcal{U}\to\mathcal{A}$ *que estende* α.

Demonstração. A existência de $\overline{\alpha}$ é garantida pelo facto de $\mathcal{U}$ ser livre para $\mathbf{K}$ sobre X. A unicidade de $\overline{\alpha}$ resulta de $\mathcal{U}$ ser gerada por X. □

Teorema 3.8.9. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O,τ), $\mathcal{U}_1=(U_1;F)$, $\mathcal{U}_2=(U_2;G)$ *álgebras de* $\mathbf{K}$ *e* X *e* Y *subconjuntos de* U_1 *e* U_2, *respetivamente. Se* $\mathcal{U}_1$ *e* $\mathcal{U}_2$ *são álgebras livres para* $\mathbf{K}$ *sobre* X *e* Y, *respetivamente, e* $|X|=|Y|$, *então* $\mathcal{U}_1\cong\mathcal{U}_2$.

Demonstração. Assumindo que $|X|=|Y|$, existe uma bijeção $h: X\to Y$. Por conseguinte,

$$h_1:\begin{array}{ccc} X & \to & U_2\\ x & \mapsto & h(x)\end{array} \quad \text{e} \quad h_2:\begin{array}{ccc} Y & \to & U_1\\ y & \mapsto & h^{-1}(y)\end{array}$$

são aplicações. Uma vez que $\mathcal{U}_2\in\mathbf{K}$ e $\mathcal{U}_1$ é uma álgebra livre para $\mathbf{K}$ sobre X, existe um homomorfismo $\overline{h}_1:\mathcal{U}_1\to\mathcal{U}_2$ que estende h_1. De forma análoga, uma vez que $\mathcal{U}_1\in\mathbf{K}$ e $\mathcal{U}_2$ é uma álgebra livre para $\mathbf{K}$ sobre Y, existe um homomorfismo $\overline{h}_2:\mathcal{U}_2\to\mathcal{U}_1$ que estende h_2. Assim, $\overline{h}_2\circ\overline{h}_1$ é um endomorfismo de $\mathcal{U}_1$ que estende a aplicação identidade id_X. Obviamente, $id_{\mathcal{U}_1}$ também é um homomorfismo que estende id_X. Então, pelo Lema 3.8.8 segue que $\overline{h}_2\circ\overline{h}_1=id_{\mathcal{U}_1}$. De forma análoga, conclui-se que $\overline{h}_1\circ\overline{h}_2=id_{\mathcal{U}_2}$. Por conseguinte, $\overline{h}_1$ e $\overline{h}_2$ são isomorfismos e, portanto, $\mathcal{U}_1\cong\mathcal{U}_2$. □

Teorema 3.8.10. *Sejam* (O,τ) *um tipo algébrico,* $\mathbf{K}$ *a classe de todas as álgebras de tipo* (O,τ) *e* X *um conjunto tal que* $X\cup O_0\neq\emptyset$. *Então a álgebra* $\mathcal{T}(X)$ *é livre para* $\mathbf{K}$ *sobre* X.

Demonstração. Já foi observado anteriormente que X gera $\mathcal{T}(X)$. Também se prova que, para cada álgebra $\mathcal{A}=(A;F)\in\mathbf{K}$ e para cada função $\alpha: X\to A$, existe um homomorfismo $\overline{\alpha}:\mathcal{T}(X)\to\mathcal{A}$ que estende α. De facto, é simples verificar que a aplicação $\overline{\alpha}: T(X)\to A$ definida recursivamente por

(i) $\overline{\alpha}(x) = \alpha(x)$, para todo $x \in X$,

(ii) $\overline{\alpha}(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(\overline{\alpha}(t_1), \ldots, \overline{\alpha}(t_n))$, para quaisquer $n \in \tau(O)$, $f \in O_n$ e $(t_1, \ldots, t_n) \in (T(X))^n$,

é um homomorfismo de $\mathcal{T}(X)$ em $\mathcal{A}$ que estende α. □

Teorema 3.8.11. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ), X *um conjunto de variáveis tal que* $X \cup O_0 \neq \emptyset$,

$$\begin{aligned} \Phi_{\mathbf{K}}(X) &= \{\phi \in \operatorname{Con} \mathcal{T}(X) \mid \mathcal{T}(X)/\phi \in IS(\mathbf{K})\} \\ &= \{\ker \varphi \mid \varphi : \mathcal{T}(X) \to \mathcal{A} \text{ é um homomorfismo, para algum } \mathcal{A} \in \mathbf{K}\} \end{aligned}$$

e

$$\theta_{\mathbf{K}}(X) = \bigcap \Phi_{\mathbf{K}}(X).$$

Então $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ *é uma álgebra livre para* $\mathbf{K}$ *sobre* $X/\theta_{\mathbf{K}}(X)$.

Demonstração. Facilmente se verifica que a álgebra $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ é gerada por $X/\theta_{\mathbf{K}}(X)$. Resta mostrar que, para cada álgebra $\mathcal{A} = (A; F) \in \mathbf{K}$ e para cada aplicação $\alpha : X/\theta_{\mathbf{K}}(X) \to A$, existe um homomorfismo $\overline{\alpha}$ de $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ em $\mathcal{A}$ que estende α. Para tal, considere-se a aplicação natural $\pi_{\theta_{\mathbf{K}}(X)} : X \to X/\theta_{\mathbf{K}}(X)$, definida por $\pi_{\theta_{\mathbf{K}}(X)}(x) = [x]_{\theta_{\mathbf{K}}(X)}$, para cada $x \in X$. Então $\alpha \circ \pi_{\theta_{\mathbf{K}}(X)}$ é uma aplicação de X em A. Como $\mathcal{T}(X)$ é uma álgebra livre para $\mathbf{K}$ sobre X, existe um homomorfismo $\beta : \mathcal{T}(X) \to \mathcal{A}$ que estende $\alpha \circ \pi_{\theta_{\mathbf{K}}(X)}$. Atendendo à definição de $\theta_{\mathbf{K}}(X)$, é imediato que $\theta_{\mathbf{K}}(X) \subseteq \ker \beta$ (pois $\ker \beta \in \Phi_{\mathbf{K}}(X)$). A correspondência $\overline{\alpha} : T(X)/\theta_{\mathbf{K}}(X) \to A$ definida por $\overline{\alpha}([t]_{\theta_{\mathbf{K}}(X)}) = \beta(t)$ é um homomorfismo tal que $\overline{\alpha} \circ \pi_{\theta_{\mathbf{K}}(X)} = \beta$. Além disso, para todo $[t]_{\theta_{\mathbf{K}}(X)} \in X/\theta_{\mathbf{K}}(X)$,

$$\begin{aligned} \overline{\alpha}([t]_{\theta_{\mathbf{K}}(X)}) &= \beta(t) \\ &= \alpha \circ \pi_{\theta_{\mathbf{K}}(X)}(t) \\ &= \alpha([t]_{\theta_{\mathbf{K}}(X)}) \end{aligned}$$

e, portanto, $\overline{\alpha}$ estende α. Desta forma, ficou provado que $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ é uma álgebra livre para $\mathbf{K}$ sobre $X/\theta_{\mathbf{K}}(X)$. □

Definição 3.8.12. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ), X *um conjunto de variáveis tal que* $X \cup O_0 \neq \emptyset$ *e* $\theta_{\mathbf{K}}(X)$ *a congruência em* $\mathcal{T}(X)$ *dada por*

$$\theta_{\mathbf{K}}(X) = \bigcap \{\phi \in \operatorname{Con} \mathcal{T}(X) \mid T(X)/\phi \in IS(\mathbf{K})\}.$$

À álgebra $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ *dá-se a designação de* ***álgebra*** $\mathbf{K}$***-livre*** *sobre* $X/\theta_{\mathbf{K}}(X)$.

Observe-se que, dada uma classe de álgebras $\mathbf{K}$ de tipo (O, τ) e dado um conjunto X tal que $X \cup O_0 \neq \emptyset$:

(1) Se $\mathbf{K} = \emptyset$ ou $\mathbf{K}$ tem apenas álgebras triviais, então $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ é uma álgebra trivial, uma vez que $\theta_{\mathbf{K}}(X) = \nabla_{T(X)}$.

(2) Se $\mathbf{K}$ tem uma álgebra não trivial $\mathcal{A}$ e $T(X)$ existe, então $X \cap [x]_{\theta_{\mathbf{K}}(X)} = \{x\}$, uma vez que elementos distintos x, y de X podem ser separados por algum homomorfismo $\alpha : \mathcal{T}(X) \to \mathcal{A}$; neste caso, tem-se $|X/\theta_{\mathbf{K}}(X)| = |X|$.

(3) Se $\mathbf{K}$ é a classe de todas as álgebras de um dado tipo (O, τ) e X é um conjunto tal que $X \cup O_0 \neq \emptyset$, então $\mathcal{T}(X) \cong \mathcal{T}(X)/\theta_{\mathbf{K}}(X)$, uma vez que $\theta_{\mathbf{K}}(X) = \triangle_{T(X)}$.

Dada uma classe $\mathbf{K}$ de álgebras de tipo (O, τ) e dado um conjunto X, a álgebra $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ é, a menos de isomorfismo, determinada por $\mathbf{K}$ e por $|X|$.

Teorema 3.8.13. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* $\tau = (O, \tau)$ *e* X *e* Y *conjuntos de variáveis tais que* $X \cup O_0 \neq \emptyset$ *e* $|X| = |Y|$. *Então*

$$\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \cong \mathcal{T}(Y)/\theta_{\mathbf{K}}(Y).$$

Demonstração. Sejam $\mathbf{K}$ uma classe de álgebras de tipo $\tau = (O, \tau)$ e X e Y conjuntos de variáveis tais que $X \cup O_0 \neq \emptyset$ e $|X| = |Y|$. Então, pelo Teorema 3.8.6 sabe-se que existe um isomorfismo $i : \mathcal{T}(X) \to \mathcal{T}(Y)$. Fica ao cuidado do leitor a verificação de que a correspondência α de $T(X)/\theta_{\mathbf{K}}(X)$ em $T(Y)/\theta_{\mathbf{K}}(Y)$ definida por, $\alpha([t]_{\theta_{\mathbf{K}}(X)}) = [i(t)]_{\theta_{\mathbf{K}}(Y)}$, para todo $t \in T(X)$, é um isomorfismo de $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ em $\mathcal{T}(Y)/\theta_{\mathbf{K}}(Y)$. □

Teorema 3.8.14. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ) *e* $\mathcal{A} = (A; F) \in \mathbf{K}$. *Então, para qualquer conjunto de variáveis* X *tal que* $|X| \geq |A|$, *tem-se* $\mathcal{A} \in H(\{\mathcal{T}(X)/\theta_{\mathbf{K}}(X)\})$.

Demonstração. Seja X um conjunto de variáveis tal que $|X| \geq |A|$. Então $|X/\theta_{\mathbf{K}}(X)| \geq |A|$, pelo que é possível definir uma aplicação sobrejetiva de $X/\theta_{\mathbf{K}}(X)$ em A; seja $\alpha : X/\theta_{\mathbf{K}}(X) \to A$ uma dessas aplicações. Uma vez que $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ é uma álgebra livre para $\mathbf{K}$ sobre $X/\theta_{\mathbf{K}}(X)$, existe um homomorfismo $\overline{\alpha} : \mathcal{T}(X)/\theta_{\mathbf{K}}(X) \to \mathcal{A}$ que estende α. Logo $\mathcal{A} \in H(\{\mathcal{T}(X)/\theta_{\mathbf{K}}(X)\})$. □

Lema 3.8.15. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ) *e* X *um conjunto de variáveis. Então* $\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \in ISP(\mathbf{K})$.

Demonstração. Sejam $S = \{\phi \in \operatorname{Con} \mathcal{T}(X) \mid \mathcal{T}(X)/\phi \in IS(\mathbf{K})\}$,

$$\mathcal{B} = \prod_{\phi \in S} \mathcal{T}(X)/\phi$$

e

$$\alpha : T(X)/\theta_{\mathbf{K}}(X) \to \prod_{\phi \in S} T(X)/\phi$$

a correspondência definida por

$$\alpha([t]_{\theta_{\mathbf{K}}(X)})(\phi) = [t]_{\phi},$$

para cada $\phi \in S$ e para cada $t \in T(X)$. Facilmente se verifica que α é um monomorfismo de $\mathcal{T}(X)/\theta_{\mathbf{K}}(X)$ em $\mathcal{B}$. Logo $\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \cong \alpha(\mathcal{T}(X)/\theta_{\mathbf{K}}(X))$. Então, uma vez que $\alpha(\mathcal{T}(X)/\theta_{\mathbf{K}}(X))$ é uma subálgebra de $\mathcal{B}$ e $\mathcal{B} \in PIS(\mathbf{K})$, tem-se que $\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \in ISPIS(\mathbf{K})$. Por conseguinte, do Teorema 3.7.1 segue que $\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \in ISP(\mathbf{K})$. □

3.9 Identidades, Teorema de Birkhoff

Um dos mais conhecidos teoremas de Birkhoff estabelece que as classes de álgebras definidas por identidades são precisamente as classes de álgebras que são fechadas para a formação de imagens homomorfas, subálgebras e produtos diretos. Nesta secção estudamos identidades e a sua relação com álgebras livres, no sentido de se estabelecer o referido teorema.

Definição 3.9.1. *Sejam (O, τ) um tipo algébrico e X um conjunto de variáveis.*

*(1) Uma **identidade de tipo** (O, τ) **sobre** X é uma expressão da forma $p \approx q$, onde $p, q \in T(X)$. Representa-se por* $\mathrm{Id}(X)$ *o conjunto de todas as identidades de tipo (O, τ) sobre X.*

*(2) Dada uma álgebra $\mathcal{A}$ de tipo (O, τ), diz-se que **a álgebra $\mathcal{A}$ satisfaz a identidade** $p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$ se, para quaisquer $a_1, \ldots, a_n \in A$, $p^{\mathcal{A}}(a_1, \ldots, a_n) = q^{\mathcal{A}}(a_1, \ldots, a_n)$. Neste caso, diz-se que a identidade **é verdadeira em $\mathcal{A}$** ou que se **verifica em $\mathcal{A}$**, e escreve-se*

$$A \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$$

ou, mais abreviadamente, $A \models p \approx q$.

*(3) Se Σ é um conjunto de identidades, diz-se que $\mathcal{A}$ **satisfaz** Σ, e escreve-se $A \models \Sigma$, se $A \models p \approx q$, para qualquer $p \approx q \in \Sigma$.*

*(4) Uma classe de álgebras $\mathbf{K}$ **satisfaz uma identidade** $p \approx q$, e escreve-se $\mathbf{K} \models p \approx q$, se cada uma das álgebras de $\mathbf{K}$ satisfaz $p \approx q$. Diz-se que $\mathbf{K}$ **satisfaz um conjunto de identidades** Σ, e escreve-se $\mathbf{K} \models \Sigma$, se $\mathbf{K}$ satisfaz cada uma das identidades de Σ. O conjunto de todas as identidades de tipo (O, τ) sobre X que são satisfeitas por $\mathbf{K}$ é representado por* $\mathrm{Id}_{\mathbf{K}}(X)$*; i.e.,* $\mathrm{Id}_{\mathbf{K}}(X) = \{p \approx q \in \mathrm{Id}(X) : \mathbf{K} \models p \approx q\}$.

Lema 3.9.2. *Sejam $\mathbf{K}$ uma classe de álgebras de tipo (O, τ) e $p \approx q$ uma identidade de tipo (O, τ) sobre um conjunto de variáveis X. Então $\mathbf{K} \models p \approx q$ se e só se para cada álgebra $\mathcal{A} \in \mathbf{K}$ e cada homomorfismo $\alpha : \mathcal{T}(X) \to \mathcal{A}$ se tem $\alpha(p) = \alpha(q)$.*

Demonstração. ($\Rightarrow$) Sejam $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n) \in T(X)$. Suponhamos que $\mathbf{K} \models p \approx q$. Então, para qualquer álgebra $\mathcal{A} \in \mathbf{K}$ e qualquer homomorfismo $\alpha : \mathcal{T}(X) \to \mathcal{A}$, tem-se

$$p^{\mathcal{A}}(\alpha(x_1), \ldots, \alpha(x_n)) = q^{\mathcal{A}}(\alpha(x_1), \ldots, \alpha(x_n))$$

e, uma vez que

$$\begin{array}{ll} & p^{\mathcal{A}}(\alpha(x_1), \ldots, \alpha(x_n)) = q^{\mathcal{A}}(\alpha(x_1), \ldots, \alpha(x_n)) \\ \Rightarrow & \alpha(p^{\mathcal{T}(X)}(x_1, \ldots, x_n)) = \alpha(q^{\mathcal{T}(X)}(x_1, \ldots, x_n)) \\ \Rightarrow & \alpha(p(x_1, \ldots, x_n)) = \alpha(q(x_1, \ldots, x_n)), \\ \Rightarrow & \alpha(p) = \alpha(q), \end{array}$$

segue que $\alpha(p) = \alpha(q)$.

($\Leftarrow$) Sejam $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n) \in T(X)$. Pretende-se mostrar que para qualquer $\mathcal{A} \in \mathbf{K}$ e quaisquer $a_1, \ldots, a_n \in A$, $p^{\mathcal{A}}(a_1, \ldots, a_n) = q^{\mathcal{A}}(a_1, \ldots, a_n)$. Ora, considerando uma aplicação $\alpha' : X \to A$ tal que $\alpha'(x_i) = a_i$, para todo $i \in \{1, \ldots, n\}$, sabe-se que existe um homomorfismo $\alpha : \mathcal{T}(X) \to A$ que estende α, uma vez que $\mathcal{T}(X)$ é livre para $\mathbf{K}$ sobre X. Então $\alpha(x_i) = \alpha'(x_i) = a_i$, donde

$$\begin{array}{rcl} p^{\mathcal{A}}(a_1, \ldots, a_n) & = & p^{\mathcal{A}}(\alpha(x_1), \ldots, \alpha(x_n)) \\ & = & \alpha(p^{\mathcal{T}(X)}(x_1, \ldots, x_n)) \\ & = & \alpha(p(x_1, \ldots, x_n)) \\ & = & \alpha(p) \\ & = & \alpha(q) \\ & = & \alpha(q(x_1, \ldots, x_n)) \\ & = & \alpha(q^{\mathcal{T}(X)}(x_1, \ldots, x_n)) \\ & = & q^{\mathcal{A}}(\alpha(x_1), \ldots, \alpha(x_n)) \\ & = & q^{\mathcal{A}}(a_1, \ldots, a_n). \end{array}$$

Logo $\mathbf{K} \models p \approx q$. □

Lema 3.9.3. *Para qualquer classe $\mathbf{K}$ de álgebras de tipo (O, τ), as classes $\mathbf{K}$, $I(\mathbf{K})$, $S(\mathbf{K})$, $H(\mathbf{K})$, $P(\mathbf{K})$ e $HSP(\mathbf{K})$ satisfazem as mesmas identidades sobre qualquer conjunto de variáveis X.*

Demonstração. Claramente, $\mathbf{K}$ e $I(\mathbf{K})$ satisfazem as mesmas identidades. No que respeita às restantes classes, e uma vez que

$$\mathbf{K} \subseteq S(\mathbf{K}), \quad \mathbf{K} \subseteq H(\mathbf{K}) \quad \text{e} \quad \mathbf{K} \subseteq P(\mathbf{K}),$$

temos $\mathrm{Id}_{S(\mathbf{K})}(X) \subseteq \mathrm{Id}_{\mathbf{K}}(X)$, $\mathrm{Id}_{H(\mathbf{K})}(X) \subseteq \mathrm{Id}_{\mathbf{K}}(X)$ e $\mathrm{Id}_{P(\mathbf{K})}(X) \subseteq \mathrm{Id}_{\mathbf{K}}(X)$. No sentido de provar as inclusões contrárias, suponhamos que

$$\mathbf{K} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n).$$

Então, para qualquer álgebra $\mathcal{A} \in \mathbf{K}$ e para quaisquer $a_1, \ldots, a_n \in A$,

$$p^{\mathcal{A}}(a_1, \ldots, a_n) = q^{\mathcal{A}}(a_1, \ldots, a_n).$$

Assim, se $\mathcal{B}$ é subálgebra de alguma álgebra $\mathcal{A} \in \mathbf{K}$, segue que, para quaisquer $b_1, \ldots, b_n \in B \subseteq A$,

$$p^{\mathcal{A}}(b_1, \ldots, b_n) = q^{\mathcal{A}}(b_1, \ldots, b_n),$$

donde

$$p^{\mathcal{B}}(b_1, \ldots, b_n) = q^{\mathcal{B}}(b_1, \ldots, b_n)$$

e, portanto,

$$\mathcal{B} \models p \approx q.$$

Logo

$$\mathrm{Id}_{S(\mathbf{K})}(X) = \mathrm{Id}_{\mathbf{K}}(X).$$

Provemos, agora, que $\mathrm{Id}_{\mathbf{K}}(X) \subseteq \mathrm{Id}_{H(\mathbf{K})}(X)$. Ora, se $\mathcal{B} \in H(\mathbf{K})$, então existe um homomorfismo sobrejetivo $h : \mathcal{A} \to \mathcal{B}$, para alguma álgebra $\mathcal{A} \in \mathbf{K}$. Por conseguinte, para quaisquer $b_1, \ldots, b_n \in B$, existem $a_1, \ldots, a_n \in A$ tais que

$$\alpha(a_1) = b_1, \ldots, \alpha(a_n) = b_n.$$

Então, como

$$p^{\mathcal{A}}(a_1, \ldots, a_n) = q^{\mathcal{A}}(a_1, \ldots, a_n),$$

tem-se

$$\alpha(p^{\mathcal{A}}(a_1, \ldots, a_n)) = \alpha(q^{\mathcal{A}}(a_1, \ldots, a_n)),$$

pelo que

$$p^{\mathcal{B}}(b_1, \ldots, b_n) = q^{\mathcal{B}}(b_1, \ldots, b_n).$$

Logo

$$\mathcal{B} \models p \approx q.$$

Assim,

$$\mathrm{Id}_{H(\mathbf{K})}(X) = \mathrm{Id}_{\mathbf{K}}(X).$$

Por último, consideremos $\mathcal{B} \in P(\mathbf{K})$. Então $\mathcal{B} = \prod_{i \in I} \mathcal{A}_i$, para alguma família $(\mathcal{A}_i)_{i \in I}$ de álgebras de $\mathbf{K}$. Atendendo a que, para cada $i \in I$, $\mathcal{A}_i \in \mathbf{K}$, segue que, para quaisquer $a_1, \ldots, a_n \in \prod_{i \in I} A_i$,

$$p^{\mathcal{A}_i}(a_1(i), \ldots, a_n(i)) = q^{\mathcal{A}_i}(a_1(i), \ldots, a_n(i)),$$

donde

$$p^{\mathcal{B}}(a_1, \ldots, a_n)(i) = q^{\mathcal{B}}(a_1, \ldots, a_n)(i),$$

para todo $i \in I$ e, portanto,

$$p^{\mathcal{B}}(a_1, \ldots, a_n) = q^{\mathcal{B}}(a_1, \ldots, a_n).$$

Logo

$$\mathcal{B} \models p \approx q.$$

Assim,

$$\mathrm{Id}_{P(\mathbf{K})}(X) = \mathrm{Id}_{\mathbf{K}}(X).$$

Atendendo ao que foi provado anteriormente é imediato que $HSP(\mathbf{K})$ satisfaz as mesmas identidades que $\mathbf{K}$. □

Teorema 3.9.4. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O,τ)*,* X *um conjunto de variáveis e* $p,q \in T(X)$ *de tipo* (O,τ)*. Então as afirmações seguintes são equivalentes:*

(i) $\mathbf{K} \models p \approx q$.

(ii) $\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \models p \approx q$.

(iii) $(p,q) \in \theta_{\mathbf{K}}(X)$

Demonstração. Sejam $p = p(x_1,\ldots,x_n), q = q(x_1,\ldots,x_n) \in T(X)$.

(i) $\Rightarrow$ (iii) Assumindo que $\mathbf{K} \models p \approx q$, então

$$\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \models p \approx q,$$

pois $\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \in ISP(\mathbf{K})$.

(ii) $\Rightarrow$ (iii) Suponhamos que $\mathcal{T}(X)/\theta_{\mathbf{K}}(X) \models p \approx q$. Então, para qualquer homomorfismo $\alpha : \mathcal{T}(X) \to \mathcal{T}(X)/\theta_{\mathbf{K}}(X)$, $\alpha(p) = \alpha(q)$. Em particular, considerando o homomorfismo natural $\pi_{\theta_{\mathbf{K}}(X)} : \mathcal{T}(X) \to \mathcal{T}(X)/\theta_{\mathbf{K}}(X)$, temos

$$\pi_{\theta_{\mathbf{K}}(X)}(p) = \pi_{\theta_{\mathbf{K}}(X)}(q)$$

e, portanto,

$$[p]_{\theta_{\mathbf{K}}(X)} = [q]_{\theta_{\mathbf{K}}(X)}.$$

Logo $(p,q) \in \theta_{\mathbf{K}}(X)$.

(ii) $\Rightarrow$ (iii) Da definição de $\theta_{\mathbf{K}}(X)$ segue que, para qualquer álgebra $\mathcal{A} \in \mathbf{K}$ e para qualquer homomorfismo $\varphi : \mathcal{T}(X) \to \mathcal{A}$, $\theta_{\mathbf{K}}(X) \subseteq \ker\varphi$.
Assim, se $(p,q) \in \theta_{\mathbf{K}}(X)$, tem-se $\varphi(p) = \varphi(q)$ para qualquer homomorfismo $\varphi : \mathcal{T}(X) \to \mathcal{A}$, e pelo Teorema 3.9.2 conclui-se que $\mathbf{K} \models p \approx q$. □

Corolário 3.9.5. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O,τ)*,* X *um conjunto de variáveis e* $p,q \in T(X)$*. Então, para qualquer conjunto de variáveis* Y *tal que* $|Y| \geq |X|$*, tem-se*

$$\mathbf{K} \models p \approx q \text{ se e só se } \mathcal{T}(Y)/\theta_{\mathbf{K}}(Y) \models p \approx q.$$

Demonstração. ($\Rightarrow$) Esta implicação é imediata, uma vez que $\mathcal{T}(Y)/\theta_{\mathbf{K}}(Y) \in ISP(\mathbf{K})$.

($\Leftarrow$) Consideremos um conjunto de variáveis X_0 tal que $X \subseteq X_0$ e $|X_0| = |Y|$. Então $p,q \in T(X_0)$ e

$$\mathcal{T}(X_0)/\theta_{\mathbf{K}}(X_0) \cong \mathcal{T}(Y)/\theta_{\mathbf{K}}(Y).$$

Consequentemente, atendendo aos teoremas 3.9.3 e 3.9.4,

$$\mathcal{T}(Y)/\theta_{\mathbf{K}}(Y) \models p \approx q \;\Rightarrow\; \mathcal{T}(X_0)/\theta_{\mathbf{K}}(X_0) \models p \approx q \;\Rightarrow\; \mathbf{K} \models p \approx q.$$

□

Corolário 3.9.6. *Sejam* $\mathbf{K}$ *uma classe de álgebras de tipo* (O,τ) *e* X *um conjunto de variáveis. Então, para qualquer conjunto infinito de variáveis* Y*, tem-se*

$$\mathrm{Id}_{\mathbf{K}}(X) = \mathrm{Id}_{\{\mathcal{T}(Y)/\theta_{\mathbf{K}}(Y)\}}(X).$$

Demonstração. Seja $p \approx q \in \mathrm{Id}_{\mathbf{K}}(X)$, onde $p = p(x_1, \ldots, x_n)$ e $q = (x_1, \ldots, x_n)$. Como $p, q \in T(\{x_1, \ldots, x_n\})$ e $|\{x_1, \ldots, x_n\}| \leq |Y|$, então pelo Corolário 3.9.5 tem-se que

$$\mathbf{K} \models p \approx q \text{ sse } \mathcal{T}(Y)/\theta_{\mathbf{K}}(Y) \models p \approx q.$$

□

Definição 3.9.7. *Dado um conjunto Σ de identidades de tipo (O, τ), define-se $M(\Sigma)$ como sendo a classe de todas as álgebras que satisfazem Σ. Uma classe $\mathbf{K}$ de álgebras de tipo (O, τ) diz-se uma* ***classe equacional*** *se existe um conjunto de identidades Σ tal que $\mathbf{K} = M(\Sigma)$. Neste caso, diz-se que a classe $\mathbf{K}$ é* ***definida*** *ou* ***axiomatizada*** *por Σ.*

Lema 3.9.8. *Se $\mathbf{K}$ é uma variedade e X é um conjunto infinito de variáveis, então $\mathbf{K} = M(\mathrm{Id}_{\mathbf{K}}(X))$.*

Demonstração. Seja $\mathbf{K}' = M(\mathrm{Id}_{\mathbf{K}}(X))$. Então $\mathbf{K} \subseteq \mathbf{K}'$, pois $\mathbf{K} \models \mathrm{Id}_{\mathbf{K}}(X)$. Logo $\mathrm{Id}_{\mathbf{K}'}(X) \subseteq \mathrm{Id}_{\mathbf{K}}(X)$. Da definição de $\mathbf{K}'$ segue a inclusão $\mathrm{Id}_{\mathbf{K}}(X) \subseteq \mathrm{Id}_{\mathbf{K}'}(X)$. Assim, $\mathrm{Id}_{\mathbf{K}'}(X) = \mathrm{Id}_{\mathbf{K}}(X)$. Por conseguinte, pelo Teorema 3.9.4, $\theta_{\mathbf{K}'}(X) = \theta_{\mathbf{K}}(X)$, donde

$$\mathcal{T}(X)/\theta'_{\mathbf{K}}(X) = \mathcal{T}(X)/\theta_{\mathbf{K}}(X).$$

Desta última igualdade segue pelo Corolário 3.9.6 que, para qualquer conjunto de variáveis Y,

$$\mathrm{Id}_{\mathbf{K}'}(Y) = \mathrm{Id}_{\{\mathcal{T}(X)/\theta_{\mathbf{K}'}(X)\}}(Y) = \mathrm{Id}_{\{\mathcal{T}(X)/\theta_{\mathbf{K}}(X)\}}(Y) = \mathrm{Id}_{\mathbf{K}}(Y).$$

Então, novamente pelo Teorema 3.9.4, tem-se $\theta_{\mathbf{K}'}(Y) = \theta_{\mathbf{K}}(Y)$, pelo que

$$\mathcal{T}(Y)/\theta_{\mathbf{K}'}(Y) = \mathcal{T}(Y)/\theta_{\mathbf{K}}(Y).$$

Daqui segue que $\mathbf{K}' \subseteq \mathbf{K}$, pois, para qualquer álgebra $\mathcal{A} \in \mathbf{K}'$ temos

$$\mathcal{A} \in H(\{\mathcal{T}(Y)/\theta_{\mathbf{K}'}(Y)\}),$$

para algum conjunto Y adequado, donde

$$\mathcal{A} \in H(\{\mathcal{T}(Y)/\theta_{\mathbf{K}}(Y)\}) \subseteq \mathbf{K}.$$

Uma vez que $\mathbf{K} \subseteq \mathbf{K}'$ e $\mathbf{K}' \subseteq \mathbf{K}$, então $\mathbf{K}' = \mathbf{K}$. □

Teorema 3.9.9. *Seja $\mathbf{K}$ uma classe de álgebras de tipo (O, τ). Então $\mathbf{K}$ é uma classe equacional se e só se $\mathbf{K}$ é uma variedade.*

Demonstração. ($\Rightarrow$) Suponhamos que $\mathbf{K} = M(\Sigma)$, para algum conjunto de identidades Σ. Então, pelo Lema 3.9.3, $V(\mathbf{K}) \models \Sigma$. Assim, $V(\mathbf{K}) \subseteq M(\Sigma)$, e, portanto, $V(\mathbf{K}) = \mathbf{K}$, i.e., $\mathbf{K}$ é uma variedade.

($\Leftarrow$) Resulta do Lema 3.9.8. □

Exemplo 3.9.10.

(1) Grupos: A classe $\mathbf{G}$ *dos grupos vistos como álgebras de tipo (2,1,0) é uma variedade:*

$$\mathbf{G} \models \{a(bc) \approx (ab)c, a1 \approx 1a \approx a, aa^{-1} \approx a^{-1}a \approx 1\}.$$

A classe dos grupos vistos como álgebras do tipo (2) não é uma variedade.

(2) Semigrupos: A classe $\mathbf{S}$ *dos semigrupos é uma variedade:*

$$\mathbf{S} \models \{a(bc) \approx (ab)c\}.$$

(3) Reticulados: A classe $\mathbf{R}$ *dos reticulados é uma variedade*

$$\begin{aligned} \mathbf{R} \models \quad & \{a \wedge b \approx b \wedge a, a \vee b \approx b \vee a, \\ & a \wedge (b \wedge c) \approx (a \wedge b) \wedge c, a \vee (b \vee c) \approx (a \vee b) \vee c, \\ & a \vee (a \wedge b) \approx a, a \wedge (a \vee b) \approx a\}. \end{aligned}$$