UMinho | 2021

Um estudo sobre reticulados distributivos

João Manuel Guerra Fontes Gonçalves


**Universidade do Minho**
Escola de Ciências



João Manuel Guerra Fontes Gonçalves


# Um estudo sobre reticulados distributivos


Dezembro, 2021

**Universidade do Minho**
Escola de Ciências

João Manuel Guerra Fontes Gonçalves

# Um estudo sobre reticulados distributivos

Dissertação de Mestrado
Mestrado em Matemática

Trabalho realizado sob a orientação da
**Doutora Carla Albertina Carvalhinho da Silva Mendes**

Dezembro, 2021

# Agradecimentos

Gostaria de manifestar a minha sincera gratidão à Doutora Carla Albertina Carvalhinho da Silva Mendes por todo o seu trabalho em orientar-me ao longo de toda a elaboração desta dissertação de mestrado. Todos os seus conselhos e sugestões, todo o conhecimento que me transmitiu, toda a ajuda que me prestou foram verdadeiramente indispensáveis para a conclusão e aperfeiçoamento deste trabalho.

## DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

# Resumo

Nesta dissertação de mestrado, intitulada ”Um estudo sobre reticulados distributivos”, é desenvolvido um estudo sobre um dos ramos mais antigos da teoria de reticulados: os reticulados distributivos.

Um reticulado distributivo é um reticulado cujas operações binárias são distributivas uma face à outra. Assim sendo, quando a teoria dos reticulados é restringida apenas ao estudo destes reticulados, torna-se necessário saber caraterizar e representar os reticulados distributivos de modo a simplificar a sua identificação em relação aos restantes reticulados. Como será constatado ao longo da dissertação, existem, de facto, várias formas de os caraterizar e representar; para tal, tem-se por auxílio alguns conceitos da teoria de reticulados como os ideais/filtros, as relações de congruência, os homomorfismos e os elementos $\wedge$-irredutíveis/$\vee$-irredutíveis/primos/complementados.

Inicialmente, são recordados conceitos básicos sobre conjuntos parcialmente ordenados, álgebra universal e teoria geral de reticulados; destaque-se que é equivalente um reticulado ser considerado como um conjunto parcialmente ordenado ou como uma estrutura algébrica.

O capítulo final desta dissertação é reservado ao estudo das álgebras de Boole. O interesse em abordar estas álgebras deve-se ao facto de as mesmas terem um reticulado distributivo como reduto, para além de serem as estruturas algébricas que estão envolvidas na génese da teoria de reticulados e, em particular, da de reticulados distributivos. São apresentadas várias propriedades destas estruturas algébricas, com o objetivo de encontrar caraterizações e representações das mesmas.

**Palavras-chave:** Álgebra; Álgebra de Boole; Conjunto parcialmente ordenado; Reticulado; Reticulado distributivo.

# Abstract

In this master's dissertation, entitled "A study on distributive lattices", a study is developed on one of the oldest branches of lattice theory: the distributive lattices.

A distributive lattice is a lattice whose binary operations are distributive towards each other. Therefore, when the lattice theory is restricted to the study of these lattices, it becomes necessary to know how to characterize and represent the distributive lattices in order to simplify their identification in relation to the other lattices. As will be seen throughout the dissertation, there are, in fact, several ways to characterize and represent them; for that, some concepts of the lattice theory, such as ideals/filters, congruence relations, homomorphisms and $\wedge$-irreducible/$\vee$-irreducible/prime/complemented elements, are used as help.

Initially, basic concepts about partially ordered sets, universal algebra and general lattice theory are recalled; it shall be highlighted that it is equivalent for a lattice to be considered as a partially ordered set or as an algebraic structure.

The final chapter of this dissertation is reserved for the study of Boolean algebras. The interest in approaching these algebras is due to the fact that they have a distributive lattice as a reduct, in addition to being the algebraic structures that are involved in the genesis of the lattice theory and, in particular, of the distributive lattice theory. Several properties of these algebraic structures are presented, with the aim of finding characterizations and representations of them.

**Keywords:** Algebra; Boolean algebra; Distributive lattice; Lattice; Partially ordered set.

# Índice

# Introdução

O tema da presente dissertação insere-se num dos ramos que mais recentemente surgiram na história da matemática: a teoria de reticulados. O grande desenvolvimento deste ramo da matemática deve-se em muito aos estudos que Garrett Birkhoff realizou em meados da década de 1930; porém, a origem da teoria de reticulados remonta ao século XIX quando George Boole, nos seus estudos em lógica clássica, investigava estruturas algébricas que viriam mais tarde a ser conhecidas como álgebras de Boole, as quais, como agora se sabe, formam uma classe especial de álgebras que admitem como reduto um reticulado distributivo. No entanto, só em finais do século XIX é que veio a ser formalizado o atual conceito de reticulado, por Charles Pierce e Ernst Schröder, aquando das suas investigações acerca de axiomas relativos às álgebras de Boole. No mesmo período de tempo, outro matemático, Richard Dedekind, nos seus estudos em teoria de números, introduzia a noção de reticulado modular, sendo a classe dos reticulados distributivos uma subclasse da classe dos reticulados modulares.

Os reticulados distributivos são, portanto, um dos tópicos mais antigos da teoria de reticulados e um dos mais envolvidos na origem desta área matemática. O objetivo principal desta dissertação é, precisamente, estudar os reticulados distributivos e as suas propriedades, sobretudo aquelas que tornam mais fácil a sua distinção em relação aos restantes reticulados.

Assim, recordam-se, num capítulo inicial, alguns conceitos básicos sobre conjuntos parcialmente ordenados, álgebra universal e teoria de reticulados, que são cruciais para a definição de reticulado distributivo. Em particular, são recordadas as duas noções equivalentes (cf. Teorema 0.3.4) de reticulado que se podem formular: um reticulado pode ser definido como um conjunto parcialmente ordenado ou como uma álgebra munida de duas operações binárias. São também estudados vários tópicos da teoria geral de reticulados por serem essenciais para os assuntos a tratar nos capítulos posteriores.

O Capítulo 1 é a parte central da dissertação, no qual são desenvolvidos os assuntos relativos aos reticulados distributivos; nele são apresentadas as principais noções relacionadas com os reticulados distributivos e são investigadas as suas propriedades, recorrendo, para o efeito, a conceitos como os de ideal/filtro, de congruência, de homomorfismo, de elemento irredutível, definidos e estudados no Capítulo 0, com o objetivo de estabelecer resultados que auxiliem na caraterização e representação de reticulados distributivos.

No Capítulo 2, faz-se um estudo sobre álgebras de Boole e as suas principais propriedades. Grosso modo, uma álgebra de Boole é um reticulado distributivo limitado ao qual é associada a operação de complementação, para além das operações de ínfimo e supremo que um reticulado já possui por definição. São também apresentados alguns teoremas de caraterização e de representação das álgebras de Boole.

# 0 Conceitos introdutórios

Neste capítulo, recordam-se, nas duas primeiras secções, conceitos e resultados básicos sobre conjuntos parcialmente ordenados e noções básicas de álgebra universal, para assim, numa última secção, poderem ser abordados tópicos relativos à teoria geral de reticulados, que se revelam fundamentais para o estudo desenvolvido nesta dissertação.

Para uma melhor compreensão por parte do leitor, admitem-se conhecidos conceitos básicos de Teoria de Conjuntos (cf. [1], pp. 1–3; [3], pp. 1–3) e de assuntos relacionados com estes conceitos introdutórios; neste capítulo, apenas se fará referência ao que é considerado essencial para o presente trabalho.

## 0.1 Relações de ordem e relações de equivalência

No início desta secção, relembram-se alguns conceitos básicos sobre relações binárias.

**Definição 0.1.1.** Seja $X$ um conjunto. Chama-se *relação binária em* $X$ a qualquer subconjunto de $X^2 = X \times X$.

Sendo $\rho$ uma relação binária num conjunto $X$, é usual escrever-se $x \rho y$ em vez de $(x, y) \in \rho$.

**Definição 0.1.2.** Uma relação binária $\rho$ num conjunto $X$ diz-se:

- *reflexiva* se, para qualquer $x \in X$, $x \rho x$;
- *simétrica* se, para quaisquer $x, y \in X$, $x \rho y \implies y \rho x$;
- *antissimétrica* se, para quaisquer $x, y \in X$, $(x \rho y \wedge y \rho x) \implies x = y$;
- *transitiva* se, para quaisquer $x, y, z \in X$, $(x \rho y \wedge y \rho z) \implies x \rho z$.

Para o estudo de reticulados são importantes as relações binárias designadas por relações de ordem parcial.

**Definição 0.1.3.** Seja $X$ um conjunto. Chama-se *relação de ordem parcial em* $X$ ou, simplesmente, *ordem parcial em* $X$ a qualquer relação binária em $X$ que seja, simultaneamente, reflexiva, antissimétrica e transitiva.

Dado um conjunto $X$, representa-se uma ordem parcial em $X$ por $\leq_X$, ou apenas por $\leq$, caso não haja ambiguidade.

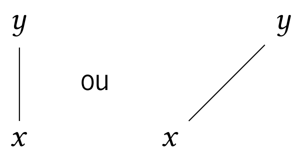
**Definição 0.1.4.** Sejam $P$ um conjunto não vazio e $\leq$ uma relação binária em $P$. Diz-se que o par $(P; \leq)$ é um *conjunto parcialmente ordenado* (abreviadamente, *c.p.o.*) ou que o conjunto $P$ é *ordenado pela relação* $\leq$ se $\leq$ for uma ordem parcial em $P$.

Um c.p.o. $(P; \leq)$ poderá ser representado apenas por $P$ no caso de ser óbvia a ordem parcial considerada; além disso, dados $x, y \in P$, é usual escrever-se:

- $x \leq y$, e dizer-se que $x$ *é menor ou igual a* $y$, para representar $(x, y) \in \leq$;
- $x \geq y$, e dizer-se que $x$ *é maior ou igual a* $y$, em alternativa a $y \leq x$;
- $x < y$, e dizer-se que $x$ *é menor que* $y$, se $x \leq y$ e $x \neq y$;
- $x > y$, e dizer-se que $x$ *é maior que* $y$, em alternativa a $y < x$;
- $x \prec y$, e dizer-se que $y$ *é um sucessor de* $x$ *em* $P$ ou que $x$ *é um antecessor de* $y$ *em* $P$, caso $x < y$ e não exista qualquer $z \in P$ tal que $x < z < y$.

**Definição 0.1.5.** Seja $(P; \leq)$ um c.p.o.. Dois elementos $x$ e $y$ de $P$ dizem-se *comparáveis* se $x \leq y$ ou $y \leq x$; caso contrário, diz-se que $x$ e $y$ são *incomparáveis*.

Qualquer c.p.o. finito $P$ pode ser representado através de um diagrama, designado por *diagrama de Hasse*, onde cada elemento de $P$ é representado pelo respetivo símbolo e, sempre que, em $P$, $x \prec y$, posiciona-se o símbolo de $y$ acima do símbolo de $x$ e unem-se ambos os símbolos com um segmento de reta, como por exemplo,




.

A partir de uma ordem parcial definida num conjunto $P$, é possível definirem-se, de forma natural, outras relações de ordem parcial.

**Proposição 0.1.6.** *Sejam $(P; \leq)$ um c.p.o. e $Q$ um subconjunto não vazio de $P$. A relação binária $\leq_{|Q}$, definida em $Q$ de tal modo que, para quaisquer $x, y \in Q$,*

$$x \leq_{|Q} y \text{ se } x \leq y \text{ em } P,$$

*é uma ordem parcial em $Q$, ou seja, $(Q; \leq_{|Q})$ é um c.p.o..*

**Definição 0.1.7.** Sejam $(P; \leq)$ um c.p.o. e $Q$ um subconjunto não vazio de $P$. Chama-se *ordem parcial induzida por $\leq$ em $Q$* à ordem parcial $\leq_{|Q}$ tal como definida na proposição anterior e diz-se que $(Q; \leq_{|Q})$ é um *c.p.o. em $(P; \leq)$*.

**Proposição 0.1.8.** *Sejam $(P; \leq)$ um c.p.o. e $\leq^{\delta}$ a relação binária em $P$ definida por*

$$x \leq^{\delta} y \ \text{ se } \ y \leq x,$$

*para quaisquer $x, y \in P$. Então, $(P; \leq^{\delta})$ é um c.p.o..*

**Definição 0.1.9.** Seja $(P; \leq)$ um c.p.o.. Chama-se *ordem parcial dual de $\leq$* à ordem parcial $\leq^{\delta}$ definida tal como na proposição anterior e dá-se a designação de *conjunto parcialmente ordenado dual de $P$* ao c.p.o. $(P; \leq^{\delta})$.

Dado um c.p.o. $(P; \leq)$, denota-se o c.p.o. $(P; \leq^{\delta})$ por $P^{\delta}$; além disso, é habitual usar-se a notação $\geq$ para representar a relação $\leq^{\delta}$.

**Definição 0.1.10.** Seja $\Phi$ uma afirmação sobre c.p.o.. Chama-se *afirmação dual de $\Phi$* à afirmação $\Phi^{\delta}$, obtida a partir de $\Phi$ substituindo cada ocorrência, quer explícita quer implícita, de $\leq$ por $\leq^{\delta}$.

Note-se que quando uma afirmação $\Phi$ é verdadeira num c.p.o. $P$, também a afirmação $\Phi^{\delta}$ é verdadeira em $P^{\delta}$. Generalizando esta observação, obtém-se o resultado seguinte.

**Proposição 0.1.11** (Princípio de Dualidade para c.p.o.; cf. [7], p. 5)**.** *Se uma afirmação $\Phi$ for válida em qualquer c.p.o., então o mesmo sucede com a sua afirmação dual, $\Phi^{\delta}$.*

**Definição 0.1.12.** Sejam $(P; \leq)$ um c.p.o. e $Q \subseteq P$. Um elemento $x$ de $P$ diz-se:

- um *elemento minimal de $Q$* se $x \in Q$ e, para qualquer $y \in Q$, $y \leq x \implies x = y$;
- um *minorante de $Q$* se, para qualquer $y \in Q$, $x \leq y$;
- um *elemento mínimo de $Q$* se $x$ for um minorante de $Q$ tal que $x \in Q$;
- um *ínfimo de $Q$* se $x$ for um minorante de $Q$ e, para qualquer minorante $y$ de $Q$, $y \leq x$.

Os conceitos de *elemento maximal*, *majorante*, *elemento máximo* e *supremo* são duais dos conceitos anteriores, respetivamente.

Seja $P$ um c.p.o.. Um subconjunto $Q$ de $P$ tem, quando muito, um elemento mínimo; este, quando existe, denota-se por $0_Q$ ou, se não houver ambiguidade, $0$. Também o ínfimo de $Q$, quando existe, é único e representa-se por $\inf(Q)$. Se $Q = \{x_1, \ldots, x_k\}$ para certos $k \in \mathbb{N}$ e $x_1, \ldots, x_k \in P$, é habitual escrever-se $\inf\{x_1, \ldots, x_k\}$ para representar $\inf(Q)$, em vez de $\inf(\{x_1, \ldots, x_k\})$.

Pelo Princípio de Dualidade para c.p.o., os resultados duais dos descritos no parágrafo anterior também são válidos. As notações $1_Q$, $1$, $\sup(Q)$ e $\sup\{x_1, \ldots, x_k\}$ têm o significado dual de $0_Q$, $0$, $\inf(Q)$ e $\inf\{x_1, \ldots, x_k\}$, correspondentemente.

Atendendo às noções anteriormente apresentadas, não é difícil provar os seguintes resultados.

**Proposição 0.1.13.** *Seja $(P; \leq)$ um c.p.o.. Então, para quaisquer $x, y \in P$,*

$$x \leq y \iff \inf\{x, y\} = x \iff \sup\{x, y\} = y.$$

**Proposição 0.1.14.** *Seja $(P; \leq)$ um c.p.o. e sejam $x, y, z, w \in P$ tais que $x \leq z$ e $y \leq w$.*

*(i) Se existirem $\inf\{x, y\}$ e $\inf\{z, w\}$, então $\inf\{x, y\} \leq \inf\{z, w\}$.*

*(ii) Se existirem $\sup\{x, y\}$ e $\sup\{z, w\}$, então $\sup\{x, y\} \leq \sup\{z, w\}$.*

Definem-se seguidamente algumas classes de c.p.o. com propriedades especiais.

**Definição 0.1.15.** Seja $P$ um conjunto não vazio. Um par $(P; \leq)$ diz-se um *conjunto parcialmente ordenado limitado* se $(P; \leq)$ for um c.p.o. no qual exista elemento mínimo e elemento máximo, simultaneamente.

**Definição 0.1.16.** Seja $(P; \leq)$ um c.p.o..

- Diz-se que $P$ *satisfaz a condição minimal* se, para qualquer subconjunto não vazio $Q$ de $P$, algum elemento de $Q$ for minimal.
- Dualmente, diz-se que $P$ *satisfaz a condição maximal* se, para qualquer subconjunto não vazio $Q$ de $P$, algum elemento de $Q$ for maximal.

**Definição 0.1.17.** Um c.p.o. $(P; \leq)$ diz-se um *conjunto totalmente ordenado* ou uma *cadeia* se quaisquer dois elementos de $P$ forem comparáveis.

**Definição 0.1.18.** Seja $(P; \leq)$ um c.p.o.. Chama-se *cadeia em* $(P; \leq)$ a qualquer c.p.o. em $(P; \leq)$ que seja uma cadeia.

Apresentam-se seguidamente algumas condições que poderão ser satisfeitas pelas cadeias de um c.p.o e que serão úteis para o estudo a desenvolver nesta dissertação.

**Lema 0.1.19** (Lema de Zorn; cf. [7], p. 117)**.** *Sejam $A$ um conjunto e $\mathcal{X}$ um subconjunto não vazio de $\wp(A)$ tal que, para qualquer cadeia $C$ em $(\mathcal{X}; \subseteq)$, $\bigcup C \in \mathcal{X}$. Então, $\mathcal{X}$ tem um elemento maximal.*

**Definição 0.1.20.** Seja $(P; \leq)$ um c.p.o..

- Diz-se que $P$ *satisfaz a condição da cadeia ascendente* (abreviadamente, *c.c.a.*) se, para qualquer cadeia ascendente
$$x_1 \leq x_2 \leq x_3 \leq \cdots$$
em $P$, existir algum $n \in \mathbb{N}$ tal que, para qualquer $k \in \mathbb{N}$, $x_{n+k} = x_n$.

- Diz-se que $P$ *satisfaz a condição da cadeia descendente* (abreviadamente, *c.c.d.*) se, para qualquer cadeia descendente
$$x_1 \geq x_2 \geq x_3 \geq \cdots$$
em $P$, existir algum $n \in \mathbb{N}$ tal que, para qualquer $k \in \mathbb{N}$, $x_{n+k} = x_n$.

**Teorema 0.1.21** (cf. [9], Theorem 1.13, p. 17)**.** *Seja $P$ um c.p.o.. Então,*

*(i) $P$ satisfaz a c.c.d. se e só se $P$ satisfaz a condição minimal;*

*(ii) $P$ satisfaz a c.c.a. se e só se $P$ satisfaz a condição maximal.*

*Demonstração.* Como as condições *(i)* e *(ii)* são duais uma da outra, basta provar uma delas; demonstre-se *(i)*.

Suponha-se, primeiramente, que $P$ satisfaz a c.c.d.. Seja $Q$ um subconjunto não vazio de $P$. Então, tome-se arbitrariamente algum elemento de $Q$, $q_1$. Caso $q_1$ seja um elemento minimal de $Q$, dá-se por concluída a prova. Caso $q_1$ não seja um elemento minimal de $Q$, então existe $q_2 \in Q$ tal que
$$q_1 > q_2.$$
De igual modo, se $q_2$ for um elemento minimal de $Q$, a prova termina; caso contrário, existe $q_3 \in Q$ tal que
$$q_1 > q_2 > q_3.$$
Usando sucessivamente o mesmo raciocínio, ou se obtém, a dado momento, algum $q_n \in Q$ ($n \in \mathbb{N}$) tal que $q_n$ seja um elemento minimal de $Q$ ou se obtém uma cadeia ascendente infinita
$$q_1 > q_2 > q_3 > \cdots > q_n > \cdots,$$
o que, devido à hipótese, não pode acontecer. Logo, $P$ satisfaz a condição minimal.

Admita-se, agora, que $P$ satisfaz a condição minimal. Então, em particular, qualquer cadeia descendente
$$x_1 \geq x_2 \geq x_3 \geq \cdots$$
em $P$ possui algum elemento minimal $x_n$, para certo $n \in \mathbb{N}$. Logo, para qualquer $k \in \mathbb{N}$, tem-se $x_{n+k} = x_n$. Portanto, $P$ satisfaz a c.c.d.. □

De entre as aplicações entre c.p.o., destacam-se aquelas que preservam as ordens parciais dos c.p.o. envolvidos: os homomorfismos de c.p.o..

**Definição 0.1.22.** Sejam $(P; \leq_P)$ e $(Q; \leq_Q)$ c.p.o.. Uma aplicação $\varphi$ de $P$ em $Q$ diz-se:

- *isótona* ou um *homomorfismo de c.p.o.* se, para quaisquer $x, y \in P$,
$$x \leq_P y \implies \varphi(x) \leq_Q \varphi(y);$$
- um *mergulho de ordem* se, para quaisquer $x, y \in P$,
$$x \leq_P y \iff \varphi(x) \leq_Q \varphi(y);$$
- um *isomorfismo de c.p.o.* se $\varphi$ for, simultaneamente, sobrejetiva e um mergulho de ordem.

**Definição 0.1.23.** Sejam $P$ e $Q$ c.p.o.. Diz-se que $P$ *é isomorfo a* $Q$ se existir algum isomorfismo de c.p.o. de $P$ em $Q$.

Observe-se também que um mergulho de ordem é uma aplicação injetiva e que, por consequência, um isomorfismo de c.p.o. é uma bijeção.

**Proposição 0.1.24.** *Sejam $(P; \leq_P)$ e $(Q; \leq_Q)$ c.p.o.. Uma aplicação $\varphi$ de $P$ em $Q$ é um isomorfismo de c.p.o. se e só se $\varphi$ é invertível e $\varphi$ e $\varphi^{-1}$ são isótonas.*

Repare-se que, dados dois c.p.o. $P$ e $Q$, se $P$ for isomorfo a $Q$, também $Q$ será isomorfo a $P$, pelo que poderá dizer-se simplesmente que os c.p.o. $P$ e $Q$ são isomorfos, podendo, como alternativa, escrever-se $P \cong Q$ para indicar essa informação.

Um dos exemplos mais comuns de construções de c.p.o. são os produtos diretos de c.p.o..

Primeiramente, recorde-se que, sendo $I$ um conjunto, o produto cartesiano da família de conjuntos $(X_i)_{i\in I}$ é o conjunto de funções $\{f : I \to \bigcup_{i\in I} X_i \mid f(i) \in X_i\}$.

**Proposição 0.1.25.** *Sejam $I$ um conjunto, $((P_i; \leq_i))_{i\in I}$ uma família de c.p.o. e $\sqsubseteq$ a relação binária em $\prod_{i\in I} P_i$ definida de tal modo que, para quaisquer $x, y \in \prod_{i\in I} P_i$,*
$$x \sqsubseteq y \ \text{ se } \ \forall\, i \in I,\ x(i) \leq_i y(i).$$
*Então, o par $(\prod_{i\in I} P_i; \sqsubseteq)$ é um c.p.o..*

**Definição 0.1.26.** Sejam $I$ um conjunto e $((P_i; \leq_i))_{i\in I}$ uma família de c.p.o.. Designa-se o c.p.o. $(\prod_{i\in I} P_i; \sqsubseteq)$ por *produto direto de* $((P_i; \leq_i))_{i\in I}$.

Para o estudo desenvolvido nesta dissertação, é também útil recordar o conceito de relação de equivalência.

**Definição 0.1.27.** Seja $X$ um conjunto. Chama-se *relação de equivalência em* $X$ ou, simplesmente, *equivalência em* $X$ a qualquer relação binária em $X$ que seja, simultaneamente, reflexiva, simétrica e transitiva.

Sendo $X$ um conjunto, representa-se por $\mathrm{Equ}(X)$ o conjunto de todas as equivalências em $X$.

**Definição 0.1.28.** Sejam $X$ um conjunto e $\theta \in \mathrm{Equ}(X)$. Para qualquer $x \in X$, o conjunto

$$[x]_\theta = \{y \in X \mid x\theta y\}$$

diz-se uma *classe de equivalência de* $\theta$ *em* $X$; em particular, $[x]_\theta$ diz-se *a classe de equivalência de* $x$ *módulo* $\theta$, ou simplesmente *a classe de equivalência de* $x$, caso não haja ambiguidade.

Dados um conjunto $X$, $\theta \in \mathrm{Equ}(X)$ e $x \in X$, poderá representar-se a classe de equivalência $[x]_\theta$ apenas por $[x]$, quando for óbvia a relação tratada.

**Definição 0.1.29.** Sejam $X$ um conjunto e $\theta \in \mathrm{Equ}(X)$. Chama-se *conjunto quociente de* $X$ *por* $\theta$ ao conjunto de todas as classes de equivalência de $\theta$ em $X$, representado usualmente por $X/\theta$, isto é,

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

## 0.2 Álgebra universal

Nesta secção, recordam-se algumas noções básicas de álgebra universal, área matemática que generaliza o estudo que é feito em estruturas algébricas mais concretas, tais como grupos, anéis, reticulados, procurando investigar as propriedades que estas têm em comum.

A noção de álgebra é nuclear para o estudo em álgebra universal. No sentido de a formalizar, recordam-se, de seguida, alguns conceitos necessários para tal.

**Definição 0.2.1.** Sejam $A$ um conjunto não vazio e $n \in \mathbb{N}_0$. Uma aplicação $f$ de $A^n$ em $A$ diz-se uma *operação* $n$*-ária em* $A$ ou uma *operação de aridade* $n$ *em* $A$; $n$ diz-se a *aridade de* $f$.

Dados um conjunto não vazio $A$, $n \in \mathbb{N}_0$ e $f$ uma operação $n$-ária em $A$, em situações em que não seja necessário indicar a aridade de $f$, pode simplesmente dizer-se que $f$ é uma *operação em* $A$. Além disso, a operação $f$ diz-se *nulária*, *unária*, *binária* se a aridade de $f$ for, respetivamente, $0$, $1$, $2$.

**Definição 0.2.2.** Sejam $A$ um conjunto não vazio, $n \in \mathbb{N}_0$, $f$ uma operação $n$-ária em $A$ e $X \subseteq A$. O conjunto $X$ diz-se *fechado para a operação* $f$ se, para qualquer $(x_1, \ldots, x_n) \in X^n$,

$$f(x_1, \ldots, x_n) \in X.$$

Habitualmente, as operações são representadas por símbolos, tais como $f$, $g$, $+$, $\cdot$, $\times$, designados por *símbolos de operação*.

**Definição 0.2.3.** Um *tipo algébrico* ou, simplesmente, *tipo* consiste num par $(O, (n_f)_{f\in O})$ onde $O$ é um conjunto formado por símbolos de operação e $(n_f)_{f\in O}$ é uma família de números inteiros não negativos; para cada $f \in O$, $n_f$ diz-se a *aridade de* $f$.

**Definição 0.2.4.** Define-se *álgebra de tipo* $(O, (n_f)_{f\in O})$ ou, somente, *álgebra* como sendo 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 em $A$ indexada pelo conjunto $O$, de tal modo que, para cada símbolo de operação $f \in O$ de aridade $n_f$, $f^{\mathcal{A}}$ é uma operação $n_f$-ária em $A$. Designa-se o conjunto $A$ por *universo de* $\mathcal{A}$ e cada operação $f^{\mathcal{A}} \in F$ por *operação fundamental de* $\mathcal{A}$. Diz-se que o conjunto $O$ é *o conjunto dos símbolos de operação de* $\mathcal{A}$.

Para cada operação fundamental $f^{\mathcal{A}}$ de uma álgebra $\mathcal{A}$, também pode escrever-se $f$ em vez de $f^{\mathcal{A}}$, caso não haja ambiguidade.

Note-se que, dada uma álgebra $\mathcal{A} = (A; F)$ de tipo $(O, (n_f)_{f\in O})$, o conjunto de símbolos de operação de $\mathcal{A}$ pode ser finito ou infinito. Caso seja finito e não vazio, isto é, $O = \{f_1, \ldots, f_k\}$ para algum $k \in \mathbb{N}$, e supondo, sem perda de generalidade, que $n_{f_1} \geq \cdots \geq n_{f_k}$, é usual representar a álgebra $(A; F)$ por $(A; f_1^{\mathcal{A}}, \ldots, f_k^{\mathcal{A}})$ ou, se não houver ambiguidade, por $(A; f_1, \ldots, f_k)$; neste caso, também é frequente denotar o tipo de $\mathcal{A}$ por $(O, n_{f_1}, \ldots, n_{f_k})$ ou somente por $(n_{f_1}, \ldots, n_{f_k})$.

**Definição 0.2.5.** Seja $\mathcal{A} = (A; F)$ uma álgebra de tipo $(O, (n_f)_{f\in O})$. Chama-se *reduto de* $\mathcal{A}$ a qualquer álgebra $\mathcal{B} = (B; G)$ de tipo $(U, (m_g)_{g\in U})$ tal que $B = A$, $U \subseteq O$ e, para cada $g \in U$, $m_g = n_g$ e $g^{\mathcal{B}} = g^{\mathcal{A}}$.

**Definição 0.2.6.** Seja $\mathcal{A} = (A; F)$ uma álgebra. Um subconjunto $B$ de $A$ diz-se um *subuniverso de* $\mathcal{A}$ se $B$ for fechado para toda a operação fundamental de $\mathcal{A}$.

**Definição 0.2.7.** Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ duas álgebras, ambas de tipo $(O, (n_f)_{f\in O})$. Diz-se que $\mathcal{B}$ é uma *subálgebra de* $\mathcal{A}$, e escreve-se $\mathcal{B} \leq \mathcal{A}$, se $B$ for um subuniverso de $\mathcal{A}$ e, para quaisquer $f \in O$ e $(b_1, \ldots, b_{n_f}) \in B^{n_f}$,

$$f^{\mathcal{B}}(b_1, \ldots, b_{n_f}) = f^{\mathcal{A}}(b_1, \ldots, b_{n_f}).$$

O conceito de homomorfismo de álgebras consiste numa aplicação entre universos de álgebras que é compatível com as operações das álgebras envolvidas. Esta noção, que será formalizada de seguida, tem, de facto, um papel muito importante no estudo da álgebra universal.

**Definição 0.2.8.** Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ duas álgebras do mesmo tipo $(O, (n_f)_{f\in O})$. Uma aplicação $\varphi$ de $A$ em $B$ diz-se:

- um *homomorfismo de $\mathcal{A}$ em $\mathcal{B}$*, e escreve-se $\varphi : \mathcal{A} \to \mathcal{B}$, se, para quaisquer $f \in O$ e $(a_1, \dots, a_{n_f}) \in A^{n_f}$,
$$\varphi(f^{\mathcal{A}}(a_1, \dots, a_{n_f})) = f^{\mathcal{B}}(\varphi(a_1), \dots, \varphi(a_{n_f}));$$
- um *epimorfismo* se $\varphi$ for sobrejetiva e $\varphi : \mathcal{A} \to \mathcal{B}$;
- um *monomorfismo* se $\varphi$ for injetiva e $\varphi : \mathcal{A} \to \mathcal{B}$;
- um *isomorfismo* se $\varphi$ for bijetiva e $\varphi : \mathcal{A} \to \mathcal{B}$.

**Definição 0.2.9.** Seja $\mathcal{A}$ uma álgebra. Dá-se a designação de *endomorfismo em $\mathcal{A}$* a qualquer homomorfismo de $\mathcal{A}$ em $\mathcal{A}$.

**Definição 0.2.10.** Sejam $\mathcal{A}$ e $\mathcal{B}$ álgebras do mesmo tipo. Diz-se que $\mathcal{A}$ é *isomorfa a $\mathcal{B}$* se existir algum isomorfismo de $\mathcal{A}$ em $\mathcal{B}$.

É simples verificar que, dadas duas álgebras $\mathcal{A}$ e $\mathcal{B}$ do mesmo tipo, se $\mathcal{A}$ for isomorfa a $\mathcal{B}$, então também $\mathcal{B}$ é isomorfa a $\mathcal{A}$. Por isso, poderá apenas dizer-se que $\mathcal{A}$ e $\mathcal{B}$ são isomorfas e usa-se a notação $\mathcal{A} \cong \mathcal{B}$ para indicar essa informação; neste caso, também se diz frequentemente que "$\mathcal{A}$ e $\mathcal{B}$ são iguais, a menos de um isomorfismo".

**Definição 0.2.11.** Seja $\mathcal{A}$ uma álgebra. Dá-se a designação de *imagem homomorfa de $\mathcal{A}$* a qualquer álgebra $\mathcal{B}$ tal que exista algum epimorfismo de $\mathcal{A}$ em $\mathcal{B}$.

A composição de homomorfismos de álgebras continua a ser um homomorfismo de álgebras, tal como é estabelecido no teorema seguinte.

**Proposição 0.2.12** (cf. [3], Theorem 6.5, p. 48)**.** *Sejam $\mathcal{A}$, $\mathcal{B}$ e $C$ álgebras do mesmo tipo. Para quaisquer $\varphi : \mathcal{A} \to \mathcal{B}$ e $\phi : \mathcal{B} \to C$, a composição $\phi \circ \varphi$ é um homomorfismo de $\mathcal{A}$ em $C$.*

Apresentam-se, de seguida, os conceitos de congruência numa álgebra e de álgebra quociente, e ver-se-á como estes se relacionam com a noção de homomorfismo de álgebras.

**Definição 0.2.13.** Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo $(O, (n_f)_{f \in O})$ e $\theta \in \mathrm{Equ}(A)$. Diz-se que $\theta$ é uma *relação de congruência em $\mathcal{A}$* ou, somente, *congruência em $\mathcal{A}$* se, para quaisquer $f \in O$ e $(a_1, \dots, a_{n_f}), (b_1, \dots, b_{n_f}) \in A^{n_f}$,
$$(\forall i \in \{1, \dots, n_f\},\ a_i \theta b_i) \implies f^{\mathcal{A}}(a_1, \dots, a_{n_f}) \theta f^{\mathcal{A}}(b_1, \dots, b_{n_f}).$$

O conjunto de todas as congruências em $\mathcal{A}$ é denotado por $\mathrm{Con}(\mathcal{A})$. Observe-se que $(\mathrm{Con}(\mathcal{A}); \subseteq)$ é um c.p.o. limitado, sendo a relação identidade $\triangle_A = \{(a, a) \in A^2 \mid a \in A\}$ e a relação universal $\triangledown_A = A^2$ os seus elementos mínimo e máximo, respetivamente.

**Definição 0.2.14.** Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo $(O, (n_f)_{f \in O})$ e $\theta \in \mathrm{Con}(\mathcal{A})$. Chama-se *álgebra quociente de $\mathcal{A}$ por $\theta$* à álgebra $\mathcal{A}/\theta = (A/\theta; (f^{\mathcal{A}/\theta})_{f \in O})$, também de tipo $(O, (n_f)_{f \in O})$, onde, para quaisquer $f \in O$ e $a_1, \ldots, a_{n_f} \in A$,

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

Segue-se a definição de núcleo de um homomorfismo de álgebras, o qual se prova tratar-se de uma congruência definida no domínio do homomorfismo.

**Definição 0.2.15.** Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo e $\varphi : \mathcal{A} \to \mathcal{B}$. Designa-se por *núcleo de $\varphi$* a relação binária em $A$ definida por

$$\mathrm{Nuc}(\varphi) = \{(a, b) \in A^2 : \varphi(a) = \varphi(b)\}.$$

**Proposição 0.2.16** (cf. [3], Theorem 6.8, p. 49)**.** *Sejam $\mathcal{A}$ e $\mathcal{B}$ álgebras do mesmo tipo e $\varphi : \mathcal{A} \to \mathcal{B}$. Então, $\mathrm{Nuc}(\varphi)$ é uma congruência em $\mathcal{A}$.*

**Proposição 0.2.17** (cf. [3], Theorem 6.10, p. 50)**.** *Sejam $\mathcal{A} = (A; F)$ uma álgebra e $\theta \in \mathrm{Con}(\mathcal{A})$. A correspondência $\pi_\theta$ de $A$ em $A/\theta$, definida por*

$$\pi_\theta(a) = [a]_\theta, \forall a \in A,$$

*é um epimorfismo de $\mathcal{A}$ em $\mathcal{A}/\theta$.*

**Definição 0.2.18.** Sejam $\mathcal{A} = (A; F)$ uma álgebra e $\theta \in \mathrm{Con}(\mathcal{A})$. Chama-se *homomorfismo natural de $\mathcal{A}$ em $\mathcal{A}/\theta$* ao epimorfismo $\pi_\theta$ definido tal como na proposição anterior.

**Teorema 0.2.19** (Teorema do Homomorfismo; cf. [3], Theorem 6.12, pp. 50–51)**.** *Seja $\mathcal{A} = (A; F)$ uma álgebra de tipo $(O, (n_f)_{f \in O})$. Qualquer imagem homomorfa a $\mathcal{A}$ é isomorfa a alguma álgebra quociente de $\mathcal{A}$: sendo $\mathcal{B} = (B; G)$ uma álgebra tal que existe um epimorfismo $\varphi$ de $\mathcal{A}$ em $\mathcal{B}$ e definindo $\theta = \mathrm{Nuc}(\varphi)$ e $\psi$ como sendo a correspondência de $A/\theta$ em $B$ tal que*

$$\psi([a]_\theta) = \varphi(a), \ \forall\, [a]_\theta \in A/\theta,$$

*tem-se que $\psi$ é um isomorfismo de $\mathcal{A}/\theta$ em $\mathcal{B}$ tal que $\psi \circ \pi_\theta = \varphi$, ou seja, tal que o diagrama*

$$\begin{tikzcd} \mathcal{A} \arrow[rr, "\varphi"] \arrow[dr, "\pi_\theta"'] & & \mathcal{B} \\ & \mathcal{A}/\theta \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

*é comutativo.*

Anteriormente, foram apresentados conceitos, como o de subálgebra e o de álgebra quociente, que são exemplos de processos de construção de novas álgebras a partir de outras dadas. Contudo, nos que até agora foram tratados, as álgebras obtidas têm complexidade inferior ou igual às álgebras originais. De seguida, descreve-se um processo de construção de álgebras em que, a partir da combinação de várias álgebras, se obtém uma álgebra com complexidade superior a qualquer uma das álgebras iniciais. Trata-se do produto direto de álgebras.

**Definição 0.2.20.** Sejam $I$ um conjunto e $(\mathcal{A}_i)_{i\in I} = ((A_i; F_i))_{i\in I}$ uma família de álgebras de tipo $(O, (n_f)_{f\in O})$. Chama-se *produto direto de* $(\mathcal{A}_i)_{i\in I}$ à álgebra $(\prod_{i\in I} A_i; (f^{\prod_{i\in I}\mathcal{A}_i})_{f\in O})$, também de tipo $(O, (n_f)_{f\in O})$, representada habitualmente por $\prod_{i\in I}\mathcal{A}_i$, onde, para quaisquer $f \in O$ e $x_1, \ldots, x_{n_f} \in \prod_{i\in I} A_i$,

$$f^{\prod_{i\in I}\mathcal{A}_i}(x_1, \ldots, x_{n_f})(i) = f^{\mathcal{A}_i}(x_1(i), \ldots, x_{n_f}(i)),$$

para cada $i \in I$.

Sendo $I = \{i_1, \ldots, i_k\}$, para certo $k \in \mathbb{N}$, escreve-se $\mathcal{A}_{i_1} \times \cdots \times \mathcal{A}_{i_k}$ para representar o produto direto $\prod_{i\in I}\mathcal{A}_i$. Sendo $\mathcal{A}$ uma álgebra, denota-se por $\mathcal{A}^I$ o produto direto $\prod_{i\in I}\mathcal{A}_i$ onde, para qualquer $i \in I$, $\mathcal{A}_i = \mathcal{A}$; além disso, se $I = \{i_1, \ldots, i_k\}$, para certo $k \in \mathbb{N}$, escreve-se $\mathcal{A}^k$ para representar o produto direto $\mathcal{A}_{i_1} \times \cdots \times \mathcal{A}_{i_k}$ quando $\mathcal{A}_{i_1} = \cdots = \mathcal{A}_{i_k} = \mathcal{A}$.

## 0.3 Reticulados

Nesta secção, estudam-se alguns tópicos da teoria geral de reticulados.

### 0.3.1 Duas definições de reticulado

A noção de reticulado pode ser definida sob dois pontos de vista: um reticulado pode ser tratado como um conjunto parcialmente ordenado ou como uma álgebra.

**Definição 0.3.1.** Um c.p.o. $(R; \leq)$ diz-se um *reticulado* se, em $R$, existirem $\inf\{x, y\}$ e $\sup\{x, y\}$, para quaisquer $x,y \in R$.

Equivalentemente, um c.p.o. $(R; \leq)$ é um reticulado se, para qualquer subconjunto não vazio finito $S$ de $R$, os elementos $\inf(S)$ e $\sup(S)$ existirem em $R$.

**Definição 0.3.2.** Um reticulado $(R; \leq)$ diz-se *completo* se, para qualquer subconjunto $S$ de $R$, os elementos $\inf(S)$ e $\sup(S)$ existirem em $R$.

Um reticulado pode também ser visto como uma estrutura algébrica. De facto, uma vez que, num reticulado $(R;\leq)$, existem sempre $\inf\{x,y\}$ e $\sup\{x,y\}$, para quaisquer $x,y\in R$, e ambos são univocamente determinados, então é possível definir, em $R$, operações binárias, habitualmente denotadas por $\wedge$ e $\vee$, conforme as igualdades

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

Assim, $(R;\wedge,\vee)$ é uma álgebra (de tipo $(2,2)$). Além disso, as operações $\wedge$ e $\vee$ satisfazem (ver demonstração do Teorema 0.3.4)

- a propriedade de *idempotência*, isto é, para qualquer $x\in R$,

$$x\wedge x=x\ \text{ e }\ x\vee x=x;$$

- a propriedade *comutativa*, isto é, para quaisquer $x,y\in R$,

$$x\wedge y=y\wedge x\ \text{ e }\ x\vee y=y\vee x;$$

- a propriedade *associativa*, isto é, para quaisquer $x,y,z\in R$,

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

- a propriedade de *absorção*, isto é, para quaisquer $x,y\in R$,

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

Considerando a propriedade associativa satisfeita pelas operações de um reticulado $R$, para quaisquer $x,y,z\in R$, poderá escrever-se $x\wedge y\wedge z$ em vez de $x\wedge(y\wedge z)$ ou $(x\wedge y)\wedge z$, bem como $x\vee y\vee z$ em vez de $x\vee(y\vee z)$ ou $(x\vee y)\vee z$.

Faz sentido, portanto, definir reticulado tratando-o como uma estrutura algébrica.

**Definição 0.3.3.** Seja $R$ um conjunto não vazio. Uma álgebra $(R;\wedge,\vee)$ de tipo $(2,2)$ designa-se *reticulado* se as operações binárias $\wedge$ e $\vee$ satisfizerem as propriedades de idempotência, comutativa, associativa e de absorção.

Apesar de as duas definições de reticulado aqui expostas serem de naturezas diferentes, elas relacionam-se e até podem dizer-se equivalentes no sentido em que, se um reticulado, definido sobre um conjunto $R$, satisfizer uma das definições, então é possível construir-se, de modo único, um reticulado, sobre o mesmo conjunto $R$, conforme a outra definição. Esta relação entre as duas definições de reticulado é estabelecida no resultado seguinte.

**Teorema 0.3.4** (cf. [7], Theorem 3, pp. 12–14)**.** *Seja $R$ um conjunto não vazio.*

*(i) Se $(R; \wedge, \vee)$ for um reticulado, então $(R; \leq)$, onde $\leq$ é a relação definida por*

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

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

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

*(ii) Se $(R; \leq)$ é um reticulado, então $(R; \wedge, \vee)$, onde, para quaisquer $x, y \in R$,*

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

*é um reticulado. Além disso, para quaisquer $x, y \in R$,*

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

*Demonstração.* *(i)* Suponha-se que $(R; \wedge, \vee)$ é um reticulado. A relação $\leq$ é uma ordem parcial em $R$: primeiramente, sendo $x \in R$, como, pela idempotência, $x = x \wedge x$, então $x \leq x$ e, portanto, $\leq$ é reflexiva; além disso, dados $x, y \in R$ e admitindo que $x \leq y$ e $y \leq x$, isto é, $x = x \wedge y$ e $y = y \wedge x$, segue, pela comutatividade, que $x = y$, logo $\leq$ é antissimétrica; por fim, dados $x, y, z \in R$ tais que $x \leq y$ e $y \leq z$, ou seja, $x = x \wedge y$ e $y = y \wedge z$, tem-se

$$\begin{aligned}
x \wedge z &= (x \wedge y) \wedge z && \text{[hipótese]} \\
&= x \wedge (y \wedge z) && \text{[associatividade]} \\
&= x \wedge y && \text{[hipótese]} \\
&= x, && \text{[hipótese]}
\end{aligned}$$

pelo que $x \leq z$ e, portanto, $\leq$ é transitiva. Conclui-se assim que $(R; \leq)$ é um c.p.o.. Sejam, agora, $x, y \in R$. Ora, por um lado, tem-se

$$\begin{aligned}
(x \wedge y) \wedge x &= (y \wedge x) \wedge x && \text{[comutatividade]} \\
&= y \wedge (x \wedge x) && \text{[associatividade]} \\
&= x \wedge y && \text{[idempotência e comutatividade]}
\end{aligned}$$

e, por outro lado,

$$\begin{aligned}
(x \wedge y) \wedge y &= x \wedge (y \wedge y) && \text{[associatividade]} \\
&= x \wedge y, && \text{[idempotência]}
\end{aligned}$$

o que implica que $x \wedge y$ é um minorante de $\{x, y\}$. Seja $z$ um minorante qualquer de $\{x, y\}$. Assim, $z = z \wedge x$ e $z = z \wedge y$ e, consequentemente,

$$\begin{aligned} z \wedge (x \wedge y) &= (z \wedge x) \wedge y && \text{[associatividade]} \\ &= z \wedge y && \text{[hipótese]} \\ &= z, && \text{[hipótese]} \end{aligned}$$

ou seja, $z \leq x \wedge y$, donde se conclui que $\inf\{x, y\}$ existe e é dado por $x \wedge y$. Analogamente, $\sup\{x, y\}$ também existe e coincide com $x \vee y$. Portanto, $(R; \leq)$ é um reticulado.

*(ii)* Suponha-se que $(R; \leq)$ é um reticulado. Já foi observado anteriormente que ambas as operações binárias $\wedge$ e $\vee$ estão, de facto, bem definidas, pelo que $(R; \wedge, \vee)$ é uma álgebra. É simples verificar que as operações $\wedge$ e $\vee$ satisfazem a idempotência, a comutatividade e a associatividade. A absorção também é verificada. De facto, dados $x, y \in R$, é claro que $x \leq x$ e $x \leq \sup\{x, y\}$, ou seja, $x$ é um minorante de $\{x, \sup\{x, y\}\}$. É imediato que, tomando um qualquer minorante $z$ de $\{x, \sup\{x, y\}\}$, se tem $z \leq x$. Logo,

$$\inf\{x, \sup\{x, y\}\} = x,$$

ou seja,

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

Analogamente se prova que

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

Portanto, a álgebra $(R; \wedge, \vee)$ é um reticulado. Finalmente, pela Proposição 0.1.13, é imediato que

$$x \leq y \iff x = x \wedge y \iff x \vee y = y,$$

para quaisquer $x, y \in R$. □

Atendendo ao resultado estabelecido no teorema anterior, ao longo deste trabalho, não se fará distinção entre tratar um reticulado como uma álgebra, usando a notação $(R; \wedge, \vee)$, e tratá-lo como um c.p.o., usando a notação $(R; \leq)$, a não ser que tal seja necessário. Assim, escrever-se-á simplesmente $R$ significando $(R; \wedge, \vee)$ e $(R; \leq)$, simultaneamente.

Todos os conceitos e resultados estudados na secção 0.2 podem ser especificados para o caso dos reticulados definidos como álgebras e adaptados, segundo o Teorema 0.3.4, para o caso dos reticulados tratados como c.p.o.. Apresentam-se, de seguida, alguns deles, no sentido de introduzir a notação estabelecida no caso dos reticulados.

### 0.3.2 Homomorfismos, sub-reticulados, produtos diretos

**Definição 0.3.5.** Sejam $(R; \wedge^R, \vee^R)$ e $(S; \wedge^S, \vee^S)$ reticulados. Uma aplicação $\varphi$ de $R$ em $S$ tal que, para quaisquer $x, y \in R$,

$$\varphi(x \wedge^R y) = \varphi(x) \wedge^S \varphi(y) \;\text{ e }\; \varphi(x \vee^R y) = \varphi(x) \vee^S \varphi(y),$$

diz-se um *homomorfismo de reticulados*.

Tendo em conta o que foi estudado na secção anterior, facilmente se definem os conceitos de *monomorfismo/ epimorfismo/ isomorfismo/ endomorfismo de reticulados*, *imagem homomorfa de um reticulado* e de *reticulados isomorfos*.

**Proposição 0.3.6.** *Sejam $(R; \wedge^R, \vee^R)$ e $(S; \wedge^S, \vee^S)$ reticulados e $\leq^R$ e $\leq^S$ as relações de ordem associadas, respetivamente, a $(R; \wedge^R, \vee^R)$ e a $(S; \wedge^S, \vee^S)$. Então, os reticulados $R$ e $S$ são isomorfos se e só se os c.p.o. $(R, \leq^R)$ e $(S, \leq^S)$ são isomorfos.*

O termo sub-reticulado é usado para designar uma subálgebra de um reticulado.

**Definição 0.3.7.** Seja $(R; \wedge, \vee)$ um reticulado. Uma álgebra $(S; \wedge^S, \vee^S)$ de tipo $(2, 2)$ diz-se um *sub--reticulado de* $(R; \wedge, \vee)$ se $(S; \wedge^S, \vee^S)$ é uma subálgebra de $(R; \wedge, \vee)$.

Seja $(R; \wedge, \vee)$ um reticulado. Se $(S; \wedge^S, \vee^S)$ é um sub-reticulado de $R$, então $S$ é fechado para as operações $\wedge$ e $\vee$ de $R$; além disso, para quaisquer $x, y \in S$, $x \wedge^S y = x \wedge^R y$ e $x \vee^S y = x \vee^R y$. Caso $(S; \wedge^S, \vee^S)$ seja um sub-reticulado de $(R; \wedge^R, \vee^R)$, é usual dizer-se apenas que $S$ é um sub-reticulado de $R$.

É muito simples verificar o resultado seguinte, o qual afirma que qualquer imagem homomorfa de um reticulado é um sub-reticulado.

**Proposição 0.3.8.** *Sejam $R$ e $S$ dois reticulados quaisquer e $\varphi$ um homomorfismo de $R$ em $S$. Então, $\varphi(R)$ é um sub-reticulado de $S$.*

Os subconjuntos de um reticulado a seguir definidos, designados por intervalos, são exemplos de subconjuntos fechados para as operações do reticulado e, portanto, são o universo de sub-reticulados desse reticulado.

**Definição 0.3.9.** Seja $R$ um reticulado. Um subconjunto de $R$ da forma

$$\{x \in R \mid a \leq x \leq b\},$$

onde $a$ e $b$ são elementos de $R$ tais que $a \leq b$, diz-se um *intervalo de* $R$ e representa-se por $[a, b]$.

É simples perceber que, se $[a, b]$ é um intervalo definido num reticulado $(R; \wedge, \vee)$, então a álgebra $([a, b]; \wedge', \vee')$, onde $\wedge'$ e $\vee'$ são as operações binárias definidas por

$$x \wedge' y = x \wedge y \quad \text{e} \quad x \vee' y = x \vee y,$$

para quaisquer $x, y \in [a, b]$, é um sub-reticulado de $R$.

O resultado seguinte estabelece que a classe dos reticulados é fechada para a formação de produtos diretos.

**Proposição 0.3.10.** *Sejam $(R; \wedge^R, \vee^R)$ e $(S; \wedge^S, \vee^S)$ reticulados. A álgebra $(R \times S; \sqcap, \sqcup)$, onde $\sqcap$ e $\sqcup$ são as operações definidas por*

$$(x, z) \sqcap (y, w) = (x \wedge^R y, z \wedge^S w) \ \ e \ \ (x, z) \sqcup (y, w) = (x \vee^R y, z \vee^S w),$$

*para quaisquer $(x, z), (y, w) \in R \times S$, é um reticulado.*

**Definição 0.3.11.** Sejam $R$ e $S$ reticulados. Chama-se *produto direto de $R$ por $S$* ao reticulado definido na proposição anterior.

Generalizando, obtém-se o seguinte resultado.

**Proposição 0.3.12.** *Sejam $I$ um conjunto e $((R_i; \wedge^i, \vee^i))_{i \in I}$ uma família de reticulados. A álgebra $(\prod_{i \in I} R_i; \sqcap, \sqcup)$, onde $\sqcap$ e $\sqcup$ são as operações definidas por*

$$(x_1 \sqcap x_2)(i) = x_1(i) \wedge^i x_2(i) \ \ e \ \ (x_1 \sqcup x_2)(i) = x_1(i) \vee^i x_2(i),$$

*para cada $i \in I$, para quaisquer $x_1, x_2 \in \prod_{i \in I} R_i$, é um reticulado.*

**Definição 0.3.13.** Sejam $I$ um conjunto e $((R_i; \wedge^i, \vee^i))_{i \in I}$ uma família de reticulados. Chama-se *produto direto de $(R_i)_{i \in I}$* ao reticulado definido no resultado anterior.

### 0.3.3 Ideais e filtros

De entre os subconjuntos de um reticulado $R$ que são fechados para as operações de $R$, destacam-se os ideais e filtros de $R$, devido à sua importância no estudo de reticulados.

**Definição 0.3.14.** Seja $(R; \wedge, \vee)$ um reticulado.

- Um subconjunto não vazio $I$ de $R$ diz-se um *ideal de $R$* se $I$ for fechado para as operações $\wedge$ e $\vee$ de $R$ e, para quaisquer $x \in R$ e $a \in I$, $x \wedge a \in I$. No caso de $I \subset R$, diz-se que $I$ é um *ideal próprio de $R$*. Um ideal próprio $I$ de $R$ diz-se *primo* se, para quaisquer $x, y \in R$,

$$x \wedge y \in I \implies (x \in I \ \text{ou} \ y \in I).$$

- Um subconjunto não vazio $F$ de $R$ diz-se um *filtro de* $R$ se $F$ for fechado para as operações $\wedge$ e $\vee$ de $R$ e, para quaisquer $x \in R$ e $b \in F$, $x \vee b \in F$. No caso de $F \subset R$, diz-se que $F$ é um *filtro próprio de* $R$. Um filtro próprio $F$ de $R$ diz-se *primo* se, para quaisquer $x, y \in R$,

$$x \vee y \in F \implies (x \in F \text{ ou } y \in F).$$

É simples verificar que, se $I$ é um ideal de um reticulado $(R; \wedge, \vee)$, então a álgebra $(I; \wedge^I, \vee^I)$, onde as operações $\wedge^I$ e $\vee^I$ são, respetivamente, as restrições de $\wedge$ e $\vee$ a $I$, é um sub-reticulado de $R$.

O mesmo se pode concluir sobre os filtros.

**Definição 0.3.15.** Seja $R$ um reticulado. Chama-se *espectro de* $R$, e representa-se por $\mathrm{Esp}(R)$, ao conjunto de todos os ideais primos de $R$.

O lema seguinte descreve outra forma de caraterizar um ideal de um reticulado.

**Lema 0.3.16** (cf. [7], Lemma 5 (i), p. 32)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Um subconjunto não vazio $I$ de $R$ é um ideal de $R$ se e só se ambas as condições seguintes são satisfeitas:*

*(i)* $\forall a, b \in I,\ a \vee b \in I;$

*(ii)* $\forall x \in R,\ \forall a \in I,\ x \leq a \implies x \in I.$

*Demonstração.* Seja $I$ um subconjunto não vazio de $R$.

Suponha-se, primeiramente, que $I$ é um ideal de $R$. A condição *(i)* é claramente satisfeita, visto que $I$ é fechado para as operações de $R$. Sejam $x \in R$ e $a \in I$ tais que $x \leq a$. Então, $x = x \wedge a$. Ora, pela definição de ideal, $x \wedge a \in I$. Logo, $x \in I$ e, por conseguinte, a condição *(ii)* também é satisfeita.

Reciprocamente, admita-se que as condições *(i)* e *(ii)* são válidas. Sejam $a, b \in I$. Por *(i)*, $a \vee b \in I$. Como $a \wedge b \in R$ e $a \wedge b \leq a$, então, por *(ii)*, $a \wedge b \in I$. Logo, $I$ é fechado para as operações de $R$. Além disso, dados $x \in R$ e $a \in I$, visto que $x \wedge a \leq a$, então, novamente por *(ii)*, $x \wedge a \in I$. Portanto, conclui-se que $I$ é um ideal de $R$. □

Não é difícil obter o resultado dual do lema anterior, o qual estabelece uma caraterização alternativa de um filtro de um reticulado.

Sendo $R$ um reticulado, representa-se o conjunto de todos os ideais de $R$ por $\mathrm{Id}(R)$, sobre o qual pode ser definido um reticulado, tal como estabelece o seguinte teorema.

**Teorema 0.3.17** (cf. [2], Theorem 2.6, p. 27)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, o conjunto $\mathrm{Id}(R)$, quando ordenado pela relação de inclusão, é um reticulado, onde, para quaisquer $I, J \in \mathrm{Id}(R)$,*

*(a)* $I \wedge J = I \cap J;$

*(b)* $I \vee J = \{x \in R \mid x \leq a \vee b$, *para alguns* $a \in I$ *e* $b \in J\}$.

*Demonstração.* Sejam $I, J \in \mathrm{Id}(R)$.

Primeiramente, como $I \neq \emptyset$ e $J \neq \emptyset$, existem $a \in I$ e $b \in J$. Então, uma vez que $I, J \in \mathrm{Id}(R)$, segue que $a \wedge b \in I$ e $a \wedge b \in J$, pelo que $a \wedge b \in I \cap J$. Logo, $I \cap J$ é um subconjunto não vazio de $R$. Dados $a, b \in I \cap J$, tem-se que $a, b \in I$ e $a, b \in J$. Assim, como $I$ e $J$ são fechados para as operações de $R$, segue que $a \vee b \in I$ e $a \vee b \in J$, ou seja, $a \vee b \in I \cap J$. Sejam, agora, $x \in R$ e $a \in I \cap J$ tais que $x \leq a$. Então, como $a \in I$ e $I \in \mathrm{Id}(R)$, tem-se, por *(ii)* do Lema 0.3.16, que $x \in I$. De forma análoga, também se confirma que $x \in J$. Logo, $x \in I \cap J$. Portanto, pelo Lema 0.3.16, $I \cap J \in \mathrm{Id}(R)$. Como $I \cap J$ é um minorante de $\{I, J\}$ e, para qualquer $C \in \mathrm{Id}(R)$ tal que $C \subseteq I$ e $C \subseteq J$, se tem $C \subseteq I \cap J$, conclui-se que existe ínfimo de $\{I, J\}$, o qual é dado por $I \cap J$, pelo que $I \wedge J = I \cap J$.

Considerando, agora,

$$L = \{x \in R \mid x \leq a \vee b, \text{ para alguns } a \in I \text{ e } b \in J\},$$

tem-se que $L \neq \emptyset$. De facto, como $I \neq \emptyset$ e $J \neq \emptyset$, existem $a \in I$ e $b \in J$. Assim, uma vez que $a \leq a \vee b$, $a \in L$. Sejam, agora, $x, y \in L$. Então, $x \leq a \vee b$ e $y \leq c \vee d$, para certos $a, c \in I$ e $b, d \in J$. Como $I, J \in \mathrm{Id}(R)$, então $a \vee c \in I$ e $b \vee d \in J$ e, uma vez que

$$\begin{aligned} x \vee y &\leq (a \vee b) \vee (c \vee d) && \text{[Proposição 0.1.14]} \\ &= (a \vee c) \vee (b \vee d), && \text{[comutatividade e associatividade]} \end{aligned}$$

e $x \vee y \in R$, tem-se que $x \vee y \in L$. Sejam, agora, $x \in R$ e $c \in L$ tais que $x \leq c$. Então, $c \leq a \vee b$, para certos $a \in I$ e $b \in J$. Logo, por transitividade, $x \leq a \vee b$, pelo que $x \in L$. Portanto, pelo Lema 0.3.16, $L \in \mathrm{Id}(R)$. Também se prova que $L$ é um majorante de $\{I, J\}$: de facto, dado $a \in I$, tem-se que, para qualquer $b \in J$, $a \leq a \vee b$ e, portanto, visto que $J \neq \emptyset$, $a \in L$. Logo, $I \subseteq L$. Analogamente se verifica que $J \subseteq L$. Considere-se, agora, qualquer $D \in \mathrm{Id}(R)$ tal que $I \subseteq D$ e $J \subseteq D$. Seja $c \in L$. Então, $c \leq a \vee b$, para certos $a \in I$ e $b \in J$. Assim, $a, b \in D$, donde, por $D \in \mathrm{Id}(R)$, resulta que $a \vee b \in D$. Logo, por *(ii)* do Lema 0.3.16, $c \in D$. Portanto, $L \subseteq D$. Conclui-se, assim, que existe supremo de $\{I, J\}$, o qual é dado por $L$, pelo que $I \vee J = L$.

Confirma-se, enfim, que $\mathrm{Id}(R)$, quando ordenado pela relação de inclusão de conjuntos, constitui um reticulado. □

**Definição 0.3.18.** Seja $R$ um reticulado. Ao reticulado $(\mathrm{Id}(R), \subseteq)$ dá-se a designação de reticulado dos ideais de $R$.

Observe-se que, dado um reticulado $R$, o reticulado $(\mathrm{Id}(R), \subseteq)$, enquanto estrutura algébrica, é a álgebra $(\mathrm{Id}(R), \wedge, \vee)$, onde $\wedge$ e $\vee$ são as operações binárias definidas de acordo com o indicado no Teorema 0.3.17.

Dado um reticulado $R$, denota-se o conjunto de todos os filtros de $R$ por $\mathrm{Fil}(R)$ e, por dualidade, tem-se o resultado seguinte.

**Teorema 0.3.19.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, o conjunto $\mathrm{Fil}(R)$, quando ordenado pela relação de inclusão, é um reticulado, onde, para quaisquer $F, G \in \mathrm{Fil}(R)$,*

*(a)* $F \wedge G = F \cap G$;

*(b)* $F \vee G = \{x \in R \mid a \wedge b \leq x,$ *para certos* $a \in F$ *e* $b \in G\}$.

**Definição 0.3.20.** Seja $R$ um reticulado. Chama-se *reticulado dos filtros de $R$* ao reticulado $(\mathrm{Fil}(R); \subseteq)$.

Apresenta-se, de seguida, a noção de ideal gerado por um subconjunto não vazio de um reticulado.

Observe-se, primeiramente, que, dado um reticulado $R$, a interseção de uma família de ideais de $R$ continua a ser um ideal de $R$; além disso, dado um subconjunto não vazio $S$ de $R$, existe sempre um ideal de $R$ que contém $S$: basta tomar o próprio $R$.

**Proposição 0.3.21.** *Sejam $R$ um reticulado e $S$ um subconjunto não vazio de $R$. O conjunto dado por*

$$\bigcap\{J \in \mathrm{Id}(R) \mid S \subseteq J\}$$

*é um ideal de $R$, sendo, aliás, o menor ideal de $R$ que contém $S$.*

**Definição 0.3.22.** Sejam $R$ um reticulado e $S$ um subconjunto não vazio de $R$. Chama-se *ideal de $R$ gerado por $S$*, e representa-se por $\mathrm{id}(S)$, ao menor ideal de $R$ que contém $S$.

Dados um reticulado $R$ e $x \in R$, escreve-se $\mathrm{id}(x)$ para denotar $\mathrm{id}(\{x\})$.

**Proposição 0.3.23** (cf. [7], Lemma 5 (ii), pp. 32–33)**.** *Sejam $(R; \wedge, \vee)$ um reticulado e $S$ um subconjunto não vazio de $R$. Então,*

$$\mathrm{id}(S) = \{x \in R \mid x \leq s_1 \vee \cdots \vee s_n, \text{ para alguns } n \in \mathbb{N} \text{ e } s_1, \ldots, s_n \in S\}.$$

*Demonstração.* Denote-se o conjunto

$$\{x \in R \mid x \leq s_1 \vee \cdots \vee s_n, \text{ para alguns } n \in \mathbb{N} \text{ e } s_1, \ldots, s_n \in S\}$$

por $L$. Claramente, $L$ é não vazio e, usando o Lema 0.3.16, é muito simples justificar que $L$ é um ideal de $R$. Também é óbvio que $S \subseteq L$. Seja $I$ um ideal de $R$ tal que $S \subseteq I$. Ora, dado $x \in L$, tem-se que

$$x \leq s_1 \vee \cdots \vee s_n,$$

para certos $n \in \mathbb{N}$ e $s_1, \ldots, s_n \in S$. Assim, $s_1, \ldots, s_n \in I$ e, por aplicação sucessiva de *(i)* do Lema 0.3.16,

$$s_1 \vee \cdots \vee s_n \in I.$$

Logo, por *(ii)* do mesmo lema, tem-se que $x \in I$, pelo que $L \subseteq I$. Portanto, conclui-se que, de facto, $\mathrm{id}(S) = L$. □

Como consequência imediata da proposição anterior, tem-se o seguinte resultado.

**Corolário 0.3.24** (cf. [7], Lemma 5 (iii), pp. 32–33)**.** *Sejam $(R; \wedge, \vee)$ um reticulado e $x \in R$. Então,*

$$\mathrm{id}(x) = \{y \in R \mid y \leq x\} = \{x \wedge y \mid y \in R\}.$$

**Definição 0.3.25.** Sejam $R$ um reticulado e $x \in R$. Dá-se a designação de *ideal principal de $R$ gerado por $x$* ao ideal $\mathrm{id}(x)$.

**Teorema 0.3.26** (cf. [7], Corollary 7, p. 33)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, a aplicação $\phi$ de $R$ em $\mathrm{Id}(R)$ definida por*

$$\phi(x) = \mathrm{id}(x)$$

*é um monomorfismo de reticulados de $(R; \wedge, \vee)$ em $(\mathrm{Id}(R); \wedge, \vee)$.*

*Demonstração.* Sejam $x, y \in R$.

Claramente, a aplicação $\phi$ está bem definida, uma vez que, sempre que $x = y$, se tem $\mathrm{id}(x) = \mathrm{id}(y)$. Suponha-se, agora, que $\mathrm{id}(x) = \mathrm{id}(y)$. Então, para qualquer $a \in R$,

$$a \leq x \iff a \leq y.$$

Assim, como $x \leq x$, tem-se também que $x \leq y$. Além disso, como $y \leq y$, então $y \leq x$. Logo, pela antissimetria, $x = y$. Portanto, a aplicação $\phi$ é injetiva.

Por último, mostre-se que $\phi$ é um morfismo de reticulados.

Seja

$$z \in \mathrm{id}(x) \wedge \mathrm{id}(y) = \mathrm{id}(x) \cap \mathrm{id}(y).$$

Assim, $z \leq x$ e $z \leq y$. Logo, $z \leq x \wedge y$, pelo que

$$z \in \mathrm{id}(x \wedge y).$$

Reciprocamente, se

$$z \in \mathrm{id}(x \wedge y),$$

então $z \leq x \wedge y$. Como $x \wedge y \leq x$ e $x \wedge y \leq y$, então $z \leq x$ e $z \leq y$, pelo que

$$z \in \mathrm{id}(x) \cap \mathrm{id}(y) = \mathrm{id}(x) \wedge \mathrm{id}(y).$$

Portanto,

$$\mathrm{id}(x) \wedge \mathrm{id}(y) = \mathrm{id}(x \wedge y),$$

ou seja,

$$\phi(x) \wedge \phi(y) = \phi(x \wedge y).$$

Seja, agora,

$$z \in \mathrm{id}(x) \vee \mathrm{id}(y).$$

Assim, pelo Teorema 0.3.17, $z \leq a \vee b$, para certos $a \in \mathrm{id}(x)$ e $b \in \mathrm{id}(y)$. Como $a \leq x$ e $b \leq y$, tem-se $a \vee b \leq x \vee y$, logo $z \leq x \vee y$, ou seja,

$$z \in \mathrm{id}(x \vee y).$$

Reciprocamente, se

$$z \in \mathrm{id}(x \vee y),$$

então $z \leq x \vee y$, com $x \in \mathrm{id}(x)$ e $y \in \mathrm{id}(y)$. Assim,

$$z \in \mathrm{id}(x) \vee \mathrm{id}(y).$$

Logo,

$$\mathrm{id}(x) \vee \mathrm{id}(y) = \mathrm{id}(x \vee y),$$

ou seja,

$$\phi(x) \vee \phi(y) = \phi(x \vee y).$$

Portanto, $\phi$ é, de facto, um monomorfismo de reticulados. □

Dado um reticulado $R$, definem-se, por dualidade, os conceitos de *filtro de $R$ gerado por $S$*, sendo $S$ um subconjunto não vazio de $R$, e *filtro principal de $R$ gerado por $x$*, onde $x \in R$, os quais são representados, respetivamente, por $\mathrm{fil}(S)$ e $\mathrm{fil}(x)$, bem como se estabelecem os resultados duais dos anteriores, envolvendo estes conceitos.

### 0.3.4 Relações de congruência

Também as relações de congruência têm um papel relevante no estudo de reticulados.

**Definição 0.3.27.** Sejam $(R; \wedge, \vee)$ um reticulado e $\theta \in \mathrm{Equ}(R)$. Diz-se que $\theta$ é uma *relação de congruência em $R$* ou, simplesmente, *congruência em $R$* se, para quaisquer $x, y, z, w \in R$,

$$(x\theta z \text{ e } y\theta w) \implies ((x \wedge y)\theta(z \wedge w) \text{ e } (x \vee y)\theta(z \vee w)).$$

Os resultados seguintes são úteis no estudo de congruências.

**Lema 0.3.28** (cf. [9], Theorem 9.2, p. 181)**.** *Sejam $(R; \wedge, \vee)$ um reticulado e $\theta \in \mathrm{Equ}(R)$. A relação $\theta$ é uma congruência em $R$ se e só se, para quaisquer $x, y, z \in R$,*

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

**Lema 0.3.29** (cf. [7], Lemma 11, pp. 37–38)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Uma relação binária $\theta$ em $R$ é uma congruência se e só se cada uma das condições seguintes é verificada:*

*(i)* *$\theta$ é reflexiva;*

*(ii)* *para quaisquer $x, y \in R$,*

$$x\theta y \iff (x \wedge y)\theta(x \vee y);$$

*(iii)* *para quaisquer $x, y, z \in R$ tais que $x \leq y \leq z$,*

$$(x\theta y \text{ e } y\theta z) \implies x\theta z;$$

*(iv)* *para quaisquer $x, y \in R$ tais que $x \leq y$,*

$$x\theta y \implies (\forall w \in R,\ (x \wedge w)\theta(y \wedge w) \text{ e } (x \vee w)\theta(y \vee w)).$$

*Demonstração.* Seja $\theta$ uma relação binária em $R$.

Suponha-se, primeiramente, que $\theta$ é uma congruência. É óbvio que *(i)* e *(iii)* são satisfeitas, além de que *(iv)* é uma consequência imediata do Lema 0.3.28. Mostre-se que *(ii)* também se verifica. Sejam $x, y \in R$. Supondo que $x\theta y$, segue, pelo Lema 0.3.28, que $(x \wedge x)\theta(y \wedge x)$, pelo que $x\theta(x \wedge y)$. Dualmente, $x\theta(x \vee y)$. Logo, pela simetria e transitividade de $\theta$, $(x \wedge y)\theta(x \vee y)$. Reciprocamente, suponha-se que $(x \wedge y)\theta(x \vee y)$. Assim, usando novamente o Lema 0.3.28, tem-se que

$$((x \wedge y) \wedge x)\theta((x \vee y) \wedge x),$$

donde $(x \wedge y)\theta x$. Analogamente, $(x \wedge y)\theta y$. Logo, pela simetria e transitividade de $\theta$, $x\theta y$.

Admita-se, agora, que a relação $\theta$ satisfaz *(i)–(iv)*. A reflexividade de $\theta$ é garantida por *(i)*. Quanto à simetria de $\theta$, é facilmente retirada de *(ii)*: dados $x, y \in R$ tais que $x\theta y$, então $(x \wedge y)\theta(x \vee y)$, donde, pela comutatividade de $\wedge$ e de $\vee$, segue que $(y \wedge x)\theta(y \vee x)$, pelo que $y\theta x$. Prove-se, agora, que $\theta$ é transitiva. Nesse sentido, repare-se, primeiramente, que, para quaisquer $x, y, a, b \in R$ tais que $x \leq a \leq y$, $x \leq b \leq y$ e $x\theta y$, tem-se que $a\theta b$. De facto, como $x\theta y$ e $x \leq y$, então, por *(iv)*,

$$(x \wedge (a \vee b))\theta(y \wedge (a \vee b)).$$

Claramente, $x \wedge (a \vee b) = x$ e $y \wedge (a \vee b) = a \vee b$. Logo,

$$x\theta(a \vee b).$$

Seguidamente, como $x \leq a \vee b$, então, por *(iv)*,

$$(x \vee (a \wedge b))\theta((a \vee b) \vee (a \wedge b)).$$

É claro que $(a \vee b) \vee (a \wedge b) = a \vee b$. Além disso, tem-se $x \leq a \wedge b$, pelo que $x \vee (a \wedge b) = a \wedge b$. Por conseguinte,

$$(a \wedge b)\theta(a \vee b).$$

Portanto, por *(ii)*, $a\theta b$. Sejam, agora, $x, y, z \in R$ tais que $x\theta y$ e $y\theta z$. Assim, por *(ii)*,

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

Uma vez que $x \wedge y \leq x \vee y$, segue, por *(iv)*, que

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

e, consequentemente, como $y \wedge z \leq x \vee y$, tem-se

$$(x \wedge y \wedge z)\theta(y \wedge z).$$

De forma semelhante, obtém-se que

$$(y \vee z)\theta(x \vee y \vee z).$$

Ora, como

$$x \wedge y \wedge z \leq y \wedge z \leq y \vee z \leq x \vee y \vee z$$

e

$$(x \wedge y \wedge z)\theta(y \wedge z), \ (y \wedge z)\theta(y \vee z) \text{ e } (y \vee z)\theta(x \vee y \vee z),$$

então, aplicando *(iii)* duas vezes, tem-se que

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

Agora, como $u = x \wedge y \wedge z$, $v = x \vee y \vee z$, $x$ e $z$ são elementos de $R$ tais que $u \leq x \leq v$, $u \leq z \leq v$ e $u\theta v$, então, tendo em conta o que foi provado anteriormente, tem-se que $x\theta z$, concluindo, assim, a prova da transitividade de $\theta$. Portanto, $\theta \in \mathrm{Equ}(R)$. Sejam, agora, $x, y, z \in R$ com $x\theta y$. Então, por *(ii)*, $(x \wedge y)\theta(x \vee y)$, donde, por *(iv)*, segue que

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

e

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

Assim, uma vez que $u = x \wedge y \wedge z$, $v = (x \vee y) \wedge z$, $a = x \wedge z$, $b = y \wedge z$ são elementos de $R$ tais que $u \leq a \leq v$, $u \leq b \leq v$ e $u\theta v$, tem-se que $a\theta b$, ou seja, $(x \wedge z)\theta(y \wedge z)$. Mais, visto que $r = (x \wedge y) \vee z$, $s = x \vee y \vee z$, $c = x \vee z$ e $d = y \vee z$ são elementos de $R$ tais que $r \leq c \leq s$, $r \leq d \leq s$ e $r\theta s$, tem-se que $c\theta d$, ou seja, $(x \vee z)\theta(y \vee z)$. Portanto, pelo Lema 0.3.28, $\theta$ é uma congruência. □

O conjunto de todas as congruências num reticulado $R$ é denotado por $\mathrm{Con}(R)$. Observe-se que o par $(\mathrm{Con}(R), \subseteq)$ é um c.p.o..

O resultado seguinte é muito simples de provar, mas facilita a demonstração do teorema que se lhe segue.

**Lema 0.3.30** (cf. [7], Theorem 12, p. 38)**.** *Seja $R$ um reticulado. Então, para qualquer $X \subseteq \mathrm{Con}(R)$, $\bigcap X \in \mathrm{Con}(R)$.*

**Teorema 0.3.31** (cf. [7], Theorem 12, pp. 38–39)**.** *Seja $(R; \wedge, \vee)$ um reticulado. O c.p.o. $(\mathrm{Con}(R); \subseteq)$ é um reticulado, onde, para quaisquer $\theta, \vartheta \in \mathrm{Con}(R)$,*

- $\theta \wedge \vartheta = \theta \cap \vartheta$*;*
- $\theta \vee \vartheta = \left\{ (x, y) \in R^2 \;\middle|\; \begin{array}{l} \exists\, n \in \mathbb{N},\ \exists\, r_1, r_2, \ldots, r_n \in R : \\ x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_n = x \vee y, \\ \forall\, i \in \{1, 2, \ldots, n-1\},\ r_i \theta r_{i+1} \ \textit{ou}\ r_i \vartheta r_{i+1} \end{array} \right\}.$

*Demonstração.* Sejam $\theta, \vartheta \in \mathrm{Con}(R)$.

Tendo em conta o lema anterior e as propriedades da interseção de conjuntos, é muito simples verificar que $\theta \cap \vartheta$ é o ínfimo de $\{\theta, \vartheta\}$, pelo que $\theta \wedge \vartheta = \theta \cap \vartheta$.

Represente-se por $\xi$ a relação binária dada por

$$\left\{ (x, y) \in R^2 \;\middle|\; \begin{array}{l} \exists\, n \in \mathbb{N},\ \exists\, r_1, r_2, \ldots, r_n \in R : \\ x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_n = x \vee y, \\ \forall\, i \in \{1, 2, \ldots, n-1\},\ r_i \theta r_{i+1} \ \text{ou}\ r_i \vartheta r_{i+1} \end{array} \right\}.$$

Prove-se, primeiramente, que $\xi \in \mathrm{Con}(R)$. Para tal, basta mostrar que $\xi$ observa cada uma das condições *(i)–(iv)* do Lema 0.3.29. Ora, é óbvio que $\xi$ é reflexiva, ou seja, satisfaz *(i)* do Lema 0.3.29. Também não é difícil verificar que $\xi$ satisfaz a condição *(ii)* do mesmo lema. Prove-se, agora, *(iii)*. Sejam $x, y, z \in R$ tais que $x \leq y \leq z$, $x \xi y$ e $y \xi z$. Por um lado, existem $r_1, r_2, \ldots, r_n \in R$, para algum $n \in \mathbb{N}$, tais que

$$x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_n = x \vee y$$

e, para cada $i \in \{1, 2, \ldots, n-1\}$, $r_i \theta r_{i+1}$ ou $r_i \vartheta r_{i+1}$. Por outro lado, existem $s_1, s_2, \ldots, s_m \in R$, para algum $m \in \mathbb{N}$, tais que

$$y \wedge z = s_1 \leq s_2 \leq \cdots \leq s_m = y \vee z$$

e, para cada $j \in \{1, 2, \ldots, m-1\}$, $s_j \theta s_{j+1}$ ou $s_j \vartheta s_{j+1}$. Ora,

$$\begin{aligned} x \wedge z = x = x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_{n-1} \\ \leq r_n = x \vee y = y = y \wedge z = s_1 \leq s_2 \leq \cdots \leq s_{m-1} \\ \leq s_m = y \vee z = z = x \vee z, \end{aligned}$$

ou seja,

$$x \wedge z = r_1 \leq r_2 \leq \cdots \leq r_n = s_1 \leq s_2 \leq \cdots \leq s_m = x \vee z.$$

Defina-se $p = n + m - 1 \in \mathbb{N}$ e $t_1, t_2, \ldots, t_p$ como sendo os elementos de $R$ tais que, para cada $k \in \{1, 2, \ldots, p\}$,

*(a)* $t_k = r_k$ se $k \in \{1, 2, \ldots, n\}$;

*(b)* $t_k = s_{k-n+1}$ se $k \in \{n+1, n+2, \ldots, p\}$.

Assim, tem-se que

$$x \wedge z = t_1 \leq t_2 \leq \cdots \leq t_p = x \vee z,$$

onde, para cada $l \in \{1, 2, \ldots, p-1\}$, se tem, claramente, que $t_l \theta t_{l+1}$ ou $t_l \vartheta t_{l+1}$. Logo, $x \xi z$. Portanto, a condição *(iii)* do Lema 0.3.29 é observada por $\xi$. Para mostrar que a propriedade *(iv)* do Lema 0.3.29 também se verifica, tomem-se arbitrariamente $x, y \in R$ tais que $x \leq y$ e $x \xi y$. Então, existem $r_1, r_2, \ldots, r_n \in R$, para algum $n \in \mathbb{N}$, tais que

$$x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_n = x \vee y$$

e, para cada $i \in \{1, 2, \ldots, n-1\}$, $r_i \theta r_{i+1}$ ou $r_i \vartheta r_{i+1}$. Seja $w \in R$. Ora, pela Proposição 0.1.14,

$$(x \wedge y) \wedge w = r_1 \wedge w \leq r_2 \wedge w \leq \cdots \leq r_n \wedge w = (x \vee y) \wedge w;$$

além disso, tem-se, claramente, que

$$(x \wedge w) \wedge (y \wedge w) = (x \wedge y) \wedge w;$$

também não é difícil ver que

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

Assim, definindo $s_1, s_2, \ldots, s_n$ como sendo os elementos de $R$ tais que, para cada $k \in \{1, 2, \ldots, n\}$, $s_k = r_k \wedge w$, tem-se que

$$(x \wedge w) \wedge (y \wedge w) = s_1 \leq s_2 \leq \cdots \leq s_n = (x \wedge w) \vee (y \wedge w),$$

onde, para cada $j \in \{1, 2, \ldots, n-1\}$, $s_j \theta s_{j+1}$ ou $s_j \vartheta s_{j+1}$, uma vez que $\theta$ e $\vartheta$ são congruências em $R$. Logo, $(x \wedge w) \xi (y \wedge w)$. Por analogia, também se prova que $(x \vee w) \xi (y \vee w)$. Conclui-se, assim, que $\xi \in \mathrm{Con}(R)$.

Mostre-se, agora, que $\xi$ é o supremo de $\{\theta, \sigma\}$. Sejam $x, y \in R$ tais que $x \theta y$. Então, por *(ii)* do Lema 0.3.29, tem-se $(x \wedge y) \theta (x \vee y)$. Como, além disso, $x \wedge y \leq x \vee y$, segue que $x \xi y$. Logo, $\theta \subseteq \xi$. Por argumentos semelhantes, também se mostra que $\vartheta \subseteq \xi$. Falta verificar que $\xi$ é a menor congruência nestas condições. Seja $\zeta \in \mathrm{Con}(R)$ tal que $\theta \subseteq \zeta$ e $\vartheta \subseteq \zeta$. O objetivo é mostrar que $\xi \subseteq \zeta$. Sejam, então, $x, y \in R$ tais que $x\xi y$. Assim, existem $r_1, r_2, \ldots, r_n \in R$, para algum $n \in \mathbb{N}$, tais que

$$x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_n = x \vee y$$

e, para cada $i \in \{1, 2, \ldots, n-1\}$, $r_i\theta r_{i+1}$ ou $r_i\vartheta r_{i+1}$. Por conseguinte, para cada $i \in \{1, 2, \ldots, n-1\}$, $r_i\zeta r_{i+1}$. Pela transitividade de $\zeta$, tem-se que $r_1\zeta r_n$, ou seja, $(x \wedge y)\zeta(x \vee y)$, donde segue, por *(ii)* do Lema 0.3.29, que $x\zeta y$. Efetivamente, $\xi \subseteq \zeta$. Portanto, $\xi$ é o supremo de $\{\theta, \vartheta\}$, pelo que $\theta \vee \vartheta = \xi$.

Fica, assim, concluída a prova de que $(\mathrm{Con}(R); \subseteq)$ é um reticulado. □

**Definição 0.3.32.** Seja $R$ um reticulado. Chama-se *reticulado das congruências em* $R$ ao reticulado $(\mathrm{Con}(R); \subseteq)$.

Observe-se que, de acordo com o que foi estudado na Secção 0.2, o reticulado das congruências de um reticulado é limitado.

Tendo em conta o Teorema 0.3.31, é simples deduzir o seguinte resultado.

**Teorema 0.3.33** (cf. [7], Theorem 37, p. 51)**.** *Sejam* $(R; \wedge, \vee)$ *um reticulado e* $I$ *um conjunto. Então,* $\mathrm{Con}(R)$ *é um reticulado completo e, dada uma qualquer família* $(\theta_i)_{i\in I}$ *de congruências em* $R$*, tem-se*

- $\bigwedge_{i\in I} \theta_i = \bigcap_{i\in I} \theta_i$;
- $\bigvee_{i\in I} \theta_i = \left\{ (x, y) \in R^2 \;\middle|\; \begin{array}{l} \exists\, n \in \mathbb{N},\ \exists\, r_1, r_2, \ldots, r_n \in R : \\ x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_n = x \vee y, \\ \forall\, j \in \{1, 2, \ldots, n-1\},\ \exists\, i \in I : \ r_j\theta_i r_{j+1} \end{array} \right\}$.

Define-se, de seguida, o conceito de congruência gerada por uma relação binária não vazia. Para tal, veja-se, primeiramente, o seguinte resultado.

**Proposição 0.3.34** (cf. [7], Lemma 13, p. 39)**.** *Sejam* $R$ *um reticulado e* $\rho$ *uma relação binária não vazia em* $R$*. O conjunto dado por*

$$\bigcap\{\theta \in \mathrm{Con}(R) \mid \rho \subseteq \theta\}$$

*é uma congruência em* $R$*, sendo, aliás, a menor congruência em* $R$ *que contém* $\rho$*.*

*Demonstração.* Seja

$$\vartheta = \bigcap\{\theta \in \mathrm{Con}(R) \mid \rho \subseteq \theta\}.$$

Pelo Lema 0.3.30, é imediato que $\vartheta \in \mathrm{Con}(R)$. Sendo também óbvio que $\rho \subseteq \vartheta$, resta demonstrar que $\vartheta$ é a menor congruência em $R$ nestas condições. Seja $\xi \in \mathrm{Con}(R)$ tal que $\rho \subseteq \xi$. Por conseguinte,

$$\xi \in \{\theta \in \mathrm{Con}(R) \mid \rho \subseteq \theta\}.$$

Logo, é claro que $\vartheta \subseteq \xi$. Portanto, $\vartheta$ é a menor congruência em $R$ que contém $\rho$. □

**Definição 0.3.35.** Sejam $R$ um reticulado e $\rho$ uma relação binária não vazia em $R$. Chama-se *congruência em $R$ gerada por $\rho$*, e representa-se por $\mathrm{con}(\rho)$, à menor congruência em $R$ que contém $\rho$. Se $\rho = \{(x, y)\}$, para alguns $x, y \in R$, a relação $\mathrm{con}(\rho)$ designa-se por *congruência principal em $R$ gerada por $\{(x, y)\}$*.

Sendo $R$ um reticulado e $x, y \in R$, é usual representar-se a relação $\mathrm{con}(\{(x, y)\})$ por $\mathrm{con}(x, y)$. Além disso, dado um ideal $I$ de $R$, é usual denotar-se a congruência $\mathrm{con}(I^2)$ por $\mathrm{con}(I)$.

O seguinte resultado é uma consequência trivial da condição *(ii)* do Lema 0.3.29.

**Proposição 0.3.36.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, para quaisquer $x, y \in R$,*

$$\mathrm{con}(x, y) = \mathrm{con}(x \wedge y, x \vee y).$$

A proposição anterior é importante, pois dela se conclui que, para o estudo das congruências principais num reticulado, basta que sejam consideradas aquelas que são geradas por pares de elementos comparáveis.

Com o conceito de congruência principal, é possível estabelecer a seguinte forma de descrever uma congruência gerada por alguma relação binária não vazia.

**Proposição 0.3.37** (cf. [7], Lemma 14, p. 39)**.** *Sejam $R$ um reticulado e $\rho$ uma relação binária não vazia em $R$. Então,*

$$\mathrm{con}(\rho) = \bigvee\{\mathrm{con}(x, y) \mid x\rho y\}.$$

*Demonstração.* Seja

$$\theta = \bigvee\{\mathrm{con}(x, y) \mid x\rho y\}.$$

Pelo Teorema 0.3.33, é imediato que $\theta \in \mathrm{Con}(R)$. Também não é difícil verificar que $\rho \subseteq \theta$. De facto, para quaisquer $x, y \in R$ tais que $x\rho y$, tem-se $\mathrm{con}(x, y) \subseteq \theta$, logo $x\theta y$. Seja, agora, $\vartheta \in \mathrm{Con}(R)$ tal que $\rho \subseteq \vartheta$. Então, para todo $(x, y) \in \rho$, tem-se $(x, y) \in \vartheta$, pelo que $\mathrm{con}(x, y) \subseteq \vartheta$. Logo $\theta \subseteq \vartheta$. Portanto, $\mathrm{con}(\rho) = \theta$. □

**Proposição 0.3.38** (cf. [9], Theorem 9.10, pp. 189–190)**.** *Sejam $(R; \wedge, \vee)$ um reticulado e $\theta$ uma congruência em $R$. O conjunto quociente de $R$ por $\theta$, $R/\theta$, quando munido das operações $\wedge^\theta$ e $\vee^\theta$ tais que, para quaisquer $x, y \in R$,*

$$[x]_\theta \wedge^\theta [y]_\theta = [x \wedge y]_\theta \text{ e } [x]_\theta \vee^\theta [y]_\theta = [x \vee y]_\theta,$$

*é um reticulado.*

**Definição 0.3.39.** Sejam $(R; \wedge, \vee)$ um reticulado e $\theta \in \mathrm{Con}(R)$. Chama-se *reticulado quociente de $R$ por $\theta$* ao reticulado $(R/\theta; \wedge^\theta, \vee^\theta)$ definido tal como na proposição anterior.

**Definição 0.3.40.** Sejam $R$ um reticulado, $\theta \in \mathrm{Con}(R)$ e $R/\theta$ o reticulado quociente de $R$ por $\theta$. Chama-se *classe de congruência* a qualquer $[x]_\theta \in R/\theta$.

### 0.3.5 Elementos especiais

Existem classes de elementos que desempenham um papel importante no estudo de reticulados. Definem-se seguidamente alguns desses elementos.

**Definição 0.3.41.** Seja $(R; \wedge, \vee)$ um reticulado com elemento mínimo $0$. Um elemento $x$ de $R$ diz-se um *átomo de* $R$ se $0 \prec x$.

Seja $(R; \wedge, \vee)$ um reticulado com elemento mínimo. Representa-se por $\mathrm{At}(R)$ o conjunto de todos os átomos do reticulado $R$. Além disso, dado $x \in R$, representa-se por $\mathrm{at}(x)$ o conjunto de todos os átomos $a$ de $R$ tais que $a \leq x$, ou seja,

$$\mathrm{at}(x) = \{y \in \mathrm{At}(R) \mid y \leq x\}.$$

**Definição 0.3.42.** Seja $(R; \wedge, \vee)$ um reticulado com elemento mínimo $0$. O reticulado $R$ diz-se *atómico* se, para qualquer $x \in R \setminus \{0\}$, existe $a \in \mathrm{At}(R)$ tal que $a \leq x$.

**Exemplo 0.3.43.** Sendo $X$ um conjunto, o reticulado $(\wp(X); \cap, \cup)$ é atómico, onde

$$\mathrm{At}(\wp(X)) = \{\{x\} \mid x \in X\}.$$

Faz-se, agora, um estudo acerca dos elementos irredutíveis de um reticulado.

**Definição 0.3.44.** Seja $(R; \wedge, \vee)$ um reticulado.

- Um elemento $x$ de $R$ diz-se $\wedge$-*irredutível* se $x \neq 1$ (no caso de $R$ ter elemento máximo) e, para quaisquer $r, s \in R$,
$$x = r \wedge s \implies (x = r \text{ ou } x = s).$$

- Um elemento $y$ de $R$ diz-se $\vee$-*irredutível* se $y \neq 0$ (no caso de $R$ ter elemento mínimo) e, para quaisquer $r, s \in R$,
$$y = r \vee s \implies (y = r \text{ ou } y = s).$$

Seja $R$ um reticulado. Representa-se por $\mathcal{I}(R)$ o conjunto de todos os elementos $\wedge$-irredutíveis de $R$ e por $\mathcal{S}(R)$ o conjunto de todos os elementos $\vee$-irredutíveis de $R$. Para cada $x \in R$, denota-se por $\mathcal{S}(x)$ o conjunto de todos os elementos $\vee$-irredutíveis de $R$ menores ou iguais a $x$, isto é,

$$\mathcal{S}(x) = \{y \in \mathcal{S}(R) \mid y \leq x\}.$$

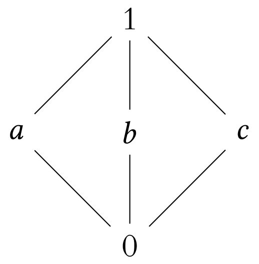
**Exemplo 0.3.45.** Seguem-se alguns exemplos de elementos $\wedge$-irredutíveis e $\vee$-irredutíveis de reticulados.

- Em qualquer cadeia, apenas o elemento $1$, caso exista, não é $\wedge$-irredutível.

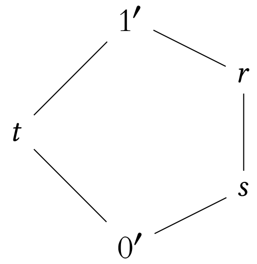
- Em qualquer reticulado $(\wp(X); \cap, \cup)$, onde $X$ é um conjunto não vazio qualquer e $\wp(X)$ representa o conjunto das partes de $X$, tem-se

$$\mathcal{S}(\wp(X)) = \{\{x\} \mid x \in X\}.$$

- Nos reticulados $M_3$ e $N_5$ dados, respetivamente, por




e




,

tem-se $\mathcal{I}(M_3) = \{a, b, c\} = \mathcal{S}(M_3)$ e $\mathcal{I}(N_5) = \{r, s, t\} = \mathcal{S}(N_5)$.

**Proposição 0.3.46.** *Sejam $(R; \wedge^R, \vee^R)$ e $(S; \wedge^S, \vee^S)$ reticulados e seja $\varphi$ um isomorfismo de $R$ em $S$. Então, para qualquer $x \in R$,*

*(i)* $x \in \mathcal{I}(R)$ *se e só se* $\varphi(x) \in \mathcal{I}(S)$*;*

*(ii)* $x \in \mathcal{S}(R)$ *se e só se* $\varphi(x) \in \mathcal{S}(S)$*.*

*Demonstração.* Observe-se, primeiramente, que, sendo $R$ e $S$ reticulados isomorfos, $R$ tem elemento máximo (mínimo) se e só se $S$ tem elemento máximo (mínimo). Ora, caso $R$ tenha máximo, para qualquer $x \in R$, tem-se $x = 1_R$ se e só se $\varphi(x) = 1_S$. De facto, se $x = 1_R$ e uma vez que, para qualquer $y \in S$, $y = \varphi(z)$, para certo $z \in R$,

$$\begin{aligned} y \vee^S \varphi(x) &= y \vee^S \varphi(1_R) \\ &= \varphi(z) \vee^S \varphi(1_R) \\ &= \varphi(z \vee^R 1_R) \\ &= \varphi(1_R) \\ &= \varphi(x), \end{aligned}$$

donde se obtém $\varphi(x) = 1_S$. Reciprocamente, se $\varphi(x) = 1_S$, então, para qualquer $w \in R$,

$$\begin{aligned} \varphi(x) &= \varphi(x) \vee^S \varphi(w) \\ &= \varphi(x \vee^R w), \end{aligned}$$

donde, pela injetividade de $\varphi$, se obtém $x = x \vee^R w$. Logo, $x = 1_R$. De modo análogo, caso $R$ tenha mínimo, tem-se $x = 0_R$ se e só se $\varphi(x) = 0_S$.

Seja $x \in R$.

Mostre-se que *(i)* é verificada. Suponha-se que $x \in \mathcal{I}(R)$. Sejam $a, b \in S$ tais que $\varphi(x) = a \wedge^S b$. Como $\varphi$ é um isomorfismo de reticulados, existem $u, v \in R$ tais que $a = \varphi(u)$ e $b = \varphi(v)$. Assim,

$$\varphi(x) = a \wedge^S b = \varphi(u) \wedge^S \varphi(v) = \varphi(u \wedge^R v).$$

Pela injetividade de $\varphi$, $x = u \wedge^R v$. Por hipótese,

$$x = u \text{ ou } x = v,$$

pelo que

$$\varphi(x) = \varphi(u) = a \text{ ou } \varphi(x) = \varphi(v) = b.$$

Além disso, como $x \neq 1_R$, então, pelo que se provou antes, $\varphi(x) \neq 1_S$. Logo, $\varphi(x) \in \mathcal{I}(S)$.

Reciprocamente, admitindo-se que $\varphi(x) \in \mathcal{I}(S)$ e tomando-se quaisquer $y, z \in R$ tais que $x = y \wedge^R z$, tem-se

$$\varphi(x) = \varphi(y \wedge^R z) = \varphi(y) \wedge^S \varphi(z),$$

donde, por hipótese, se retira que

$$\varphi(x) = \varphi(y) \text{ ou } \varphi(x) = \varphi(z)$$

e, pela injetividade de $\varphi$, segue

$$x = y \text{ ou } x = z.$$

Além disso, como $\varphi(x) \neq 1_S$, então, pelo que foi visto inicialmente, $x \neq 1_R$. Portanto, $x \in \mathcal{I}(R)$.

Conclui-se que *(i)* é válida e, por raciocínios análogos, também se verifica *(ii)*. □

**Teorema 0.3.47** (cf. [2], Theorem 4.8, p. 59)**.** *Seja $(R; \wedge, \vee)$ um reticulado que satisfaz a c.c.d.. Então, $R$ tem elemento mínimo e qualquer $x \in R \setminus \{0\}$ pode ser representado como o supremo de um número finito de elementos $\vee$-irredutíveis de $R$.*

*Demonstração.* Por *(ii)* do Teorema 0.1.21, tem-se que $R$ satisfaz a condição minimal, pelo que, em particular, $R$ tem, pelo menos, um elemento minimal, $x_1$. Se $R$ contivesse algum outro elemento minimal, $x_2$, então não existiria $x_1 \wedge x_2$, o que não acontece pois $R$ é um reticulado. Logo, $x_1$ é o único elemento minimal de $R$. Portanto, $x_1 = 0$.

Seja, agora, $x \in R \setminus \{0\}$. Se $x \in \mathcal{S}(R)$, a prova termina. Se $x \notin \mathcal{S}(R)$, então existem $y, z \in R$ tais que $x = y \vee z$, $x > y$ e $x > z$. Se $y, z \in \mathcal{S}(R)$, conclui-se o pretendido. Caso $y \notin \mathcal{S}(R)$ ou $z \notin \mathcal{S}(R)$, então $y = u \vee v$, para certos $u, v \in R$ tais que $y > u$ e $y > v$, ou $z = r \vee s$, para certos $r, s \in R$ tais que $z > r$ e $z > s$. Repetindo este procedimento, ou se obtém que $x$ é o supremo de um número finito de elementos $\vee$-irredutíveis ou se obtém alguma cadeia descendente infinita. No entanto, o segundo caso é falso, pois contraria a c.c.d..

Dá-se, assim, por concluída a prova. □

**Corolário 0.3.48.** *Seja $(R; \wedge, \vee)$ um reticulado que satisfaz a c.c.d.. Então, para qualquer $x \in R$,*

$$x = \bigvee \mathcal{S}(x).$$

*Demonstração.* É trivial que

$$0 = \bigvee \emptyset = \bigvee \mathcal{S}(0).$$

Além disso, dado $x \in R \setminus \{0\}$, como $R$ satisfaz a c.c.d., tem-se, pelo Teorema 0.3.47, que $x$ é o supremo de algum conjunto de elementos $\vee$-irredutíveis menores ou iguais a $x$, ou seja, $x = \bigvee S$, onde $S \subseteq \mathcal{S}(x)$. Assim,

$$x = \bigvee S \leq \bigvee \mathcal{S}(x) \leq x,$$

pelo que, de facto,

$$x = \bigvee \mathcal{S}(x),$$

como era pretendido mostrar. □

Outra noção importante é a de elemento primo de um reticulado.

**Definição 0.3.49.** Seja $(R; \wedge, \vee)$ um reticulado. Um elemento $x$ de $R$ diz-se *primo* se $x \neq 0$ (caso $0$ exista) e, para quaisquer $r, s \in R$,

$$x \leq r \vee s \implies (x \leq r \text{ ou } x \leq s).$$

Sendo $(R; \wedge, \vee)$ um reticulado, denota-se o conjunto de todos os elementos primos de $R$ por $\mathcal{P}(R)$; dado $x \in R$, representa-se por $\mathcal{P}(x)$ o conjunto dos elementos primos de $R$ menores ou iguais a $x$, isto é,

$$\mathcal{P}(x) = \{y \in \mathcal{P}(R) \mid y \leq x\}.$$

**Proposição 0.3.50** (cf. [6], p. 92)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, $\mathcal{P}(R) \subseteq \mathcal{S}(R)$.*

*Demonstração.* Seja $x \in \mathcal{P}(R)$. Então, $x \neq 0$, caso $0$ exista, e, para quaisquer $r, s \in R$ tais que $x = r \vee s$, tem-se $x \leq r$ ou $x \leq s$. Por um lado, se $x \leq r$, tem-se

$$x \leq r \leq r \vee s = x,$$

donde se retira $x = r$. Por outro lado, se $x \leq s$, então, de forma análoga, tem-se $x = s$. Portanto, $x \in \mathcal{S}(R)$. □

Estes últimos conceitos apresentados são particularmente importantes no estudo de reticulados finitos.

**Teorema 0.3.51** (cf. [6], Theorem 1, pp. 92–93)**.** *Seja* $(R; \wedge, \vee)$ *um reticulado finito e considere-se* $n \in \mathbb{N}_0$ *como sendo o número máximo de elementos primos de* $R$ *incomparáveis dois a dois. Se* $n \geq 1$*, então existem* $n$ *cadeias finitas* $C_1, C_2, \ldots, C_n$ *em* $R$ *e um homomorfismo de reticulados* $\psi$ *de* $R$ *no produto direto* $\prod_{i=1}^{n} C_i$ *tais que, para quaisquer* $x, y \in R$*,*

$$\psi(x) = \psi(y) \iff \mathcal{P}(x) = \mathcal{P}(y).$$

*Demonstração.* Suponha-se que $n \geq 1$. Como $n$ é o número máximo de elementos primos de $R$ incomparáveis dois a dois, então qualquer conjunto de $n+1$ elementos de $\mathcal{P}(R)$ contém, pelo menos, dois elementos comparáveis. Por isso, atendendo ao Teorema 1.1 de [5], p. 161, tem-se que $\mathcal{P}(R)$ é a união disjunta de $n$ cadeias $D_1, D_2, \ldots, D_n$. Para cada $i \in \{1, 2, \ldots, n\}$, defina-se $C_i = D_i \cup \{0\}$ (note-se que $C_1, C_2, \ldots, C_n$ são cadeias em $R$). Para cada $x \in R$ e $i \in \{1, 2, \ldots, n\}$, seja

$$x_i = \bigvee \{z \in C_i \mid z \leq x\}.$$

Seja $\psi$ a aplicação de $R$ em $\prod_{i=1}^{n} C_i$ tal que, para cada $x \in R$,

$$\psi(x) = (x_1, x_2, \ldots, x_n).$$

A aplicação $\psi$ está bem definida; de facto, é claro que $\psi(R) \subseteq \prod_{i=1}^{n} C_i$ e que, dados $x, y \in R$ tais que $x = y$, $\psi(x) = \psi(y)$.

Mostre-se que $\psi$ é um homomorfismo de reticulados.

Sejam $x, y \in R$ quaisquer.

Pretende-se provar que

$$\psi(x \vee y) = \psi(x) \sqcup \psi(y),$$

isto é,

$$((x \vee y)_1, \ldots, (x \vee y)_n) = (x_1, \ldots, x_n) \sqcup (y_1, \ldots, y_n),$$

ou seja,

$$((x \vee y)_1, \ldots, (x \vee y)_n) = (x_1 \vee y_1, \ldots, x_n \vee y_n).$$

Assim, é suficiente demonstrar que, para cada $i \in \{1, \ldots, n\}$, $(x \vee y)_i = x_i \vee y_i$. Tome-se, então, arbitrariamente algum $i \in \{1, \ldots, n\}$. Ora,

$$(x \vee y)_i = \bigvee \{z \in C_i \mid z \leq x \vee y\}$$

e

$$\begin{aligned} x_i \vee y_i &= \left(\bigvee \{z \in C_i \mid z \leq x\}\right) \vee \left(\bigvee \{z \in C_i \mid z \leq y\}\right) \\ &= \bigvee \{z \in C_i \mid z \leq x \text{ ou } z \leq y\}. \end{aligned}$$

Assim, definindo-se

$$L = \{z \in C_i \mid z \leq x \vee y\}$$

e

$$K = \{z \in C_i \mid z \leq x \text{ ou } z \leq y\},$$

basta demonstrar que $L = K$. Ora, é óbvio que $K \subseteq L$. Seja, agora, $z \in L$. Então, $z \in C_i$ e $z \leq x \vee y$. Caso $z = 0$, é óbvio que $z \leq x$ e $z \leq y$, pelo que $z \in K$. Caso $z \in D_i$, então $z \in \mathcal{P}(R)$ e, por conseguinte, como $z \leq x \vee y$, tem-se $z \leq x$ ou $z \leq y$. Logo, $z \in K$. Conclui-se assim que $L \subseteq K$ e, portanto, $L = K$.

Prove-se, agora, que

$$\psi(x \wedge y) = \psi(x) \sqcap \psi(y).$$

Ora, pelo que se acabou de provar, tem-se

$$\psi(x) = \psi(x \vee (x \wedge y)) = \psi(x) \sqcup \psi(x \wedge y),$$

donde

$$\psi(x \wedge y) \sqsubseteq \psi(x).$$

De forma semelhante,

$$\psi(x \wedge y) \sqsubseteq \psi(y).$$

Logo,

$$\psi(x \wedge y) \sqsubseteq \psi(x) \sqcap \psi(y).$$

Resta mostrar que

$$\psi(x) \sqcap \psi(y) \sqsubseteq \psi(x \wedge y),$$

isto é,

$$(x_1 \wedge y_1, \ldots, x_n \wedge y_n) \sqsubseteq ((x \wedge y)_1, \ldots, (x \wedge y)_n).$$

Seja $i \in \{1, \ldots, n\}$. Como

$$x_i = \bigvee \{z \in C_i \mid z \leq x\} \leq x$$

e

$$y_i = \bigvee \{z \in C_i \mid z \leq y\} \leq y,$$

tem-se $x_i \wedge y_i \leq x \wedge y$. Além disso, é claro que $x_i \wedge y_i \in C_i$. Logo, $x_i \wedge y_i \leq (x \wedge y)_i$, constatando-se assim o que era pretendido. Portanto, $\psi$ é, efetivamente, um homomorfismo de reticulados.

Resta provar que, para quaisquer $x, y \in R$,

$$\psi(x) = \psi(y) \iff \mathcal{P}(x) = \mathcal{P}(y).$$

Sejam $x, y \in R$. Suponha-se que

$$\psi(x) = \psi(y),$$

isto é,

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n).$$

Assim, para cada $i \in \{1, \ldots, n\}$, $x_i = y_i$, ou seja,

$$\bigvee\{z \in C_i \mid z \leq x\} = \bigvee\{w \in C_i \mid w \leq y\}.$$

Seja $p \in \mathcal{P}(x)$. Então, $p \in \mathcal{P}(R)$ e $p \leq x$. Assim, existe $j \in \{1, \ldots, n\}$ tal que $p \in D_j \subseteq C_j$, pelo que

$$p \in \{z \in C_j \mid z \leq x\}.$$

Então,

$$p \leq \bigvee\{z \in C_j \mid z \leq x\} = \bigvee\{w \in C_j \mid w \leq y\} \leq y.$$

Logo, $p \in \mathcal{P}(y)$. Portanto, $\mathcal{P}(x) \subseteq \mathcal{P}(y)$. A inclusão contrária prova-se de forma análoga, donde resulta que $\mathcal{P}(x) = \mathcal{P}(y)$.

Reciprocamente, assuma-se que $\mathcal{P}(x) = \mathcal{P}(y)$. Pretende-se provar que $x = y$, o que equivale a mostrar que, para cada $i \in \{1, \ldots, n\}$, $x_i = y_i$. Seja $i \in \{1, \ldots, n\}$. Para mostrar que $x_i = y_i$, basta ver que $L = K$, sendo

$$L = \{z \in C_i \mid z \leq x\}$$

e

$$K = \{w \in C_i \mid w \leq y\}.$$

Seja $z \in L$. Então, $z \in C_i$ e $z \leq x$. Ora, se $z = 0$, é trivial que $z \leq y$, pelo que $z \in K$. Caso $z \in D_i$, então

$$z \in \mathcal{P}(x) = \mathcal{P}(y),$$

pelo que $z \leq y$. Logo, $z \in K$. Portanto, $L \subseteq K$. Analogamente se prova que $K \subseteq L$, donde se conclui o pretendido. Portanto, $\psi(x) = \psi(y)$. □

**Teorema 0.3.52** (cf. [6], Theorem 2, pp. 93–94)**.** *Sejam $R$ um reticulado finito, $n \in \mathbb{N}_0$ o número máximo de elementos primos de $R$ incomparáveis dois a dois, $m \in \mathbb{N}_0$ o número máximo de sucessores distintos de um qualquer elemento de $R$ e $p \in \mathbb{N}_0$ o número máximo de elementos $\vee$-irredutíveis de $R$ incomparáveis dois a dois. Então, $n \leq m \leq p$.*

*Demonstração.* Prove-se, em primeiro lugar, que $n \leq m$. Se $n = 0$, é imediato. Se $n \neq 0$, sejam $r_1, r_2, \ldots, r_n \in \mathcal{P}(R)$ incomparáveis dois a dois. Definam-se os elementos

$$s = r_1 \vee r_2 \vee \cdots \vee r_n$$

e, para cada $i \in \{1, 2, \ldots, n\}$,

$$u_i = r_1 \vee \cdots \vee r_{i-1} \vee r_{i+1} \vee \cdots \vee r_n.$$

Além disso, considerem-se os elementos

$$t = u_1 \wedge u_2 \wedge \cdots \wedge u_n$$

e, para cada $i \in \{1, 2, \ldots, n\}$,

$$v_i = u_1 \wedge \cdots \wedge u_{i-1} \wedge u_{i+1} \wedge \cdots \wedge u_n.$$

Claramente, $u_i \leq s$, para cada $i \in \{1, 2, \ldots, n\}$. Suponha-se, por absurdo, que $u_i = s$, para algum $i \in \{1, 2, \ldots, n\}$. Sem perda de generalidade, considere-se que $u_n = s$, ou seja,

$$r_1 \vee \cdots \vee r_{n-1} = r_1 \vee \cdots \vee r_n.$$

Ora,

$$r_n \leq r_1 \vee \cdots \vee r_n = r_1 \vee \cdots \vee r_{n-1}.$$

Então, como $r_n \in \mathcal{P}(R)$, tem-se que $r_n \leq r_j$, para algum $j \in \{1, 2, \ldots, n-1\}$, o que é um absurdo, visto que os elementos $r_1, r_2, \ldots, r_n$ são incomparáveis dois a dois. Logo, $u_i < s$, para cada $i \in \{1, 2, \ldots, n\}$. É também fácil constatar que, para cada $i \in \{1, 2, \ldots, n\}$, $t \leq v_i$. Admita-se, por absurdo, que $t = v_j$, para algum $j \in \{1, 2, \ldots, n\}$. Sem perda de generalidade, considere-se que $t = v_n$, ou seja,

$$u_1 \wedge \cdots \wedge u_n = u_1 \wedge \cdots \wedge u_{n-1}.$$

Assim,

$$u_1 \wedge \cdots \wedge u_{n-1} = t \leq u_n.$$

Além disso, como $r_n \leq u_i$, para cada $i \in \{1, 2, \ldots, n-1\}$, então

$$r_n \leq u_1 \wedge \cdots \wedge u_{n-1}.$$

Logo, $r_n \leq u_n$. Sendo assim,

$$u_n = r_n \vee u_n = s,$$

algo que já foi provado ser impossível. Portanto, $t < v_i$, para todo o $i \in \{1, 2, \ldots, n\}$. Para cada $i \in \{1, 2, \ldots, n\}$, seja $w_i \in R$ tal que $t \prec w_i \leq v_i$. Assim, para quaisquer $i, j \in \{1, 2, \ldots, n\}$ tais que $i \neq j$, tem-se

$$t \leq w_i \wedge w_j \leq v_i \wedge v_j = t.$$

Portanto, $t = w_i \wedge w_j$, donde resulta que $w_i \neq w_j$; caso contrário, ter-se-ia $t = w_i$, o que contradiria o facto de $t \prec w_i$. Então, $w_1, \ldots, w_n$ são sucessores distintos de $t$, donde se conclui que $n \leq m$.

Prove-se, agora, que $m \leq p$.

Tome-se $x \in R$. Considere-se que os elementos $z_1, z_2, \ldots, z_m \in R$ são $m$ sucessores distintos de $x$. Então, não é difícil ver que, para cada $k \in \{1, 2, \ldots, m\}$, $\mathcal{S}(x) \subseteq \mathcal{S}(z_k)$ mas $\mathcal{S}(x) \neq \mathcal{S}(z_k)$; de facto, se existisse $k \in \{1, 2, \ldots, m\}$ tal que $\mathcal{S}(x) = \mathcal{S}(z_k)$, pelo Corolário 0.3.48, ter-se-ia

$$x = \bigvee \mathcal{S}(x) = \bigvee \mathcal{S}(z_k) = z_k,$$

o que seria uma contradição ao facto de $x \prec z_k$. Assim, para cada $k \in \{1, 2, \ldots, m\}$, existe $w_k \in \mathcal{S}(z_k)$ mas $w_k \notin \mathcal{S}(x)$. Suponha-se que existem $k, l \in \{1, \ldots, m\}$ tais que $k \neq l$ e $w_k$ e $w_l$ são comparáveis, assumindo, sem perda de generalidade, que $w_k \leq w_l$. Assim, $w_k \leq w_l \leq z_l$. Como também $w_k \leq z_k$, tem-se

$$w_k \leq z_k \wedge z_l = x,$$

o que significa que $w_k \in \mathcal{S}(x)$, uma contradição. Portanto, $w_1, \ldots, w_m$ são $m$ elementos $\vee$-irredutíveis de $R$ incomparáveis dois a dois, o que leva à conclusão de que, efetivamente, $m \leq p$, terminando assim a prova. □

Num reticulado limitado podem encontrar-se outros elementos especiais: os elementos complementados.

**Definição 0.3.53.** Sejam $(R; \wedge, \vee)$ um reticulado limitado e $x \in R$. Um elemento $x$ de $R$ diz-se *complementado* se existir $y \in R$ tal que

$$x \wedge y = 0 \ \text{ e } \ x \vee y = 1;$$

neste caso, diz-se que $y$ é um *complemento de $x$ em $R$*.

Claramente, qualquer complemento de um elemento complementado é também, por si só, um elemento complementado.

**Definição 0.3.54.** Um reticulado limitado $R$ diz-se *complementado* se qualquer elemento de $R$ for complementado.

Generalizando o conceito de complemento, introduz-se o conceito de complemento relativo.

**Definição 0.3.55.** Sejam $(R; \wedge, \vee)$ um reticulado e $r, s \in R$ tais que $r \leq s$. O intervalo $[r, s]$ diz-se *complementado* se, para qualquer $x \in [r, s]$, existir $y \in [r, s]$ tal que

$$x \wedge y = r \ \text{ e } \ x \vee y = s;$$

neste caso, diz-se que $y$ é um *complemento relativo de $x$ em $[r, s]$*.

**Definição 0.3.56.** Diz-se que um reticulado $R$ é *relativamente complementado* se, para quaisquer $r, s \in R$, o intervalo $[r, s]$ for complementado.

# 1 Reticulados distributivos

Ao longo deste capítulo, estudam-se os assuntos relativos ao tema central desta dissertação: os reticulados distributivos. Numa primeira secção, apresentam-se conceitos básicos relacionados com esta classe de reticulados, bem como algumas das suas principais propriedades. Na secção seguinte e suas subsecções, estudam-se propriedades dos reticulados distributivos, recorrendo, para tal, a noções como as de ideal/filtro, relação de congruência, elemento $\wedge$-irredutível/$\vee$-irredutível, complemento (relativo) com o objetivo de estabelecer resultados que auxiliem na caraterização e na representação de reticulados distributivos.

## 1.1 Definições e propriedades principais

Existem reticulados $(R; \wedge, \vee)$ em que as operações $\wedge$ e $\vee$ satisfazem propriedades adicionais àquelas que constam na definição 0.3.3, dos quais se destacam os reticulados distributivos e os reticulados modulares.

**Definição 1.1.1.** Seja $(R; \wedge, \vee)$ um reticulado. Diz-se que $R$ é um *reticulado distributivo* se as operações $\wedge$ e $\vee$ satisfizerem as *propriedades distributivas*, isto é, para quaisquer $x, y, z \in R$,

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

**Exemplo 1.1.2.** Alguns exemplos de reticulados distributivos são

- $(\mathbb{Z}; \inf, \sup)$, onde $\inf$ e $\sup$ representam, respetivamente, as operações ínfimo e supremo quando em $\mathbb{Z}$ se considera a relação de ordem $\leq$ usual;
- $(\wp(X); \cap, \cup)$, onde $X$ é um conjunto qualquer, $\wp(X)$ representa o conjunto das partes de $X$ e $\cap$ e $\cup$ são, respetivamente, as operações de interseção e de união;
- $(\mathbb{N}; \text{m.d.c.}, \text{m.m.c.})$, onde m.d.c. e m.m.c. denotam, respetivamente, as operações máximo divisor comum e mínimo múltiplo comum.

Para um reticulado ser distributivo, basta que uma das propriedades da Definição 1.1.1 seja satisfeita, uma vez que estas são equivalentes.

**Proposição 1.1.3** (cf. [4], Secção 4.3, pp. 85–86)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, são equivalentes as seguintes condições:*

*(i) para quaisquer $x, y, z \in R$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$;*

*(ii) para quaisquer $u, v, w \in R$, $u \vee (v \wedge w) = (u \vee v) \wedge (u \vee w)$.*

*Demonstração.* Suponha-se que a condição *(i)* é satisfeita. Sejam $u, v, w \in R$. Então,

$$\begin{aligned}
(u \vee v) \wedge (u \vee w) &= ((u \vee v) \wedge u) \vee ((u \vee v) \wedge w) && \text{[hipótese]}\\
&= u \vee (w \wedge (u \vee v)) && \text{[comutatividade e absorção]}\\
&= u \vee (w \wedge u) \vee (w \wedge v) && \text{[hipótese]}\\
&= u \vee (v \wedge w). && \text{[comutatividade e absorção]}
\end{aligned}$$

Logo,

$$u \vee (v \wedge w) = (u \vee v) \wedge (u \vee w),$$

ou seja, a condição *(ii)* é verificada.

Por raciocínios análogos, prova-se que o recíproco também é válido. □

Repare-se que, em qualquer reticulado, verificam-se as desigualdades

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

Portanto, para averiguar se um reticulado é distributivo, basta verificar se

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

Os reticulados distributivos são casos particulares de uma classe de reticulados mais abrangente: os reticulados modulares.

**Definição 1.1.4.** Seja $(R; \wedge, \vee)$ um reticulado. Diz-se que $R$ é um *reticulado modular* se for verificada a *propriedade modular*, isto é, para quaisquer $x, y, z \in R$,

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

Equivalentemente, um reticulado $(R; \wedge, \vee)$ é modular se, para quaisquer $x, y, z \in R$,

$$(x \wedge y) \vee (y \wedge z) = y \wedge ((x \wedge y) \vee z) \quad \text{ou} \quad x \vee ((x \vee y) \wedge z) = (x \vee y) \wedge (x \vee z),$$

já que $x \leq y$ se e só se $x = x \wedge y$ se e só se $y = x \vee y$. Além disso, facilmente se verifica que em todo o reticulado são válidas as desigualdades

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

pelo que, para provar que um reticulado é modular, é suficiente justificar que

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

**Proposição 1.1.5** (cf. [3], Theorem 3.4, p. 13)**.** *Qualquer reticulado distributivo é um reticulado modular.*

*Demonstração.* Sejam $(R; \wedge, \vee)$ um reticulado distributivo e $x, y, z \in R$. Então,

$$\begin{aligned} (x \wedge y) \vee (y \wedge z) &= ((x \wedge y) \vee y) \wedge ((x \wedge y) \vee z) && \text{[hipótese]} \\ &= y \wedge ((x \wedge y) \vee z), && \text{[comutatividade e absorção]} \end{aligned}$$

donde segue que o reticulado $R$ é modular. □

Como já foi estudado, é possível formar novos reticulados a partir de outros já dados, como é o caso dos sub-reticulados, produtos diretos de reticulados e imagens homomorfas de reticulados. A questão que pode ser levantada é se estes processos de construção de reticulados respeitam as propriedades de distributividade e modularidade. Ora, segundo o que afirma o resultado que se segue, a distributividade e a modularidade são preservadas por estas construções.

**Proposição 1.1.6** (cf. [4], Secção 4.7, p. 88)**.** *(i) Se $R$ é um reticulado distributivo (modular), então qualquer sub-reticulado de $R$ é distributivo (modular).*

*(ii) Se $R$ e $S$ são reticulados distributivos (modulares), então o produto direto $R \times S$ é distributivo (modular).*

*(iii) Se $R$ é um reticulado distributivo (modular), então qualquer imagem homomorfa de $R$ é distributiva (modular).*

*Demonstração.* Faz-se a prova apenas para a distributividade, visto que são semelhantes os argumentos usados para provar ambos os casos.

*(i)* É imediato.

*(ii)* Sejam $(R; \wedge^R, \vee^R)$ e $(S; \wedge^S, \vee^S)$ reticulados distributivos e $(x, u), (y, v), (z, w) \in R \times S$. Então, pela Proposição 0.3.10, $(R \times S; \sqcap, \sqcup)$ é um reticulado; além disso,

$$
\begin{aligned}
&(x, u) \sqcap ((y, v) \sqcup (z, w)) \\
&\quad = (x, u) \sqcap (y \vee^R z, v \vee^S w) && \text{[Definição 0.3.11]} \\
&\quad = (x \wedge^R (y \vee^R z), u \wedge^S (v \vee^S w)) && \text{[Definição 0.3.11]} \\
&\quad = ((x \wedge^R y) \vee^R (x \wedge^R z), (u \wedge^S v) \vee^S (u \wedge^S w)) && \text{[distributividade de } R \text{ e de } S\text{]} \\
&\quad = (x \wedge^R y, u \wedge^S v) \sqcup (x \wedge^R z, u \wedge^S w) && \text{[Definição 0.3.11]} \\
&\quad = ((x, u) \sqcap (y, v)) \sqcup ((x, u) \sqcap (z, w)). && \text{[Definição 0.3.11]}
\end{aligned}
$$

Logo, o produto direto $(R \times S; \sqcap, \sqcup)$ é distributivo.

*(iii)* Seja $(R; \wedge^R, \vee^R)$ um reticulado distributivo. Sejam $(S; \wedge^S, \vee^S)$ um reticulado e $\varphi$ um homomorfismo de reticulados de $R$ em $S$. Ora, pela Proposição 0.3.8, sabe-se que a imagem homomorfa $(\varphi(R); \wedge^S, \vee^S)$ de $R$ é um sub-reticulado de $S$. Prove-se que o reticulado $(\varphi(R); \wedge^S, \vee^S)$ é distributivo. Sejam $p, q, r \in \varphi(R)$. Então, existem $x, y, z \in R$ tais que $p = \varphi(x)$, $q = \varphi(y)$ e $r = \varphi(z)$. Ora,

$$
\begin{aligned}
p \wedge^S (q \vee^S r) &= \varphi(x) \wedge^S (\varphi(y) \vee^S \varphi(z)) \\
&= \varphi(x \wedge^R (y \vee^R z)) && [\varphi \text{ é um homomorfismo}] \\
&= \varphi((x \wedge^R y) \vee^R (x \wedge^R z)) && \text{[distributividade de } R\text{]} \\
&= (\varphi(x) \wedge^S \varphi(y)) \vee^S (\varphi(x) \wedge^S \varphi(z)) && [\varphi \text{ é um homomorfismo}] \\
&= (p \wedge^S q) \vee^S (p \wedge^S r).
\end{aligned}
$$

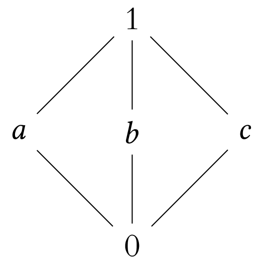
Portanto, o reticulado $(\varphi(R); \wedge^S, \vee^S)$ é, de facto, distributivo. □

## 1.2 Teoremas de caraterização e de representação

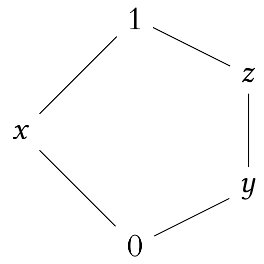
O objetivo desta secção é estabelecer teoremas e resultados que auxiliem na caraterização e representação de reticulados distributivos, recorrendo, para tal, a conceitos e propriedades fundamentais da teoria de reticulados.

### 1.2.1 Critério de distributividade de Birkhoff e outras caraterizações

Considerem-se os reticulados representados pelos diagramas de Hasse




e




e habitualmente designados por $M_3$ e $N_5$, respetivamente. Observe-se que nenhum destes reticulados é distributivo. De facto, não é difícil ver que, em $M_3$,

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

e, em $N_5$,

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

Quanto à modularidade, esta não é respeitada no reticulado $N_5$, uma vez que

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

Contudo, com uma verificação simples, prova-se que o reticulado $M_3$ é modular. Estes reticulados permitem estabelecer dois critérios que caraterizam a modularidade e a distributividade de um reticulado, os quais se apresentam no teorema seguinte.

**Teorema 1.2.1** (Critério de modularidade de Dedekind e Critério de distributividade de Birkhoff; cf. [3], Theorem 3.5 + Theorem 3.6, pp. 14–16)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então,*

*(i) $R$ é modular se e só se $R$ não possui qualquer sub-reticulado isomorfo a $N_5$;*

*(ii) $R$ é distributivo se e só se $R$ não possui qualquer sub-reticulado isomorfo a $M_3$ ou a $N_5$.*

*Demonstração.* *(i)* Como o reticulado $N_5$ não é modular, então, por *(i)* e *(iii)* da Proposição 1.1.6, se $N_5$ for isomorfo a algum sub-reticulado $S$ de $R$, o reticulado $R$ não será modular.

Reciprocamente, admita-se que $R$ não é modular. Assim, existem $x, y, z \in R$ tais que

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

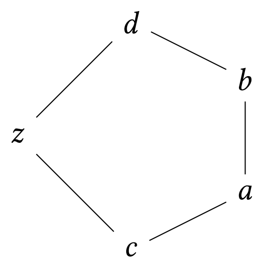
Então, considerando $a = (x \wedge y) \vee (y \wedge z)$ e $b = y \wedge ((x \wedge y) \vee z)$, tem-se que

$$\begin{aligned} z \wedge b &= z \wedge y \wedge ((x \wedge y) \vee z) \\ &= z \wedge y && \text{[comutatividade e absorção]} \end{aligned}$$

e

$$\begin{aligned} z \vee a &= z \vee (x \wedge y) \vee (y \wedge z) \\ &= z \vee (x \wedge y). && \text{[comutatividade e absorção]} \end{aligned}$$

Além disso, como $z \wedge y \leq a < b$, segue que $z \wedge y \leq z \wedge a \leq z \wedge b = z \wedge y$, pelo que $z \wedge a = z \wedge b = z \wedge y$. Analogamente, também se tem $z \vee a = z \vee b = z \vee (x \wedge y)$. Ora, fazendo $c = z \wedge y$ e $d = z \vee (x \wedge y)$, não é difícil verificar que os elementos $c, z, a, b, d$ são distintos dois a dois. Conclui-se assim que o reticulado




é um sub-reticulado de $R$ isomorfo a $N_5$.

*(ii)* Como os reticulados $M_3$ e $N_5$ não são distributivos, então, se existir algum sub-reticulado $S$ de $R$ isomorfo a $M_3$ ou a $N_5$, é imediato, por *(i)* e *(iii)* da Proposição 1.1.6, que $R$ não será distributivo.

Reciprocamente, suponha-se que $R$ não é distributivo e que $R$ não contém qualquer sub-reticulado isomorfo a $N_5$. Então, existem $x, y, z \in R$ tais que

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

e, por *(i)*, $R$ é modular. Sendo $d$, $e$, $a$, $b$ e $c$ os elementos de $R$ dados por

$$\begin{aligned} d &= (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \\ e &= (x \vee y) \wedge (x \vee z) \wedge (y \vee z) \\ a &= (x \wedge e) \vee d \\ b &= (y \wedge e) \vee d \\ c &= (z \wedge e) \vee d, \end{aligned}$$

não é difícil de verificar que, para qualquer $u \in \{a, b, c\}$, $d \leq u \leq e$. De facto, é óbvio que $d \leq a$. Além disso, como $x \wedge y \leq x \vee y$, $x \wedge y \leq x \vee z$ e $x \wedge y \leq y \vee z$, então

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

Analogamente, prova-se que

$$x \wedge z \leq e \quad \text{e} \quad y \wedge z \leq e.$$

Logo,

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

Adicionalmente, uma vez que

$$\begin{aligned} e \vee a &= e \vee (x \wedge e) \vee d \\ &= e \vee d && \text{[comutatividade e absorção]} \\ &= e, && [d \leq e] \end{aligned}$$

tem-se que $a \leq e$. Portanto, $d \leq a \leq e$. Por raciocínios análogos, prova-se que $d \leq b \leq e$ e $d \leq c \leq e$. Observe-se, agora, que

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

e

$$\begin{aligned} x \wedge d &= x \wedge ((x \wedge y) \vee (x \wedge z) \vee (y \wedge z)) \\ &= (x \wedge y) \vee (x \wedge ((x \wedge z) \vee (y \wedge z))) && \text{[modularidade]} \\ &= (x \wedge y) \vee (x \wedge z) \vee (x \wedge y \wedge z) && \text{[modularidade]} \\ &= (x \wedge y) \vee (x \wedge z), && [x \wedge y \wedge z \leq x \wedge z] \end{aligned}$$

pelo que $x \wedge d < x \wedge e$. Como $d = e$ conduz a uma contradição, conclui-se que $d < e$.

Demonstra-se, de seguida, que $b \wedge c = d$. Ora,

$$\begin{aligned} b \wedge c &= ((y \wedge e) \vee d) \wedge ((z \wedge e) \vee d) \\ &= d \vee ((d \vee (y \wedge e)) \wedge z \wedge e) && \text{[comutatividade e modularidade]} \\ &= d \vee (e \wedge (d \vee y) \wedge z \wedge e) && \text{[comutatividade e modularidade (} d \leq e \text{)]} \\ &= d \vee ((d \vee y) \wedge z \wedge e) && \text{[comutatividade e idempotência]} \\ &= d \vee (z \wedge ((x \wedge z) \vee y) \wedge (x \vee y)) && \text{[absorção e comutatividade]} \\ &= d \vee (((x \wedge z) \vee (z \wedge y)) \wedge (x \vee y)) && \text{[modularidade]} \\ &= d \vee (x \wedge z) \vee (z \wedge y) && [(x \wedge z) \vee (z \wedge y) \leq x \vee y] \\ &= d. && \text{[idempotência]} \end{aligned}$$

Por demonstrações análogas, conclui-se que $a \wedge b = d$ e $a \wedge c = d$. Argumentos semelhantes mostram que $a \vee b = e$, $a \vee c = e$ e $b \vee c = e$.

Por fim, resta verificar que os elementos $d$, $e$, $a$, $b$ e $c$ são distintos dois a dois. Suponha-se que $a = b$. Então,

$$d = a \wedge b = a \wedge a = a = a \vee a = a \vee b = e,$$

o que é uma contradição. Logo, $a \neq b$. Analogamente, mostra-se que $a \neq c$ e $b \neq c$. Admita-se, agora, que $e = b$. Assim, por um lado,

$$d = a \wedge b = a \wedge e = a \wedge (a \vee b) = a$$

e, por outro lado,

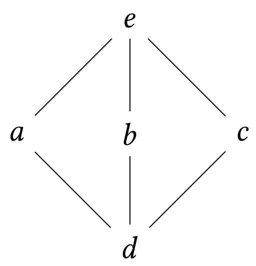
$$d = b \wedge c = e \wedge c = (b \vee c) \wedge c = c,$$

pelo que

$$d = a \vee c = e,$$

o que é impossível. Logo, $e \neq b$. Os restantes casos provam-se de forma análoga.

Portanto, o reticulado




é um sub-reticulado de $R$ isomorfo a $M_3$. □

Seguem-se mais alguns resultados que estabelecem formas de caraterizar a distributividade de um reticulado.

**Teorema 1.2.2** (cf. [2], Exercise 5.3, p. 67)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, $R$ é distributivo se e só se, para quaisquer $x, y, z \in R$,*

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

*Demonstração.* Suponha-se, primeiramente, que o reticulado $R$ é distributivo. Sejam $x, y, z \in R$. Então,

$$\begin{aligned}
(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) &= (y \wedge (x \vee z)) \vee (z \wedge x) && \text{[comutatividade e hipótese]} \\
&= (y \vee (z \wedge x)) \wedge ((x \vee z) \vee (z \wedge x)) && \text{[hipótese]} \\
&= (y \vee (z \wedge x)) \wedge (x \vee z) && [z \wedge x \leq x \vee z] \\
&= (x \vee y) \wedge (y \vee z) \wedge (z \vee x). && \text{[hipótese e comutatividade]}
\end{aligned}$$

Reciprocamente, admita-se que, para quaisquer $x, y, z \in R$,

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

Então, para quaisquer $u, v, w \in R$,

$$((u \wedge v) \wedge v) \vee (v \wedge w) \vee (w \wedge (u \wedge v)) = ((u \wedge v) \vee v) \wedge (v \vee w) \wedge (w \vee (u \wedge v)),$$

donde, pelas propriedades das operações $\wedge$ e $\vee$, segue

$$(u \wedge v) \vee (v \wedge w) \vee (w \wedge u \wedge v) = v \wedge (v \vee w) \wedge (w \vee (u \wedge v))$$

e, consequentemente,

$$(u \wedge v) \vee (v \wedge w) = v \wedge ((u \wedge v) \vee w). \quad \textit{(I)}$$

Da hipótese, também resulta que, para quaisquer $u, v, w \in R$,

$$u \wedge ((u \wedge v) \vee (v \wedge w) \vee (w \wedge u)) = u \wedge ((u \vee v) \wedge (v \vee w) \wedge (w \vee u)),$$

e, por absorção, obtém-se

$$u \wedge ((u \wedge v) \vee (v \wedge w) \vee (w \wedge u)) = u \wedge (v \vee w). \quad \textit{(II)}$$

Assim, dados $u, v, w \in R$,

$$\begin{aligned}
u \wedge (v \vee w) &= u \wedge ((u \wedge v) \vee (v \wedge w) \vee (w \wedge u)) && [\textit{(II)}] \\
&= (u \wedge v) \vee (u \wedge ((w \wedge u) \vee (v \wedge w))) && [\textit{(I)} \text{ e comutatividade}] \\
&= (u \wedge v) \vee (w \wedge u) \vee (u \wedge v \wedge w) && [\textit{(I)}] \\
&= (u \wedge v) \vee (u \wedge w). && [\text{comutatividade e } u \wedge v \wedge w \leq u \wedge w]
\end{aligned}$$

Logo, o reticulado $R$ é distributivo. □

**Teorema 1.2.3** (cf. [2], Theorem 5.1, p. 67)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, $R$ é distributivo se e só se, para quaisquer $x, y, z \in R$,*

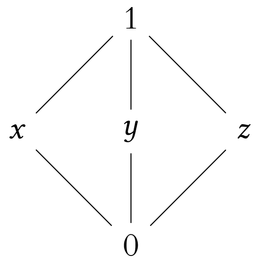
$$(x \wedge z = y \wedge z \quad e \quad x \vee z = y \vee z) \implies x = y.$$

*Demonstração.* Suponha-se, primeiramente, que $R$ é distributivo. Sejam $x, y, z \in R$ tais que $x \wedge z = y \wedge z$ e $x \vee z = y \vee z$. Então,

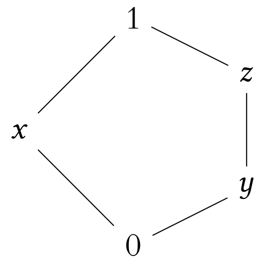
$$\begin{aligned}
x &= x \wedge (x \vee z) && [\text{absorção}] \\
&= x \wedge (y \vee z) && [\text{hipótese}] \\
&= (x \wedge y) \vee (x \wedge z) && [\text{distributividade}] \\
&= (x \wedge y) \vee (y \wedge z) && [\text{hipótese}] \\
&= y \wedge (x \vee z) && [\text{distributividade e comutatividade}] \\
&= y \wedge (y \vee z) && [\text{hipótese}] \\
&= y. && [\text{absorção}]
\end{aligned}$$

Logo, $x = y$.

Reciprocamente, admita-se que $R$ não é distributivo. Então, por *(ii)* do Teorema 1.2.1, $R$ possui algum sub-reticulado $S$ isomorfo a $M_3$ ou a $N_5$. Assim, o diagrama de Hasse de $S$ tem uma das seguintes formas:




ou




.

Em ambos os casos, observa-se que $x \wedge z = y \wedge z$ e $x \vee z = y \vee z$, mas $x \neq y$.

Dá-se, assim, por concluída a prova. $\square$

Existem também aplicações especiais que ajudam na caraterização de reticulados distributivos.

Sejam $(R; \wedge, \vee)$ um reticulado e $a \in R$. Representa-se por $\wedge_a$ a aplicação de $R$ em $R$ tal que, para cada $x \in R$, $\wedge_a(x) = x \wedge a$; e por $\vee_a$ a aplicação de $R$ em $R$ tal que, para cada $x \in R$, $\vee_a(x) = x \vee a$. Mais, dados $a, b \in R$, usar-se-ão as notações $\varphi_a$ e $\psi_b$ para denotar, respetivamente, as aplicações

$$\begin{array}{rcl} [b, a \vee b] & \to & [a \wedge b, a] \\ x & \mapsto & \wedge_a(x) \end{array} \quad \text{e} \quad \begin{array}{rcl} [a \wedge b, a] & \to & [b, a \vee b] \\ x & \mapsto & \vee_b(x) \end{array}.$$

Além disso, para qualquer subconjunto $S$ de $R$, denota-se a aplicação identidade em $S$ por $\iota_S$.

**Teorema 1.2.4** (cf. [9], Theorem 4.9, p. 103)**.** *Seja* $(R; \wedge, \vee)$ *um reticulado. Então,*

*(i)* *$R$ é distributivo se e só se, para qualquer $a \in R$, a aplicação $\wedge_a$ é um homomorfismo de reticulados;*

*(ii)* *$R$ é distributivo se e só se, para qualquer $a \in R$, a aplicação $\vee_a$ é um homomorfismo de reticulados.*

*Demonstração.* Como as condições *(i)* e *(ii)* são duais uma da outra, basta provar uma delas; neste caso, demonstrar-se-á *(i)*.

Suponha-se, primeiramente, que $R$ é distributivo. Seja $a \in R$. Ora, para quaisquer $x, y \in R$,

$$\wedge_a(x \wedge y) = x \wedge y \wedge a = (x \wedge a) \wedge (y \wedge a) = \wedge_a(x) \wedge \wedge_a(y)$$

e, por hipótese,

$$\wedge_a(x \vee y) = (x \vee y) \wedge a = (x \wedge a) \vee (y \wedge a) = \wedge_a(x) \vee \wedge_a(y).$$

Logo, $\wedge_a$ é um homomorfismo de reticulados.

Reciprocamente, admitindo-se que, para qualquer $a \in R$, $\wedge_a$ é um homomorfismo de reticulados, então, para quaisquer $x, y, z \in R$, tem-se

$$\wedge_x(y \vee z) = \wedge_x(y) \vee \wedge_x(z),$$

ou seja,

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

Portanto, $R$ é distributivo. □

**Teorema 1.2.5** (cf. [9], Theorem 4.10, p. 104)**.** *Seja $(R; \wedge, \vee)$ um reticulado. Então, as seguintes afirmações são equivalentes:*

*(i)* *$R$ é modular;*

*(ii)* *para quaisquer $a, b \in R$,*

$$\varphi_a \circ \psi_b = \iota_{[a \wedge b, a]};$$

*(iii)* *para quaisquer $a, b \in R$,*

$$\psi_b \circ \varphi_a = \iota_{[b, a \vee b]};$$

*(iv)* *para quaisquer $a, b \in R$, ambas as aplicações $\varphi_a$ e $\psi_b$ são isomorfismos de reticulados satisfazendo*

$$\varphi_a(x) = y \iff \psi_b(y) = x,$$

*para quaisquer $x \in [b, a \vee b]$ e $y \in [a \wedge b, a]$.*

*Demonstração.* As condições *(ii)* e *(iii)* são claramente equivalentes, pois são duais uma da outra.

Suponha-se que *(i)* é válida e sejam $a, b \in R$. É claro que tanto $\varphi_a \circ \psi_b$ como $\iota_{[a \wedge b, a]}$ são aplicações de $[a \wedge b, a]$ em $[a \wedge b, a]$. Mais, para qualquer $x \in [a \wedge b, a]$, tem-se

$$\begin{aligned}
(\varphi_a \circ \psi_b)(x) &= \wedge_a(\vee_b(x)) = \wedge_a(x \vee b) \\
&= (x \vee b) \wedge a \\
&= x \vee (b \wedge a) && [x \leq a \text{ e } (i)] \\
&= x && [a \wedge b \leq x] \\
&= \iota_{[a \wedge b, a]}(x).
\end{aligned}$$

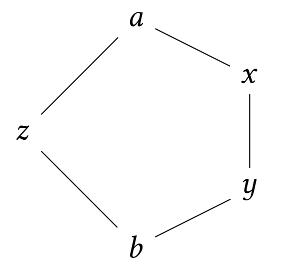
Logo, $\varphi_a \circ \psi_b = \iota_{[a \wedge b, a]}$, pelo que *(ii)* é satisfeita, donde *(i)* $\Longrightarrow$ *(ii)*.

Admita-se, agora, que *(ii)* é válida. Então, *(iii)* também o é. Logo, para quaisquer $a, b \in R$, as aplicações $\varphi_a$ e $\psi_b$ são invertíveis, sendo $\varphi_a$ a inversa de $\psi_b$. Além disso, é óbvio que as aplicações $\varphi_a$ e $\psi_b$ são isótonas. Logo, pelas Proposições 0.1.24 e 0.3.6, $\varphi_a$ e $\psi_b$ são isomorfismos de reticulados. Falta verificar que, para quaisquer $x \in [b, a \vee b]$ e $y \in [a \wedge b, a]$,

$$\varphi_a(x) = y \iff \psi_b(y) = x.$$

De facto, esta verificação é imediata, uma vez que $\varphi_a$ e $\psi_b$ são funções invertíveis, sendo que uma é a inversa da outra. Isto conclui a demonstração de *(iv)*, pelo que *(ii)* $\Longrightarrow$ *(iv)*.

Assuma-se, agora, que *(iv)* é válida. Suponha-se, por absurdo, que $R$ não é modular. Então $R$ contém algum sub-reticulado isomorfo a $N_5$, isto é, existem $x, y, z, a, b \in R$ relacionados conforme o diagrama de Hasse




.

Em particular, tem-se que $y \in [b, x] = [x \wedge z, x]$. Ora,

$$\psi_z(y) = y \vee z = a,$$

com $a \in [z, x \vee z]$, mas

$$\varphi_x(a) = a \wedge x = x \neq y,$$

o que contradiz *(iv)*. Portanto, $R$ é modular, donde *(iv)* $\implies$ *(i)*.

Fica assim concluída a demonstração do teorema. □

Repare-se que, tendo em conta a Proposição 1.1.5 e o teorema anterior, num reticulado distributivo também são observadas as condições (ii)–(iv) do referido teorema.

### 1.2.2 Caraterização e representação de reticulados distributivos recorrendo a ideais e filtros

Nesta subsecção, estudam-se propriedades dos reticulados distributivos relacionadas com as noções de ideal e filtro.

**Teorema 1.2.6** (cf. [9], Theorem 4.6 2), p. 98; [7], Corollary 104, p. 111)**.** *Seja* $(R; \wedge, \vee)$ *um reticulado. Então são equivalentes as seguintes condições:*

*(i)* $R$ *é distributivo;*

*(ii)* *o reticulado dos ideais de* $R$*,* $\mathrm{Id}(R)$*, é distributivo;*

*(iii)* *para quaisquer* $I, J \in \mathrm{Id}(R)$*,* $I \vee J = \{a \vee b \mid a \in I, b \in J\}$*.*

*Demonstração.* Suponha-se, primeiramente, que $R$ é distributivo. Aplicando sucessivamente o Teorema 0.3.17, prova-se que $\mathrm{Id}(R)$ é distributivo. De facto, dados $I, J, K \in \mathrm{Id}(R)$ e

$$x \in I \wedge (J \vee K),$$

tem-se que $x \in I$ e $x \in J \vee K$, donde segue que $x \leq a \vee b$, para alguns $a \in J$ e $b \in K$ e, como $I, J \in \mathrm{Id}(R)$, tem-se que $x \wedge a \in I \cap J$. Analogamente, verifica-se que $x \wedge b \in I \cap K$. Além disso,

$$\begin{aligned} x &= x \wedge (a \vee b) && [x \leq a \vee b] \\ &= (x \wedge a) \vee (x \wedge b), && [\text{hipótese}] \end{aligned}$$

donde, em particular, se retira que

$$x \leq (x \wedge a) \vee (x \wedge b).$$

Logo,

$$x \in (I \wedge J) \vee (I \wedge K).$$

Portanto,

$$I \wedge (J \vee K) \subseteq (I \wedge J) \vee (I \wedge K).$$

Para provar a inclusão contrária, tome-se

$$x \in (I \wedge J) \vee (I \wedge K)$$

arbitrariamente. Assim, tem-se que $x \leq a \vee b$, para determinados $a \in I \cap J$ e $b \in I \cap K$. Como $a, b \in I$, segue, por *(i)* do Lema 0.3.16, que $a \vee b \in I$ e, consequentemente, por *(ii)* do mesmo lema, $x \in I$. Além disso, é trivial que $x \in J \vee K$, uma vez que $a \in J$ e $b \in K$. Logo,

$$x \in I \wedge (J \vee K).$$

Assim,

$$(I \wedge J) \vee (I \wedge K) \subseteq I \wedge (J \vee K).$$

Portanto,

$$I \wedge (J \vee K) = (I \wedge J) \vee (I \wedge K),$$

o que demonstra o pretendido.

Suponha-se, agora, que $\mathrm{Id}(R)$ é distributivo. Sejam $I, J \in \mathrm{Id}(R)$. Pelo Teorema 0.3.17, para provar que

$$I \vee J = \{a \vee b \mid a \in I, b \in J\},$$

basta verificar que $L = K$, onde

$$L = \{x \in R \mid x \leq a \vee b, \textit{ para certos } a \in I \text{ e } b \in J\} \quad \text{e} \quad K = \{a \vee b \mid a \in I, b \in J\}.$$

Ora, é óbvio que $K \subseteq L$. Seja $x \in L$. Então, existem $a \in I$ e $b \in J$ tais que $x \leq a \vee b$. Assim, $x = x \wedge (a \vee b)$, donde segue que

$$\begin{aligned}
\mathrm{id}(x) &= \mathrm{id}(x \wedge (a \vee b)) \\
&= \mathrm{id}(x) \wedge (\mathrm{id}(a) \vee \mathrm{id}(b)) && \text{[Teorema 0.3.26]} \\
&= (\mathrm{id}(x) \wedge \mathrm{id}(a)) \vee (\mathrm{id}(x) \wedge \mathrm{id}(b)) && \text{[hipótese]} \\
&= \mathrm{id}((x \wedge a) \vee (x \wedge b)). && \text{[Teorema 0.3.26]}
\end{aligned}$$

Assim, novamente pelo Teorema 0.3.26, tem-se $x = (x \wedge a) \vee (x \wedge b)$; logo, uma vez que $x \wedge a \in I$ e $x \wedge b \in J$, $x \in K$. Portanto, $L \subseteq K$ e assim se conclui que

$$I \vee J = \{a \vee b \mid a \in I, b \in J\}.$$

Admita-se, agora, que, para quaisquer $I, J \in \mathrm{Id}(R)$,

$$I \vee J = \{a \vee b \mid a \in I, b \in J\}.$$

No sentido de provar que $R$ é distributivo, mostre-se, inicialmente, que

$$\mathrm{id}(x \wedge (y \vee z)) = \mathrm{id}((x \wedge y) \vee (x \wedge z)).$$

Sejam $x, y, z \in R$. Tome-se qualquer

$$r \in \mathrm{id}(x) \wedge (\mathrm{id}(y) \vee \mathrm{id}(z)).$$

Então, $r \leq x$ e $r = a \vee b$, para certos $a \leq y$ e $b \leq z$. Assim, tem-se

$$a \leq a \vee b = r \leq x \quad \text{e} \quad b \leq a \vee b = r \leq x,$$

pelo que

$$a \in \mathrm{id}(x) \wedge \mathrm{id}(y)$$

e

$$b \in \mathrm{id}(x) \wedge \mathrm{id}(z).$$

Logo,

$$r \in (\mathrm{id}(x) \wedge \mathrm{id}(y)) \vee (\mathrm{id}(x) \wedge \mathrm{id}(z)).$$

Reciprocamente, dado

$$r \in (\mathrm{id}(x) \wedge \mathrm{id}(y)) \vee (\mathrm{id}(x) \wedge \mathrm{id}(z)),$$

tem-se que $r = a \vee b$, onde $a \leq x$, $a \leq y$, $b \leq x$ e $b \leq z$. Assim, $r \leq x$ e $r = a \vee b$, com $a \in \mathrm{id}(y)$ e $b \in \mathrm{id}(z)$, pelo que

$$r \in \mathrm{id}(x) \wedge (\mathrm{id}(y) \vee \mathrm{id}(z)).$$

Portanto, conclui-se que

$$\mathrm{id}(x) \wedge (\mathrm{id}(y) \vee \mathrm{id}(z)) = (\mathrm{id}(x) \wedge \mathrm{id}(y)) \vee (\mathrm{id}(x) \wedge \mathrm{id}(z)),$$

ou seja,

$$\mathrm{id}(x \wedge (y \vee z)) = \mathrm{id}((x \wedge y) \vee (x \wedge z)).$$

Consequentemente, pelo Teorema 0.3.26,

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

Logo, $R$ é distributivo. □

**Teorema 1.2.7** (cf, [7], Theorem 106, p. 112)**.** *Seja $(R; \wedge, \vee)$ um reticulado distributivo. Então, para qualquer $a \in R$, a aplicação $\varphi_a$ de $R$ em $\mathrm{id}(a) \times \mathrm{fil}(a)$ definida por*

$$\varphi_a(x) = (x \wedge a, x \vee a)$$

*é um monomorfismo de $(R; \wedge, \vee)$ em $(\mathrm{id}(a) \times \mathrm{fil}(a); \sqcap, \sqcup)$.*

*Demonstração.* Seja $a \in R$. É simples verificar que $\varphi_a$ está bem definida. Claramente, para qualquer $x \in R$, $(x \wedge a, x \vee a) \in \mathrm{id}(a) \times \mathrm{fil}(a)$. Além disso, se $x, y \in R$ são tais que $\varphi_a(x) = \varphi_a(y)$, tem-se $x \wedge a = y \wedge a$ e $x \vee a = y \vee a$ e, como $R$ é distributivo, pelo Teorema 1.2.3, $x = y$. Logo, a aplicação $\varphi_a$ é injetiva.

Sejam, agora, $x, y \in R$ quaisquer. Tem-se

$$\begin{aligned}
\varphi_a(x \wedge y) &= ((x \wedge y) \wedge a, (x \wedge y) \vee a) && [\text{definição de } \varphi_a]\\
&= ((x \wedge a) \wedge (y \wedge a), (x \vee a) \wedge (y \vee a)) && [\text{distributividade de } R]\\
&= (x \wedge a, x \vee a) \sqcap (y \wedge a, y \vee a) && [\text{definição de } \sqcap \text{ em } \mathrm{id}(a) \times \mathrm{fil}(a)]\\
&= \varphi_a(x) \sqcap \varphi_a(y). && [\text{definição de } \varphi_a]
\end{aligned}$$

Analogamente,

$$\varphi_a(x \vee y) = \varphi_a(x) \sqcup \varphi_a(y).$$

Portanto, $\varphi_a$ é um monomorfismo de reticulados. □

De seguida, estabelecem-se alguns resultados, que permitirão apresentar outra forma de caraterizar a distributividade de um reticulado.

**Teorema 1.2.8** (cf. [7], Theorem 115, pp. 116–117)**.** *Seja $(R; \wedge, \vee)$ um reticulado distributivo. Sejam $I \in \mathrm{Id}(R)$ e $F \in \mathrm{Fil}(R)$ tais que $I \cap F = \emptyset$. Então existe $P \in \mathrm{Esp}(R)$ tal que $I \subseteq P$ e $P \cap F = \emptyset$.*

*Demonstração.* Defina-se

$$\mathcal{X} = \{Y \in \mathrm{Id}(R) \mid I \subseteq Y,\ Y \cap F = \emptyset\}.$$

Claramente, $\mathcal{X} \subseteq \wp(R)$, uma vez que $\mathcal{X} \subseteq \mathrm{Id}(R) \subseteq \wp(R)$, e $\mathcal{X} \neq \emptyset$, pois $I \in \mathcal{X}$.

Seja $\mathcal{C}$ uma cadeia em $(\mathcal{X}; \subseteq)$ e defina-se $M = \bigcup \mathcal{C}$. Prove-se que $M \in \mathcal{X}$. Mostre-se, primeiramente, que $M \in \mathrm{Id}(R)$. Ora, como $\mathcal{C} \subseteq \mathcal{X} \subseteq \wp(R)$, então $M = \bigcup \mathcal{C} \subseteq R$. Obviamente, $M \neq \emptyset$, uma vez que $\mathcal{C} \neq \emptyset$ e, para todo $Y \in \mathrm{Id}(R)$, $Y \neq \emptyset$. Tomando, agora, quaisquer $y, z \in M$, sabe-se que existem $Y, Z \in \mathcal{C}$ tais que $y \in Y$ e $z \in Z$. Assim, $Y, Z \in \mathcal{X}$ e tem-se que $Y$ e $Z$ são comparáveis; assuma-se, sem perda de generalidade, que $Y \subseteq Z$. Então, $y, z \in Z$ e, como $Z \in \mathrm{Id}(R)$, segue, por *(i)* do Lema 0.3.16, que $y \vee z \in Z$. Logo, $y \vee z \in M$. Sejam, agora, $x \in R$ e $y \in M$ tais que $x \leq y$. Assim, existe $Y \in \mathcal{C}$ tal que $y \in Y$. Como $x \in R$, $y \in Y$, $x \leq y$ e $Y \in \mathrm{Id}(R)$, então, por *(ii)* do Lema 0.3.16, segue que $x \in Y$ e, portanto, $x \in M$. O Lema 0.3.16 permite, assim, concluir que $M \in \mathrm{Id}(R)$. Também não é difícil verificar que $I \subseteq M$. De facto, uma vez que $I \subseteq Y$, para qualquer $Y \in \mathcal{C}$, tem-se que $I \subseteq \bigcup \mathcal{C} = M$. Suponha-se, agora, por absurdo, que existe $x \in M \cap F$. Assim, em particular, $x \in M$, pelo que $x \in Y$ para algum $Y \in \mathcal{C}$. Então, $x \in Y \cap F$, logo $Y \cap F \neq \emptyset$, o que é uma contradição, visto que $Y \in \mathcal{C} \subseteq \mathcal{X}$ e, portanto, $Y \cap F = \emptyset$. Portanto, $M \cap F = \emptyset$. Fica assim provado o que era pretendido.

Por conseguinte, pelo Lema de Zorn (Lema 0.1.19), pode afirmar-se que $\mathcal{X}$ possui algum elemento maximal; seja $P$ um elemento maximal de $\mathcal{X}$. O objetivo é mostrar que $P$ é um ideal primo de $R$. Suponha-se, por absurdo, que o ideal $P$ não é primo. Então existem $a, b \in R$ tais que $a \wedge b \in P$ mas $a \notin P$ e $b \notin P$. Defina-se $Q = P \vee \mathrm{id}(a)$ e $T = P \vee \mathrm{id}(b)$. Como $P$ é um elemento maximal de $\mathcal{X}$ e $P \subset Q$, então $Q \notin \mathcal{X}$. Mais, como $Q \in \mathrm{Id}(R)$ e $I \subseteq P \subset Q$ mas $Q \notin \mathcal{X}$, tem-se que $Q \cap F \neq \emptyset$. De forma análoga, $T \cap F \neq \emptyset$. Assim, por um lado, existe $x \in F$ tal que $x \in Q$, pelo que $x = p \vee r$, para certos $p \in P$ e $r \leq a$. Por outro lado, existe $y \in F$ tal que $y \in T$, donde $y = q \vee s$, para alguns $q \in P$ e $s \leq b$. Definindo $z = x \wedge y$, tem-se que $z = (p \vee r) \wedge (q \vee s)$. Logo, $z \in F$, uma vez que $F \in \mathrm{Fil}(R)$. Além disso,

$$\begin{aligned}
z &= (p \vee r) \wedge (q \vee s) \\
&= ((p \vee r) \wedge q) \vee ((p \vee r) \wedge s) && \text{[distributividade]} \\
&= (p \wedge q) \vee (r \wedge q) \vee (p \wedge s) \vee (r \wedge s). && \text{[distributividade]}
\end{aligned}$$

Ora, tendo em conta que $P \in \mathrm{Id}(R)$ e aplicando o Lema 0.3.16, é fácil concluir que $p \wedge q$, $r \wedge q$, $p \wedge s$ e $r \wedge s$ são elementos de $P$. Por conseguinte, $z \in P$. Logo, $z \in P \cap F$, ou seja, $P \cap F \neq \emptyset$, o que contradiz o facto de que $P \in \mathcal{X}$. O absurdo resultou de se supor que o ideal $P$ não é primo. Portanto, $P$ é um ideal primo de $R$, o que conclui a demonstração. $\square$

**Corolário 1.2.9** (cf. [7], Corollary 116, p. 117)**.** *Seja $R$ um reticulado distributivo. Então, para quaisquer $I \in \mathrm{Id}(R)$ e $x \in R \setminus I$, existe $P \in \mathrm{Esp}(R)$ tal que $I \subseteq P$ e $x \notin P$.*

*Demonstração.* Seja $F = \mathrm{fil}(x)$. Tem-se que $I \cap F = \emptyset$. De facto, se existisse $y \in I \cap F$, então $y \in I$ e $x \leq y$, donde seguiria, por *(ii)* do Lema 0.3.16, que $x \in I$, o que seria uma contradição. Assim, aplicando o Teorema 1.2.8, sabe-se que existe $P \in \mathrm{Esp}(R)$ tal que $I \subseteq P$ e $P \cap F = \emptyset$. Logo, como $x \in F$, conclui-se que $x \notin P$. □

**Corolário 1.2.10** (cf. [7], Corollary 117, p. 118)**.** *Sejam $R$ um reticulado distributivo e $x, y \in R$ tais que $x \neq y$. Então existe um ideal primo de $R$ que contém exatamente um dos elementos $x$ e $y$.*

*Demonstração.* Defina-se $I = \mathrm{id}(x)$, $J = \mathrm{id}(y)$, $F = \mathrm{fil}(x)$ e $G = \mathrm{fil}(y)$. Suponha-se, por absurdo, que $I \cap G \neq \emptyset$ e $J \cap F \neq \emptyset$. Então, por um lado, existe $z \in I \cap G$, pelo que $z \leq x$ e $y \leq z$, donde, pela transitividade, segue que $y \leq x$; por outro lado, existe $w \in J \cap F$ e, analogamente, conclui-se que $x \leq y$. Assim, $x = y$, o que é um absurdo. Logo, $I \cap G = \emptyset$ ou $J \cap F = \emptyset$.

Ora, se $I \cap G = \emptyset$, então $y \notin I$. Por conseguinte, aplicando o Corolário 1.2.9, sabe-se que existe $P \in \mathrm{Esp}(R)$ tal que $I \subseteq P$ e $y \notin P$. Logo, $x \in P$ e $y \notin P$. Argumentos análogos mostram que, se $J \cap F = \emptyset$, então existe $Q \in \mathrm{Esp}(R)$ tal que $y \in Q$ e $x \notin Q$.

Portanto, em qualquer um dos casos, existe um ideal primo de $R$ que contém exatamente um dos elementos $x$ e $y$. □

Como consequência do Teorema 1.2.8, também é possível obter uma importante representação dos reticulados distributivos, provando-se que todo o reticulado distributivo é isomorfo a um sub-reticulado de $(\wp(X), \cap, \cup)$, para algum conjunto $X$. A um sub-reticulado de $(\wp(X), \cap, \cup)$ dá-se a designação de anel de conjuntos.

**Teorema 1.2.11** (cf. [7], Theorem 119, p. 118)**.** *Um reticulado $R$ é distributivo se e só se $R$ é isomorfo a algum anel de conjuntos.*

*Demonstração.* Seja $(R; \wedge, \vee)$ um reticulado.

Assuma-se, primeiramente, que $R$ é isomorfo a algum anel de conjuntos. Então, para algum conjunto $X$, $R$ é isomorfo a algum sub-reticulado de $(\wp(X); \cap, \cup)$. Assim, como $(\wp(X); \cap, \cup)$ é um reticulado distributivo, por *(i)* e *(iii)* do Teorema 1.1.6, segue que $R$ é distributivo.

Reciprocamente, admita-se que $R$ é distributivo. Para cada $x \in R$, defina-se

$$\mathcal{I}(x) = \{P \in \mathrm{Esp}(R) \mid x \notin P\}.$$

Considere-se o conjunto

$$\mathcal{I} = \{\mathcal{I}(x) \mid x \in R\}.$$

Pretende-se demonstrar que $(\mathcal{I}, \cap, \cup)$ é um anel de conjuntos.

Primeiramente, note-se que $\mathcal{I} \neq \emptyset$ (visto que $R \neq \emptyset$) e que $\mathcal{I} \subseteq \wp(\mathrm{Esp}(R))$.

Sejam $X, Y \in \mathcal{I}$. Então, $X = \mathcal{I}(x)$ e $Y = \mathcal{I}(y)$, para alguns $x, y \in R$.

Mostre-se que $X \cap Y \in \mathcal{I}$, ou seja, que existe $z \in R$ tal que $X \cap Y = \mathcal{I}(z)$. Seja $P \in X \cap Y$. Então, $P$ é um ideal primo tal que $x \notin P$ e $y \notin P$. Assim, pela definição de ideal primo (Definição 0.3.14), tem-se que $x \wedge y \notin P$. Logo, $P \in \mathcal{I}(x \wedge y)$. Portanto, $X \cap Y \subseteq \mathcal{I}(x \wedge y)$. Reciprocamente, dado $P \in \mathcal{I}(x \wedge y)$, tem-se que $P$ é um ideal primo tal que $x \wedge y \notin P$. Então, pela definição de ideal (Definição 0.3.14), tem-se que $x \notin P$ e $y \notin P$; de facto, é simples ver que, se $x \in P$ ou $y \in P$, então, pelo facto de $P$ ser ideal, ter-se-ia $x \wedge y \in P$, o que contradiria a hipótese. Logo, $P \in X \cap Y$. Portanto, $\mathcal{I}(x \wedge y) \subseteq X \cap Y$. Conclui-se, assim, o que era pretendido.

Verifique-se, agora, que $X \cup Y \in \mathcal{I}$, ou seja, que existe $w \in R$ tal que $X \cup Y = \mathcal{I}(w)$. Seja $P \in X \cup Y$. Caso $P \in X$, tem-se que $P$ é um ideal primo tal que $x \notin P$. Então, $x \vee y \notin P$; caso contrário, como $x \leq x \vee y$, ter-se-ia, por *(ii)* do Lema 0.3.16, que $x \in P$, o que não acontece. Logo, $P \in \mathcal{I}(x \vee y)$. Analogamente se prova que, se $P \in Y$, então $P \in \mathcal{I}(x \vee y)$. Portanto, $X \cup Y \subseteq \mathcal{I}(x \vee y)$. Reciprocamente, seja $P \in \mathcal{I}(x \vee y)$. Então, $P$ é um ideal primo tal que $x \vee y \notin P$. Por conseguinte, $x \notin P$ ou $y \notin P$; caso contrário, por *(i)* do Lema 0.3.16, ter-se-ia um absurdo. Portanto, $P \in X$ ou $P \in Y$, ou seja, $P \in X \cup Y$. Fica, assim, provado que $X \cup Y = \mathcal{I}(x \vee y)$, ou seja, $X \cup Y \in \mathcal{I}$.

Mostre-se, agora, que é possível definir um isomorfismo de $(R; \wedge, \vee)$ em $(I, \cap, \cup)$. Para tal, considere-se a aplicação $\varphi$ de $R$ em $\mathcal{I}$ tal que, para qualquer $x \in R$,

$$\varphi(x) = \mathcal{I}(x).$$

Esta aplicação está bem definida: para qualquer $x \in R$, $\mathcal{I}(x) \in \mathcal{I}$; além disso, é fácil ver que, dados $x, y \in R$ tais que $x = y$, se tem $\mathcal{I}(x) = \mathcal{I}(y)$, ou seja, $\varphi(x) = \varphi(y)$.

A aplicação $\varphi$ é injetiva. De facto, se $x, y \in R$ são tais que $x \neq y$, então, pelo Corolário 1.2.10, existe um ideal primo $P$ de $R$ que contém exatamente um dos elementos $x$ e $y$. Por conseguinte, $P$ pertence a exatamente um dos conjuntos $\mathcal{I}(x)$ ou $\mathcal{I}(y)$. Logo, $\mathcal{I}(x) \neq \mathcal{I}(y)$, ou seja, $\varphi(x) \neq \varphi(y)$.

Seja, agora, $X \in \mathcal{I}$. Então, $X = \mathcal{I}(x)$, para algum $x \in R$. Logo, $X = \varphi(x)$. Portanto, além de ser injetiva, a aplicação $\varphi$ é sobrejetiva, ou seja, $\varphi$ é uma bijeção.

Foi visto anteriormente que, para quaisquer $x, y \in R$, se tem

$$\mathcal{I}(x \wedge y) = \mathcal{I}(x) \cap \mathcal{I}(y) \quad \text{e} \quad \mathcal{I}(x \vee y) = \mathcal{I}(x) \cup \mathcal{I}(y),$$

ou seja,

$$\varphi(x \wedge y) = \varphi(x) \cap \varphi(y) \quad \text{e} \quad \varphi(x \vee y) = \varphi(x) \cup \varphi(y).$$

Portanto, $\varphi$ é um homomorfismo de reticulados.

Conclui-se, assim, o que era pretendido, donde resulta que $R \cong \mathcal{I}$. $\square$

### 1.2.3 Caraterização e representação de reticulados distributivos recorrendo a relações de congruência

Nesta subsecção, dá-se continuidade ao estudo sobre relações de congruência em reticulados, abordando, agora, as suas propriedades quando os reticulados aos quais estão associadas forem distributivos.

**Teorema 1.2.12** (cf. [2], Theorem 8.10, p. 126)**.** *Seja $R$ um reticulado distributivo. Então, para quaisquer $x, y \in R$,*

$$\mathrm{con}(x,y) = \{(z,w) \in R^2 \mid z \wedge x \wedge y = w \wedge x \wedge y \quad e \quad z \vee x \vee y = w \vee x \vee y\}.$$

*Demonstração.* Defina-se

$$\theta = \{(z,w) \in R^2 \mid z \wedge x \wedge y = w \wedge x \wedge y \quad \text{e} \quad z \vee x \vee y = w \vee x \vee y\}.$$

Mostre-se que $\theta$ é a menor congruência em $R$ que contém o par $(x, y)$. É óbvio que $\theta$ é reflexiva e simétrica. Sejam $z, w, v \in R$ tais que $z\theta w$ e $w\theta v$. Assim,

*(I)* $z \wedge x \wedge y = w \wedge x \wedge y$;

*(II)* $z \vee x \vee y = w \vee x \vee y$;

*(III)* $w \wedge x \wedge y = v \wedge x \wedge y$;

*(IV)* $w \vee x \vee y = v \vee x \vee y$.

Logo, por *(I)* e *(III)*, $z \wedge x \wedge y = v \wedge x \wedge y$ e, por *(II)* e *(IV)*, $z \vee x \vee y = v \vee x \vee y$, pelo que $z\theta v$, o que prova a transitividade de $\theta$. Sejam, agora, $z, w, r \in R$ tais que $z\theta w$. Então, são válidas as condições *(I)* e *(II)*, donde resulta

$$(z \wedge r) \wedge x \wedge y = (z \wedge x \wedge y) \wedge r = (w \wedge x \wedge y) \wedge r = (w \wedge r) \wedge x \wedge y$$

e

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

Logo, $(z \wedge r)\theta(w \wedge r)$. Procedendo de forma semelhante, também se conclui que $(z \vee r)\theta(w \vee r)$. Portanto, $\theta$ é uma congruência em $R$.

Também não é difícil verificar que $x\theta y$. De facto,

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

Por fim, considere-se uma qualquer congruência $\vartheta$ em $R$ tal que $x\vartheta y$. Sejam $z, w \in R$ tais que $z\theta w$. Por um lado, por definição de $\theta$, tem-se

*(V)* $z \wedge x \wedge y = w \wedge x \wedge y$;

*(VI)* $z \vee x \vee y = w \vee x \vee y$.

Por outro lado, como $\vartheta$ é uma congruência, tem-se, por *(ii)* do Lema 0.3.29, $(x \wedge y)\vartheta(x \vee y)$ e, consequentemente,

*(VII)* $(z \wedge x \wedge y)\vartheta(z \wedge (x \vee y))$;

*(VIII)* $(z \vee (x \wedge y))\vartheta(z \vee x \vee y)$.

Ora, por *(VI)* e *(VIII)*, tem-se

$$(z \vee (x \wedge y))\vartheta(w \vee x \vee y),$$

pelo que

$$(z \wedge (z \vee (x \wedge y)))\vartheta(z \wedge (w \vee x \vee y)),$$

ou seja,

$$z\vartheta((z \wedge w) \vee (z \wedge x) \vee (z \wedge y)).$$

Além disso, por *(V)* e *(VII)*, segue que

$$(w \wedge x \wedge y)\vartheta(z \wedge (x \vee y)).$$

Assim,

$$((z \wedge w) \vee (w \wedge x \wedge y))\vartheta((z \wedge w) \vee (z \wedge (x \vee y))),$$

ou seja,

$$((z \wedge w) \vee (w \wedge x \wedge y))\vartheta((z \wedge w) \vee (z \wedge x) \vee (z \wedge y)).$$

Logo, pela simetria e transitividade,

$$z\vartheta((w \wedge z) \vee (w \wedge x \wedge y)),$$

isto é,

$$z\vartheta(w \wedge (z \vee (x \wedge y))).$$

Além disso, por *(VIII)*, tem-se

$$(w \wedge (z \vee (x \wedge y)))\vartheta(w \wedge (z \vee x \vee y)),$$

onde, por *(VI)*,

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

Logo, por transitividade, $z\vartheta w$, pelo que $\theta \subseteq \vartheta$.

Portanto, $\operatorname{con}(x, y) = \theta$. □

Apresentam-se, de seguida, alguns corolários do teorema anterior.

**Corolário 1.2.13** (cf. [7], Theorem 141, pp. 138–139)**.** *Seja $R$ um reticulado distributivo. Então, para quaisquer $x, y \in R$ tais que $x \leq y$,*

$$\mathrm{con}(x, y) = \{(z, w) \in R^2 \mid z \wedge x = w \wedge x \quad \text{e} \quad z \vee y = w \vee y\}.$$

**Corolário 1.2.14** (cf. [8], Theorem 1, pp. 141–142)**.** *Seja $(R; \wedge, \vee)$ um reticulado distributivo e tomem--se $x, y \in R$ tais que $x \leq y$. Então, para quaisquer $z, w \in R$ tais que $z \leq w$, são equivalentes as condições seguintes:*

*(i)* $(z, w) \in \mathrm{con}(x, y)$;

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

*Demonstração.* Sejam $z, w \in R$ tais que $z \leq w$.

Suponha-se, primeiramente, que $(z, w) \in \mathrm{con}(x, y)$. Então, pelo Corolário 1.2.13,

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

Assim,

$$\begin{aligned} (x \vee z) \wedge w &= (x \wedge w) \vee (z \wedge w) && \text{[distributividade]} \\ &= (x \wedge z) \vee z && [x \wedge w = x \wedge z; z \leq w] \\ &= z && \text{[absorção]} \end{aligned}$$

e

$$\begin{aligned} (y \vee z) \wedge w &= (y \vee w) \wedge w && [y \vee z = y \vee w] \\ &= w. && \text{[absorção]} \end{aligned}$$

Reciprocamente, assuma-se que a condição *(ii)* é válida. Segundo o Corolário 1.2.13, para provar que $(z, w) \in \mathrm{con}(x, y)$, basta verificar que

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

Ora,

$$\begin{aligned} z \wedge x &= (x \vee z) \wedge w \wedge x && \text{[hipótese]} \\ &= w \wedge x. && \text{[absorção]} \end{aligned}$$

Além disso, como, pela Proposição 1.1.5, $R$ é também modular, segue

$$\begin{aligned} w &= (y \vee z) \wedge w && \text{[hipótese]} \\ &= (y \wedge w) \vee z. && [z \leq w \text{ e modularidade]} \end{aligned}$$

Logo,

$$\begin{aligned} w \vee y &= (y \wedge w) \vee z \vee y \\ &= z \vee y, && \text{[absorção]} \end{aligned}$$

tal como se pretendia provar.

Fica assim concluída a demonstração. □

**Corolário 1.2.15** (cf. [7], Corollary 143, p. 141)**.** *Sejam $R$ um reticulado distributivo e $x, y, z, w \in R$ tais que $x \leq y \leq z \leq w$ ou $z \leq w \leq x \leq y$. Então,*

$$(z, w) \in \operatorname{con}(x, y) \implies z = w.$$

**Teorema 1.2.16** (cf. [2], Theorem 8.11, pp. 126–127)**.** *Seja $R$ um reticulado distributivo. Então, a interseção de duas congruências principais em $R$ é também uma congruência principal. Mais precisamente, dados $x, y, z, w \in R$ tais que $x \leq y$ e $z \leq w$, tem-se*

$$\operatorname{con}(x, y) \cap \operatorname{con}(z, w) = \operatorname{con}(y \wedge w \wedge (x \vee z), y \wedge w).$$

*Demonstração.* Sejam $x, y, z, w \in R$ tais que $x \leq y$ e $z \leq w$.

Considerando o Lema 0.3.30, para mostrar que

$$\operatorname{con}(y \wedge w \wedge (x \vee z), y \wedge w) \subseteq \operatorname{con}(x, y) \cap \operatorname{con}(z, w),$$

é suficiente verificar que

$$(y \wedge w \wedge (x \vee z), y \wedge w) \in \operatorname{con}(x, y) \cap \operatorname{con}(z, w).$$

Ora, é facil ver que

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

e que

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

Logo, pelo Corolário 1.2.13,

$$(y \wedge w \wedge (x \vee z), y \wedge w) \in \operatorname{con}(x, y).$$

De forma semelhante se prova que

$$(y \wedge w \wedge (x \vee z), y \wedge w) \in \operatorname{con}(z, w).$$

Reciprocamente, seja $(r, s) \in \operatorname{con}(x, y) \cap \operatorname{con}(z, w)$. Então, sabendo que $x \leq y$ e $z \leq w$ e recorrendo ao Corolário 1.2.13, tem-se

*(I)* $r \wedge x = s \wedge x$;

*(II)* $r \vee y = s \vee y$;

*(III)* $r \wedge z = s \wedge z$;

*(IV)* $r \vee w = s \vee w$.

Além disso, como $y \wedge w \wedge (x \vee z) \leq y \wedge w$, sabe-se, pelo Corolário 1.2.13, que

$$\operatorname{con}(y \wedge w \wedge (x \vee z), y \wedge w) = \left\{ (a, b) \in R^2 \;\middle|\; \begin{array}{l} a \wedge (y \wedge w \wedge (x \vee z)) = b \wedge (y \wedge w \wedge (x \vee z)), \\ a \vee (y \wedge w) = b \vee (y \wedge w) \end{array} \right\}.$$

Ora,

$$\begin{aligned} r \wedge (y \wedge w \wedge (x \vee z)) &= (r \wedge y \wedge w \wedge x) \vee (r \wedge y \wedge w \wedge z) && \text{[distributividade]} \\ &= (r \wedge x \wedge w) \vee (r \wedge z \wedge y) && [x \leq y;\, z \leq w] \\ &= (s \wedge x \wedge w) \vee (s \wedge z \wedge y) && \text{[(I) e (III)]} \\ &= (s \wedge y \wedge w \wedge x) \vee (s \wedge y \wedge w \wedge z) && [x \leq y;\, z \leq w] \\ &= s \wedge (y \wedge w \wedge (x \vee z)) && \text{[distributividade]} \end{aligned}$$

e

$$\begin{aligned} r \vee (y \wedge w) &= (r \vee y) \wedge (r \vee w) && \text{[distributividade]} \\ &= (s \vee y) \wedge (s \vee w) && \text{[(II) e (IV)]} \\ &= s \vee (y \wedge w). && \text{[distributividade]} \end{aligned}$$

Portanto, $(r, s) \in \operatorname{con}(y \wedge w \wedge (x \vee z), y \wedge w)$. Conclui-se assim que

$$\operatorname{con}(x, y) \cap \operatorname{con}(z, w) \subseteq \operatorname{con}(y \wedge w \wedge (x \vee z), y \wedge w),$$

o que completa a prova. □

**Teorema 1.2.17** (cf. [7], Corollary 142, pp. 140–141)**.** *Sejam $R$ um reticulado distributivo e $I \in \operatorname{Id}(R)$. Então,*

$$\operatorname{con}(I) = \{(x, y) \in R^2 \mid x \vee y = (x \wedge y) \vee a, \text{ para algum } a \in I\}.$$

*Além disso, $I$ é uma classe de congruência de $\operatorname{con}(I)$ em $R$.*

*Demonstração.* Defina-se

$$\theta = \{(x, y) \in R^2 \mid x \vee y = (x \wedge y) \vee a, \text{ para algum } a \in I\}.$$

Pretende-se provar que $\theta \in \mathrm{Con}(R)$.

Seja $x \in R$. Como $I \neq \emptyset$, existe $a \in I$. Por conseguinte, $x \wedge a \in I$. Então,

$$x \vee x = x = x \vee (x \wedge a) = (x \wedge x) \vee (x \wedge a).$$

Logo, $x\theta x$. Portanto, $\theta$ satisfaz *(i)* do Lema 0.3.29.

É óbvio que $\theta$ também observa *(ii)* do mesmo lema.

Sejam $x, y, z \in R$ tais que $x \leq y \leq z$ e suponha-se que $x\theta y$ e $y\theta z$. Então, existem $a, b \in I$ tais que $x \vee y = (x \wedge y) \vee a$ e $y \vee z = (y \wedge z) \vee b$, ou seja, $y = x \vee a$ e $z = y \vee b$. Assim,

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

com $a \vee b \in I$. Logo, $x\theta z$, provando-se, assim, que *(iii)* do Lema 0.3.29 também é válida.

Sejam $x, y \in R$ tais que $x \leq y$ e $x\theta y$. Então, existe $a \in I$ tal que $x \vee y = (x \wedge y) \vee a$, ou seja, $y = x \vee a$. Assim, como, para qualquer $w \in R$, $x \wedge w \leq y \wedge w$, então

$$\begin{aligned}(x \wedge w) \vee (y \wedge w) &= y \wedge w\\ &= (x \vee a) \wedge w\\ &= (x \wedge w) \vee (a \wedge w)\\ &= ((x \wedge w) \wedge (y \wedge w)) \vee (a \wedge w),\end{aligned}$$

com $a \wedge w \in I$; também se tem $x \vee w \leq y \vee w$ e, por isso,

$$\begin{aligned}(x \vee w) \vee (y \vee w) &= y \vee w\\ &= (x \vee a) \vee w\\ &= (x \vee w) \vee a\\ &= ((x \vee w) \wedge (y \vee w)) \vee a;\end{aligned}$$

logo, $(x \wedge w)\theta(y \wedge w)$ e $(x \vee w)\theta(y \vee w)$. Portanto, $\theta$ respeita também a condição *(iv)* do Lema 0.3.29, pelo que se confirma que $\theta \in \mathrm{Con}(R)$.

Seja $(u, v) \in I^2$. Então,

$$u \vee v = (u \wedge v) \vee (u \vee v),$$

onde, claramente, $u \vee v \in I$. Logo, $u\theta v$, donde se conclui que $I^2 \subseteq \theta$.

Seja $\vartheta \in \mathrm{Con}(R)$ tal que $I^2 \subseteq \vartheta$. Sejam, também, $x, y \in R$ tais que $x\theta y$. Então, existe $a \in I$ tal que $x \vee y = (x \wedge y) \vee a$. Assim, como $x \wedge y \wedge a \in I$, tem-se $(x \wedge y \wedge a, a) \in I^2$ e, portanto, $(x \wedge y \wedge a)\vartheta a$. Como $\vartheta \in \mathrm{Con}(R)$, segue que

$$((x \wedge y) \vee (x \wedge y \wedge a))\vartheta((x \wedge y) \vee a),$$

ou seja,

$$(x \wedge y)\vartheta(x \vee y),$$

donde resulta que $x\vartheta y$. Portanto, $\theta \subseteq \vartheta$.

Conclui-se, assim, que $\mathrm{con}(I) = \theta$.

Por fim, sejam $a \in I$ e $b \in R$ tais que $(a, b) \in \mathrm{con}(I)$. Então, $a \vee b = (a \wedge b) \vee u$, para algum $u \in I$. Assim, como $a \wedge b, u \in I$, tem-se que $a \vee b = (a \wedge b) \vee u \in I$. Portanto, uma vez que $b \leq a \vee b$, segue que $b \in I$, ficando assim provado que $I$ é uma classe de congruência de $\mathrm{con}(I)$ em $R$. □

Estabelecem-se, de seguida, algumas caraterizações para reticulados distributivos, com base em propriedades de congruências.

**Teorema 1.2.18** (cf. [8], Theorem 2, pp. 143–145)**.** *Seja $R$ um reticulado. Todas as condições seguintes são equivalentes:*

*(i)* *$R$ é um reticulado distributivo;*

*(ii)* *para quaisquer $x, y, z, w \in R$, se $(z, w) \in \mathrm{con}(x, y)$, então é impossível que $x \leq w$ (ou $z \leq y$) sempre que $y \leq x$ e $w < z$;*

*(iii)* *para quaisquer $x, y \in R$ tais que $y \leq x$, o intervalo $[y, x]$ é uma classe de congruência de $\mathrm{con}(x, y)$ em $R$;*

*(iv)* *para quaisquer $x, y, z, w \in R$ tais que $w \leq z \leq y \leq x$, $\mathrm{con}(x, y) \cap \mathrm{con}(z, w) = \triangle_R$;*

*(v)* *para quaisquer $I \in \mathrm{Id}(R)$ e $x, y \in R$ tais que $y \leq x$, $(x, y) \in \mathrm{con}(I)$ se e só se $x = y \vee a$, para algum $a \in I$.*

*Demonstração.* Suponha-se, primeiramente, que o reticulado $R$ é distributivo.

Pretende-se provar *(ii)*. Para tal, sejam $x, y, z, w \in R$. Admita-se que

$$(z, w) \in \mathrm{con}(x, y) = \mathrm{con}(y, x)$$

e que $y \leq x$ e $w < z$. Assim, $(w, z) \in \mathrm{con}(x, y)$ e, pelo Corolário 1.2.14, tem-se

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

Ora, se $x \leq w$, então

$$\begin{aligned} z &= (x \vee w) \wedge z && [\textit{(II)}] \\ &= w \wedge z && [x \leq w] \\ &= w, && [w < z] \end{aligned}$$

o que contradiria a hipótese. De modo análogo se prova que, se $z \leq y$, então, por *(I)*, também haveria uma contradição. De facto, *(ii)* verifica-se.

Mostre-se, agora, que *(iii)* também é válida. Para tal, sejam $x, y \in R$ tais que $y \leq x$. Para provar que $[y, x]$ é uma classe de congruência de $\operatorname{con}(x, y)$ em $R$, uma vez que $y \in [y, x]$, basta mostrar que

$$[y, x] = [y]_{\operatorname{con}(x,y)}.$$

Seja $z \in [y, x]$. Então, $y \leq z \leq x$. Assim, como $(x, y) \in \operatorname{con}(x, y)$, tem-se

$$(z, y) = (x \wedge z, y \wedge z) \in \operatorname{con}(x, y).$$

Logo, $z \in [y]_{\operatorname{con}(x,y)}$, donde segue que

$$[y, x] \subseteq [y]_{\operatorname{con}(x,y)}.$$

Seja $z \in [y]_{\operatorname{con}(x,y)}$. Então, $(z, y) \in \operatorname{con}(x, y)$. Suponha-se, por absurdo, que $z \notin [y, x]$. Assim,

$$z \wedge y < y \quad \text{ou} \quad x < z \vee x;$$

de facto, se $z \wedge y = y$ e $x = z \vee x$, ter-se-ia $y \leq z \leq x$, ou seja, $z \in [y, x]$, o que não acontece. Mais ainda, uma vez que $(z, y) \in \operatorname{con}(x, y)$ e, consequentemente, $(z, x) \in \operatorname{con}(x, y)$, segue que

$$(z \wedge y, y) = (z \wedge y, y \wedge y) \in \operatorname{con}(x, y)$$

e

$$(z \vee x, x) = (z \vee x, x \vee x) \in \operatorname{con}(x, y).$$

Ora, caso $z \wedge y < y$, e juntando isso ao facto de $(y, z \wedge y) \in \operatorname{con}(x, y)$ e $y \leq x$, segue, por *(ii)*, que é impossível que $y \leq y$, o que é uma contradição. Analogamente se prova que $x < z \vee x$ também conduz a uma contradição. Logo, $z \in [y, x]$, pelo que

$$[y]_{\operatorname{con}(x,y)} \subseteq [y, x].$$

Conclui-se, assim, que

$$[y, x] = [y]_{\operatorname{con}(x,y)},$$

tal como era pretendido. Portanto, *(iii)* também se verifica.

Prove-se, agora, a condição *(iv)*. Para tal, tomem-se $x, y, z, w \in R$ tais que $w \leq z \leq y \leq x$. Então,

$$\begin{aligned}
\operatorname{con}(x, y) \cap \operatorname{con}(z, w) &= \operatorname{con}(y, x) \cap \operatorname{con}(w, z) && \text{[qualquer congruência é simétrica]}\\
&= \operatorname{con}(x \wedge z \wedge (y \vee w), x \wedge z) && \text{[Teorema 1.2.16]}\\
&= \operatorname{con}(z \wedge y, z) && [z \leq x \text{ e } w \leq y]\\
&= \operatorname{con}(z, z). && [z \leq y]
\end{aligned}$$

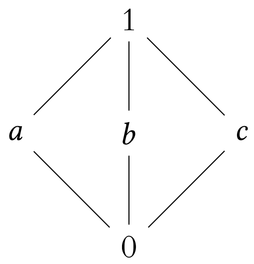
Uma vez que $\mathrm{con}(z, z) = \triangle_R$, então

$$\mathrm{con}(x, y) \cap \mathrm{con}(z, w) = \triangle_R.$$

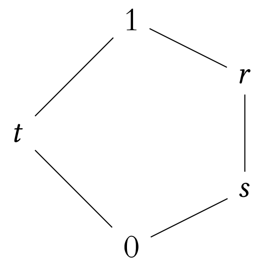
Portanto, *(iv)* também é válida.

A condição *(v)* é óbvia, atendendo ao Teorema 1.2.17.

Reciprocamente, admita-se que o reticulado $R$ não é distributivo. Então, por *(ii)* do Teorema 1.2.1, existe algum sub-reticulado $S$ de $R$ tal que $S \cong M_3$ ou $S \cong N_5$. Assim, para demonstrar que as condições *(ii)–(v)* não se verificam em $R$, basta provar que as mesmas condições falham nos reticulados $M_3$ e $N_5$ dados, respetivamente, por




e




.

Mostre-se, primeiramente, que *(ii)* não é válida em $M_3$. Ora, definindo $x = w = a$, $y = 0$ e $z = 1$, tem-se $x \leq w$, $y \leq x$ e $w < z$. Porém, como

$$(a, 0) = (x, y) \in \mathrm{con}(x, y),$$

então

$$(1, b) = (a \vee b, 0 \vee b) \in \mathrm{con}(x, y),$$

e, por conseguinte,

$$(c, 0) = (1 \wedge c, b \wedge c) \in \mathrm{con}(x, y).$$

Assim, por transitividade, $(a, c) \in \mathrm{con}(x, y)$. Logo,

$$(z, w) = (1, a) = (c \vee a, a \vee a) \in \mathrm{con}(x, y),$$

pelo que *(ii)* falha em $M_3$. Mostre-se, agora, que *(ii)* não é válida em $N_5$. Definindo, agora, $x = 1$, $y = z = r$ e $w = s$, tem-se $z \leq y$, $y \leq x$ e $w < z$. Mas, como

$$(1, r) = (x, y) \in \mathrm{con}(x, y),$$

então

$$(t, 0) = (1 \wedge t, r \wedge t) \in \mathrm{con}(x, y)$$

e, consequentemente,

$$(1, s) = (t \vee s, 0 \vee s) \in \mathrm{con}(x, y).$$

Logo, pela transitividade, tem-se

$$(z, w) = (r, s) \in \operatorname{con}(x, y),$$

o que mostra que *(ii)* também não se verifica em $N_5$.

Veja-se, agora, que *(iii)* não é válida nem em $M_3$ nem em $N_5$. Ora, em $M_3$, tem-se que $[0, a] = \{0, a\}$. Além disso, já foi visto no parágrafo anterior que $(a, 0) \in \operatorname{con}(a, 0)$ implica $(c, 0) \in \operatorname{con}(a, 0)$. Contudo, $c \notin [0, a]$. Logo, $[0, a]$ não é uma classe de congruência de $\operatorname{con}(a, 0)$ em $M_3$. De forma semelhante se prova que $[r, 1]$ não é uma classe de congruência de $\operatorname{con}(1, r)$ em $N_5$.

Mostre-se, agora, que *(iv)* não só falha em $M_3$ como também em $N_5$. Ora, em $M_3$, tem-se que $1 \geq a \geq a \geq 0$, mas

$$\operatorname{con}(1, a) \cap \operatorname{con}(a, 0) \neq \triangle_{M_3}.$$

De facto,

$$(1, a) \in \operatorname{con}(1, a) \cap \operatorname{con}(a, 0)$$

e $1 \neq a$. Analogamente, em $N_5$, tem-se

$$(r, s) \in \operatorname{con}(r, s) \cap \operatorname{con}(s, 0),$$

com $r \neq s$ e, portanto,

$$\operatorname{con}(r, s) \cap \operatorname{con}(s, 0) \neq \triangle_{N_5},$$

apesar de $r \geq s \geq s \geq 0$.

Resta provar que *(v)* não é satisfeita quer em $M_3$ quer em $N_5$. Considere-se $I \in \operatorname{Id}(N_5)$ dado por $I = \operatorname{id}(s) = \{0, s\}$. Como

$$(s, 0) \in I^2 \subseteq \operatorname{con}(I),$$

tem-se

$$(1, t) = (s \vee t, 0 \vee t) \in \operatorname{con}(I),$$

donde

$$(r, 0) = (1 \wedge r, t \wedge r) \in \operatorname{con}(I),$$

com $r \geq 0$. No entanto, não existe $u \in I$ tal que $r = 0 \vee u$. Analogamente se justifica que, considerando, em $M_3$, o ideal $J = \operatorname{id}(a) = \{0, a\}$, se obtém $(c, 0) \in \operatorname{con}(I)$, onde $c \geq 0$, mas não existe $v \in J$ tal que $c = 0 \vee v$.

Fica assim concluída a prova do teorema. □

Será interessante analisar se a distributividade se verifica em $\operatorname{Con}(R)$, sendo $R$ um reticulado.

**Teorema 1.2.19** (cf. [7], Theorem 149, pp. 145–146)**.** *Seja $R$ um reticulado. Então, o reticulado das congruências em $R$, $\operatorname{Con}(R)$, é distributivo.*

*Demonstração.* Sejam $\theta, \eta, \zeta \in \mathrm{Con}(R)$. Pelo que já foi estudado, para provar que

$$\theta \wedge (\eta \vee \zeta) = (\theta \wedge \eta) \vee (\theta \wedge \zeta),$$

basta verificar que

$$\theta \wedge (\eta \vee \zeta) \subseteq (\theta \wedge \eta) \vee (\theta \wedge \zeta).$$

Sejam $x, y \in R$ tais que $x(\theta \wedge (\eta \vee \zeta))y$. Então, aplicando sucessivamente o Teorema 0.3.31, tem-se $x\theta y$ e $x(\eta \vee \zeta)y$, pelo que existem $r_1, r_2, \ldots, r_n \in R$, para algum $n \in \mathbb{N}$, tais que

$$x \wedge y = r_1 \leq r_2 \leq \cdots \leq r_n = x \vee y$$

e, para cada $i \in \{1, 2, \ldots, n-1\}$, $r_i \eta r_{i+1}$ ou $r_i \zeta r_{i+1}$. Ora, como $x\theta y$, então $(x \wedge y)\theta(x \vee y)$, ou seja, $r_1 \theta r_n$. Assim, para cada $i \in \{1, 2, \ldots, n-1\}$,

$$(r_1, r_i) = (r_1 \wedge r_i, r_n \wedge r_i) \in \theta$$

e

$$(r_1, r_{i+1}) = (r_1 \wedge r_{i+1}, r_n \wedge r_{i+1}) \in \theta,$$

pelo que $r_i \theta r_{i+1}$. Por conseguinte, para cada $i \in \{1, 2, \ldots, n-1\}$, $r_i(\theta \wedge \eta)r_{i+1}$ ou $r_i(\theta \wedge \zeta)r_{i+1}$. Logo, $x((\theta \wedge \eta) \vee (\theta \wedge \zeta))y$, o que conclui a prova. □

### 1.2.4 Caraterização e representação de reticulados distributivos recorrendo a elementos especiais

Nesta subsecção, são abordadas propriedades dos reticulados distributivos envolvendo elementos especiais desses reticulados, como é o caso dos elementos $\wedge$-irredutíveis/$\vee$-irredutíveis, dos elementos primos e dos elementos complementados.

Em particular, prova-se que qualquer reticulado distributivo finito pode ser representado como um sub-reticulado de um produto de cadeias finitas.

O Teorema 0.3.47 enuncia que qualquer reticulado $(R; \wedge, \vee)$ que satisfaz a c.c.d. tem elemento mínimo $0$ e qualquer $x \in R \backslash \{0\}$ pode ser representado como supremo de um número finito de elementos $\vee$-irredutíveis de $R$. No caso dos reticulados distributivos, prova-se que essa representação é única.

**Teorema 1.2.20** (cf. [2], Theorem 4.9, p. 59)**.** *Sejam $(R; \wedge, \vee)$ um reticulado modular que satisfaz a c.c.d. e $x \in R \setminus \{0\}$. Suponha-se que $x$ tem duas representações*

$$x = \bigvee_{i=1}^{m} x_i = \bigvee_{j=1}^{n} y_j$$

*como supremo de um número finito ($m, n \in \mathbb{N}$) de elementos $\vee$-irredutíveis de $R$ ($x_i, y_j \in \mathcal{S}(R)$, para quaisquer $i \in \{1, \ldots, m\}$ e $j \in \{1, \ldots, n\}$). Então, para cada $i \in \{1, \ldots, m\}$, existe $j \in \{1, \ldots, n\}$ tal que*

$$x = x_1 \vee \cdots \vee x_{i-1} \vee y_j \vee x_{i+1} \vee \cdots \vee x_m.$$

*Demonstração.* Sejam $i \in \{1, \ldots, m\}$,

$$a = x_1 \vee \cdots \vee x_{i-1} \vee x_{i+1} \vee \cdots \vee x_m$$

e, para cada $t \in \{1, \ldots, n\}$, defina-se $z_t = y_t \vee a$. Então, $x = x_i \vee a$ e

$$\bigvee_{t=1}^{n} z_t = \bigvee_{t=1}^{n} y_t \vee a = x \vee a = x.$$

Como $R$ é modular, então, por *(iv)* do Teorema 1.2.5, tem-se que $[x_i \wedge a, x_i] \cong [a, x_i \vee a]$. Como $x_i \in \mathcal{S}(R)$, então $x_i \in \mathcal{S}([x_i \wedge a, x_i])$. Assim, pelo Teorema 1.2.5 e pela Proposição 0.3.46, tem-se

$$x = x_i \vee a = \psi_a(x_i) \in \mathcal{S}([a, x_i \vee a]) = \mathcal{S}([a, x]).$$

Ora, uma vez que $x = \bigvee_{t=1}^{n} z_t$, onde, para qualquer $t \in \{1, \ldots, n\}$,

$$a \leq z_t \leq \bigvee_{t=1}^{n} z_t = x,$$

isto é, $z_t \in [a, x]$, tem-se $x = z_j$, para algum $j \in \{1, \ldots, n\}$. Logo,

$$x = z_j = y_j \vee a = x_1 \vee \cdots \vee x_{i-1} \vee y_j \vee x_{i+1} \vee \cdots \vee x_m,$$

tal como era pretendido. □

Grosso modo, o Teorema 1.2.20 afirma que, num reticulado modular $R$ que satisfaz a c.c.d. e em que qualquer $x \in R \setminus \{0\}$ tem duas representações

$$x = \bigvee_{i=1}^{m} x_i = \bigvee_{j=1}^{n} y_j$$

como supremo de um número finito de elementos $\vee$-irredutíveis de $R$, qualquer $x_i$ na representação $\bigvee_{i=1}^{m} x_i$ de $x$ pode ser substituído por algum $y_j$ da representação $\bigvee_{j=1}^{n} y_j$ de $x$.

**Definição 1.2.21.** Sejam $(R; \wedge, \vee)$ um reticulado e $x \in R$ tal que

$$x = \bigvee_{i=1}^{m} x_i,$$

com $m \in \mathbb{N}$ e $x_1, \ldots, x_m \in R$. Se existir $k \in \{1, \ldots, m\}$ tal que

$$x = x_1 \vee \cdots \vee x_{k-1} \vee x_{k+1} \vee \cdots \vee x_m,$$

dir-se-á que o elemento $x_k$ é *redundante em* $\bigvee_{i=1}^{m} x_i$; caso contrário, dir-se-á que o supremo $\bigvee_{i=1}^{m} x_i$ é *não redundante*.

De modo informal, note-se que, num supremo de um número finito de elementos de um reticulado $R$ onde haja componentes redundantes, basta retirar essas componentes para obter um supremo não redundante.

Por isso, doravante apenas se considerarão supremos não redundantes.

**Teorema 1.2.22** (Teorema de Kurosh-Ore; cf. [2], Theorem 4.10, p. 60)**.** *Sejam $(R; \wedge, \vee)$ um reticulado modular que satisfaz a c.c.d. e $x \in R$. Então, todas as representações de $x$ como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$ têm o mesmo número de componentes.*

*Demonstração.* Suponha-se que

$$\bigvee_{i=1}^{m} x_i \quad \text{e} \quad \bigvee_{j=1}^{n} y_j,$$

com $m, n \in \mathbb{N}$, são duas representações de $x$ como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$. Sem perda de generalidade, admita-se que $m \in \mathbb{N}$ é o menor número possível de componentes de uma representação de $x$ como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$. Assim sendo, é claro que $m \leq n$. Resta provar que $n \leq m$. Ora, pelo Teorema 1.2.20, pode substituir-se $x_1$ em $\bigvee_{i=1}^{m} x_i$ por algum $y_{j_1}$, ou seja, existe $j_1 \in \{1, \ldots, n\}$ tal que

$$x = y_{j_1} \vee x_2 \vee \cdots \vee x_m,$$

sendo que o supremo

$$y_{j_1} \vee x_2 \vee \cdots \vee x_m$$

continua a ser não redundante; caso contrário, contradir-se-ia o que foi pressuposto relativamente a $m$. Deste modo, aplicando continuamente o Teorema 1.2.20, pode substituir-se cada $x_i$ em $\bigvee_{i=1}^{m} x_i$ por algum $y_{j_i}$, obtendo-se, assim,

$$x = y_{j_1} \vee y_{j_2} \vee \cdots \vee y_{j_m} = \bigvee_{i=1}^{m} y_{j_i},$$

onde o supremo

$$\bigvee_{i=1}^{m} y_{j_i}$$

é não redundante. Como

$$\{y_{j_1}, y_{j_2}, \ldots, y_{j_m}\} \subseteq \{y_1, y_2, \ldots, y_n\},$$

$$\bigvee_{i=1}^{m} y_{j_i} = \bigvee_{j=1}^{n} y_j$$

e o supremo

$$\bigvee_{j=1}^{n} y_j$$

é também não redundante, então todas as componentes de $\bigvee_{j=1}^{n} y_j$ têm de fazer parte das componentes da representação $\bigvee_{i=1}^{m} y_{j_i}$ de $x$; caso contrário, existiriam elementos redundantes entre as componentes da representação

$$\bigvee_{j=1}^{n} y_j$$

de $x$, o que, por hipótese, não acontece. Logo, $n \leq m$, como era pretendido. Portanto, $n = m$. $\square$

Pelo teorema anterior, num reticulado modular $(R; \wedge, \vee)$ que satisfaz a c.c.d., todas as representações de um elemento como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$ têm o mesmo número de componentes. Se, adicionalmente, $R$ for distributivo, além do que foi descrito, verifica-se que qualquer elemento de $x \in R \setminus \{0\}$ tem uma única representação como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$. É o que enuncia o teorema seguinte.

**Teorema 1.2.23** (cf. [2], Theorem 5.2, pp. 69–70)**.** *Sejam $(R; \wedge, \vee)$ um reticulado distributivo que satisfaz a c.c.d.. Então, qualquer $x \in R \setminus \{0\}$ pode ser representado, de forma única, como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$.*

*Demonstração.* Seja $x \in R \setminus \{0\}$. Pelo Teorema 0.3.47, sabe-se que $x$ admite alguma representação como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$. Assim, resta mostrar que esta representação é única. Suponha-se que $x$ tem as representações

$$x = \bigvee_{i=1}^{m} x_i = \bigvee_{j=1}^{n} y_j$$

como supremo não redundante de um número finito de elementos $\vee$-irredutíveis de $R$. Uma vez que estas duas representações de $x$ são não redundantes e, pelo Teorema 1.2.22, se tem $m = n$, resta provar que, para cada $p \in \{1, \ldots, m\}$, existe $q \in \{1, \ldots, n\}$ tal que $x_p = y_q$. Seja, então, $p \in \{1, \ldots, m\}$. Ora, pelo Teorema 1.2.20, tem-se que, para algum $q \in \{1, \ldots, n\}$, $x = x_p \vee r = y_q \vee r$, onde

$$r = x_1 \vee \cdots \vee x_{p-1} \vee x_{p+1} \vee \cdots \vee x_m.$$

Assim,

$$\begin{aligned} x_p &= x_p \wedge x && \text{[absorção]} \\ &= x_p \wedge (y_q \vee r) \\ &= (x_p \wedge y_q) \vee (x_p \wedge r), && \text{[distributividade]} \end{aligned}$$

donde, pelo facto de $x_p$ ser $\vee$-irredutível, $x_p = x_p \wedge y_q$ ou $x_p = x_p \wedge r$, ou seja, $x_p \leq y_q$ ou $x_p \leq r$. Só que não é possível que $x_p \leq r$: efetivamente, ter-se-ia $r = x_p \vee r = x$ e, portanto, $x_p$ seria redundante em $\bigvee_{i=1}^{m} x_i$, o que contradiria a hipótese. Logo, $x_p \leq y_q$. Aplicando, agora, novamente o Teorema 1.2.20, tem-se que, para algum $k \in \{1, \ldots, m\}$, $x = y_q \vee s = x_k \vee s$, onde

$$s = y_1 \vee \cdots \vee y_{q-1} \vee y_{q+1} \vee \cdots \vee y_n.$$

Por argumentos análogos aos anteriores, obtém-se $y_q \leq x_k$. Por conseguinte, $x_p \leq y_q \leq x_k$. Então, $x_k = x_p \vee x_k$, pelo que, se $p \neq k$, $x_p$ seria redundante em $\bigvee_{i=1}^{m} x_i$, o que, por hipótese, não acontece. Portanto, $p = k$, donde resulta $x_p = y_q$, tal como era pretendido. □

No resultado seguinte, estabelecem-se algumas caraterizações da distributividade de um reticulado finito com base nos conceitos de elemento $\vee$-irredutível e elemento primo.

**Teorema 1.2.24** (cf. [6], Theorem 3, p. 94). *Num reticulado finito $R$, são equivalentes as seguintes condições:*

*(i) $R$ é distributivo;*

*(ii) qualquer elemento $\vee$-irredutível de $R$ é um elemento primo, ou seja, $\mathcal{S}(R) \subseteq \mathcal{P}(R)$;*

*(iii) para qualquer $x \in R$, $x = \bigvee \mathcal{P}(x)$;*

*(iv) para quaisquer $x, y \in R$ tais que $x \neq y$, $\mathcal{P}(x) \neq \mathcal{P}(y)$.*

*Demonstração.* Seja $R$ um reticulado finito.

Suponha-se que $R$ é distributivo. Pretende-se demonstrar que $\mathcal{S}(R) \subseteq \mathcal{P}(R)$. Seja $x \in \mathcal{S}(R)$. Então, $x \neq 0$. Tomem-se quaisquer $r, s \in R$ tais que $x \leq r \vee s$. Assim,

$$x = x \wedge (r \vee s) = (x \wedge r) \vee (x \wedge s),$$

graças à distributividade de $R$. Como $x$ é $\vee$-irredutível, então $x = x \wedge r$ ou $x = x \wedge s$, ou seja, $x \leq r$ ou $x \leq s$. Logo, $x \in \mathcal{P}(R)$.

Suponha-se, agora, que $\mathcal{S}(R) \subseteq \mathcal{P}(R)$. Pretende-se comprovar a veracidade da condição *(iii)*. Seja $x \in R$. Ora, pela hipótese, é muito simples perceber que $\mathcal{S}(x) \subseteq \mathcal{P}(x)$. Além disso, pela Proposição 0.3.50, tem-se $\mathcal{P}(x) \subseteq \mathcal{S}(x)$, donde $\mathcal{S}(x) = \mathcal{P}(x)$. Logo,

$$\bigvee \mathcal{S}(x) = \bigvee \mathcal{P}(x).$$

Mais, pelo Corolário 0.3.48, obtém-se

$$x = \bigvee \mathcal{S}(x) = \bigvee \mathcal{P}(x).$$

Portanto, $x = \bigvee \mathcal{P}(x)$.

É muito simples verificar que *(iii)* $\implies$ *(iv)*. De facto, para quaisquer $x, y \in R$, tem-se, por aplicação de *(iii)*, que

$$x \neq y \implies \bigvee \mathcal{P}(x) \neq \bigvee \mathcal{P}(y) \implies \mathcal{P}(x) \neq \mathcal{P}(y).$$

Suponha-se, agora, que *(iv)* é válida. Se $R$ é um reticulado trivial, é óbvio que $R$ é distributivo. Se $R$ não é trivial, então existem $x, y \in R$ tais que $\mathcal{P}(x) \neq \mathcal{P}(y)$. Portanto, $R$ tem elementos primos. Neste caso, seja $n \in \mathbb{N}$ o número máximo de elementos primos de $R$ incomparáveis dois a dois. Pelo Teorema 0.3.51, existem $n$ cadeias finitas $C_1, C_2, \ldots, C_n$ em $R$ e um homomorfismo de reticulados $\psi$ de $R$ no produto direto $\prod_{i=1}^{n} C_i$ tais que, para quaisquer $x, y \in R$,

$$\psi(x) = \psi(y) \iff \mathcal{P}(x) = \mathcal{P}(y).$$

Facilmente se conclui por *(iv)* que $\psi$ é um monomorfismo de $R$ em $\prod_{i=1}^{n} C_i$. Logo, $\psi$ é um isomorfismo de $R$ em $\psi(R)$, onde $\psi(R)$ é um sub-reticulado de $\prod_{i=1}^{n} C_i$, como estabelece a Proposição 0.3.8. Uma vez que toda a cadeia $C_i$ é um reticulado distributivo, o produto $\prod_{i=1}^{n} C_i$ é também um reticulado distributivo. Logo, $\psi(R)$ é um reticulado distributivo. Portanto, como $R \cong \psi(R)$, $R$ é um reticulado distributivo.

Fica, assim, concluída a prova do Teorema 1.2.24. □

Com tudo o que já foi estudado, recorrendo, sobretudo, aos Teoremas 0.3.51, 0.3.52 e 1.2.24, é possível concluir que um reticulado distributivo finito pode ser mergulhado num produto direto de cadeias finitas, isto é, é isomorfo a um sub-reticulado de um produto direto de cadeias finitas. No caso de um reticulado trivial, é óbvio que esta afirmação se verifica. Na situação de um reticulado não trivial, a veracidade da referida afirmação segue do teorema seguinte.

**Teorema 1.2.25** (cf. [6], p. 94)**.** *Sejam $R$ um reticulado distributivo finito e $n \in \mathbb{N}_0$ o número máximo de sucessores distintos de um qualquer elemento de $R$. Então, o número máximo de elementos $\vee$-irredutíveis de $R$ incomparáveis dois a dois é dado também por $n$ e, se $n \geq 1$, $R$ é isomorfo a algum sub-reticulado de algum produto direto de $n$ cadeias finitas.*

*Demonstração.* Sabe-se, pelo Teorema 0.3.52, que $m \leq n \leq p$, onde $m, p \in \mathbb{N}_0$ são, respetivamente, o número máximo de elementos primos de $R$ incomparáveis dois a dois e o número máximo de elementos $\vee$-irredutíveis de $R$ incomparáveis dois a dois. Além disso, como $R$ é um reticulado distributivo finito, então, pela Proposição 0.3.50 e por *(ii)* do Teorema 1.2.24, tem-se que as noções de elemento primo e de elemento $\vee$-irredutível são equivalentes em $R$, pelo que $m = p$. Logo, $n = m = p$, donde se conclui, em particular, que, de facto, $n$ também representa o número máximo de elementos $\vee$-irredutíveis de $R$ incomparáveis dois a dois.

Suponha-se que $n \geq 1$. Então, pelo Teorema 0.3.51, existem $n$ cadeias finitas $C_1, C_2, \ldots, C_n$ em $R$ e um homomorfismo de reticulados $\psi$ de $R$ em $\prod_{i=1}^{n} C_i$ tais que, para quaisquer $x, y \in R$,

$$\psi(x) = \psi(y) \iff \mathcal{P}(x) = \mathcal{P}(y).$$

Ora, pela Proposição 0.3.8, tem-se que $\psi(R)$ é um sub-reticulado de $\prod_{i=1}^{n} C_i$. Assim, considerando-se a aplicação $\varphi$ de $R$ em $\psi(R)$ definida por

$$\varphi(x) = \psi(x),$$

para qualquer $x \in R$, facilmente se verifica que $\varphi$ é um isomorfismo de reticulados: a sobrejetividade é óbvia; a injetividade também é imediata pela condição *(iv)* do Teorema 1.2.24. Portanto, $R$ é isomorfo ao sub-reticulado $\psi(R)$ do produto direto $\prod_{i=1}^{n} C_i$ de $n$ cadeias finitas em $R$. □

Segue-se, agora, um estudo sobre reticulados distributivos e algumas das suas propriedades envolvendo elementos complementados.

**Proposição 1.2.26** (cf. [2], Theorem 6.1, p. 78)**.** *Qualquer reticulado modular complementado é relativamente complementado.*

*Demonstração.* Sejam $(R; \wedge, \vee)$ um reticulado modular complementado, $r, s \in R$ tais que $r \leq s$ e $x \in [r, s]$. Como $R$ é um reticulado complementado, $x$ possui algum complemento, $y \in R$. Seja $z \in R$ o elemento de $R$ tal que

$$z = r \vee (s \wedge y).$$

Pela modularidade, também se tem

$$z = s \wedge (r \vee y).$$

Claramente, $r \leq z$ e $z \leq s$, pelo que $z \in [r, s]$. Então,

$$\begin{aligned}
x \wedge z &= x \wedge s \wedge (r \vee y) && [z = s \wedge (r \vee y)] \\
&= x \wedge (r \vee y) && [x \leq s] \\
&= r \vee (x \wedge y) && [r \leq x \text{ e modularidade}] \\
&= r \vee 0 && [y \text{ é um complemento de } x] \\
&= r
\end{aligned}$$

e

$$
\begin{aligned}
x \vee z &= x \vee r \vee (s \wedge y) && [z = r \vee (s \wedge y)] \\
&= x \vee (s \wedge y) && [r \leq x] \\
&= s \wedge (x \vee y) && [x \leq s \text{ e modularidade}] \\
&= s \wedge 1 && [y \text{ é um complemento de } x] \\
&= s.
\end{aligned}
$$

Logo, $z$ é um complemento relativo de $x$ em $[r, s]$. Portanto, o reticulado $R$ é relativamente complementado. □

**Corolário 1.2.27.** *Qualquer reticulado distributivo complementado é relativamente complementado.*

*Demonstração.* Imediato, tendo em conta as Proposições 1.1.5 e 1.2.26. □

**Teorema 1.2.28** (cf. [2], Theorem 6.2, p. 78)**.** *Sejam $R$ um reticulado distributivo (limitado) e $x \in R$. Caso existam, os complementos relativos (e os complementos) de $x$ são únicos.*

*Demonstração.* Sejam $(R; \wedge, \vee)$ um reticulado distributivo e $x \in R$. Admita-se que existem dois complementos relativos $y, z \in R$ de $x$ num intervalo $[r, s] \subseteq R$. Então,

$$y \wedge x = r = z \wedge x \quad \text{e} \quad y \vee x = s = z \vee x.$$

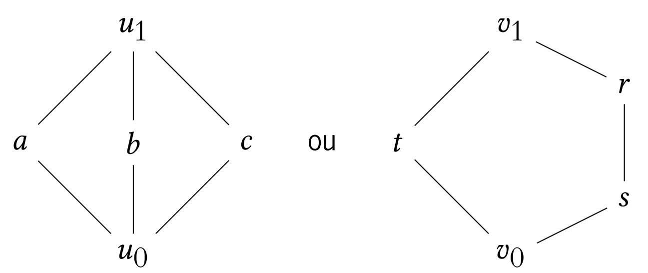
Logo, pelo Teorema 1.2.3, $y = z$. De forma semelhante se prova que, se $(R; \wedge, \vee)$ for um reticulado distributivo limitado e $x \in R$, então os complementos de $x$, caso existam, são únicos. Conclui-se assim a prova. □

**Teorema 1.2.29** (cf. [7], Corollary 103, p. 111)**.** *Um reticulado $R$ é distributivo se e só se qualquer elemento $x$ de $R$ tem, quando muito, um complemento relativo em qualquer intervalo que contenha $x$.*

*Demonstração.* Seja $(R; \wedge, \vee)$ um reticulado.

Se $R$ for distributivo, então, segundo o teorema anterior, cada $x \in R$ tem, quando muito, um complemento relativo em qualquer intervalo, em particular em qualquer intervalo que contenha $x$.

Reciprocamente, se $R$ não for distributivo, então $R$ possui algum sub-reticulado isomorfo a $M_3$ ou a $N_5$, ou seja, $R$ possui algum sub-reticulado da forma



Como facilmente se nota, em ambos os casos, existem elementos com mais do que um complemento relativo: no primeiro caso, os elementos $b \neq c$ são complementos relativos de $a$ no intervalo $[u_0, u_1]$; no caso restante, os elementos $r \neq s$ são complementos relativos de $t$ no intervalo $[v_0, v_1]$.

Fica concluída a prova. $\square$

# 2 Álgebras de Boole

Este último capítulo da dissertação é dedicado ao estudo de uma das mais conhecidas classes de álgebras que admitem como reduto algum reticulado distributivo: as álgebras de Boole. Estudam-se propriedades básicas deste tipo de álgebras e estabelecem-se teoremas de caracterização e de representação para álgebras de Boole.

## 2.1 Noções e propriedades principais

Na secção 0.3 introduziu-se o conceito de elemento complementado em reticulados limitados. O complemento de um elemento, caso exista, não é, em geral, único. Num reticulado distributivo limitado, sabe-se, no entanto, pelo Teorema 1.2.28, que cada elemento complementado admite um único complemento. É o que motiva o estudo da classe de reticulados a seguir definidos.

**Definição 2.1.1.** Chama-se *reticulado de Boole* a qualquer reticulado distributivo complementado.

Pela definição anterior, sendo $(R; \wedge, \vee)$ um reticulado de Boole, é simples concluir que

- $R$ é um reticulado limitado;
- cada elemento $x$ de $R$ admite um único complemento, que habitualmente se denota por $x'$.

O elemento mínimo de um reticulado de Boole $(R; \wedge, \vee)$ é representado por $0_R$ (ou apenas por $0$, caso não haja ambiguidade) e o elemento máximo é representado por $1_R$ (ou apenas por $1$).

Considerando que, num reticulado de Boole $R$, cada elemento admite um único complemento, pode definir-se uma operação unária em $R$, denominada *complementação*, que, a cada elemento $x \in R$, faz corresponder o seu único complemento $x'$. Esta operação é usualmente representada por $'$.

**Definição 2.1.2.** Chama-se *álgebra de Boole* a qualquer álgebra $(B; \wedge, \vee, ')$ de tipo $(2, 2, 1)$ onde

- $(B; \wedge, \vee)$ é um reticulado de Boole;
- a operação unária $'$ é a operação de complementação em $B$.

Portanto, dada uma álgebra de Boole $(B; \wedge, \vee, ')$, a álgebra $(B; \wedge, \vee)$ é um seu reduto que é um reticulado distributivo.

Para simplificar a escrita, é usual representar uma álgebra de Boole $(B; \wedge, \vee, ')$ apenas por $B$, caso não haja ambiguidade.

**Exemplo 2.1.3.** Sendo $X$ um conjunto qualquer, a álgebra $(\wp(X); \cap, \cup, ')$, onde $'$ é a operação unária em $\wp(X)$ definida por

$$Y' = X \setminus Y,$$

para qualquer $Y \in \wp(X)$, é uma álgebra de Boole.

Eis algumas das principais propriedades da operação de complementação numa álgebra de Boole.

**Lema 2.1.4** (cf. [2], Theorem 6.7, p. 82; [3], Lemma 1.2, pp. 130–131; [4], Secção 4.15, pp. 93–94; [9], Theorem 5.1, pp. 129–130)**.** *Seja $(B; \wedge, \vee, ')$ uma álgebra de Boole. Então,*

*(i)* $0' = 1$ *e* $1' = 0$*;*

*(ii) para qualquer $x \in B$, $x'' = x$;*

*(iii) para quaisquer $x, y \in B$, se $x \wedge y = 0$ e $x \vee y = 1$, então $x = y'$;*

*(iv) para quaisquer $x, y \in B$,*

$$(x \wedge y)' = x' \vee y' \quad e \quad (x \vee y)' = x' \wedge y';$$

*(v) para quaisquer $x, y \in B$,*

$$x \wedge y = \left(x' \vee y'\right)' \quad e \quad x \vee y = \left(x' \wedge y'\right)';$$

*(vi) para quaisquer $x, y \in B$,*

$$x \leq y \iff y' \leq x' \iff x \wedge y' = 0 \iff x' \vee y = 1;$$

*(vii) para quaisquer $x, y, z \in B$,*

$$x \wedge y \leq z \iff x \leq z \vee y' \quad e \quad z \leq x \vee y \iff z \wedge y' \leq x.$$

*Demonstração.* As condições *(i)* e *(ii)* são imediatas.

(iii) Sejam $x, y \in B$ tais que $x \wedge y = 0$ e $x \vee y = 1$. Então,

$$\begin{aligned} x &= x \wedge 1 \\ &= x \wedge (y \vee y') \\ &= (x \wedge y) \vee (x \wedge y') \\ &= 0 \vee (x \wedge y') \\ &= x \wedge y', \end{aligned}$$

pelo que $x \leq y'$. De forma semelhante se prova que $y' \leq x$. Logo, $x = y'$.

(iv) Sejam $x, y \in B$. Então, $x' \vee y' \in B$. Para provar que

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

basta mostrar que

$$(x \wedge y) \wedge \left(x' \vee y'\right) = 0 \quad e \quad (x \wedge y) \vee \left(x' \vee y'\right) = 1.$$

Ora,

$$\begin{aligned} (x \wedge y) \wedge \left(x' \vee y'\right) &= \left(x \wedge y \wedge x'\right) \vee \left(x \wedge y \wedge y'\right) \\ &= (y \wedge 0) \vee (x \wedge 0) \\ &= 0 \vee 0 \\ &= 0. \end{aligned}$$

Analogamente, se mostra que $(x \wedge y) \vee \left(x' \vee y'\right) = 1$. Logo, $(x \wedge y)' = x' \vee y'$. Procedendo de forma semelhante, também se prova que $(x \vee y)' = x' \wedge y'$.

(v) Sejam $x, y \in B$. Por *(ii)* e *(iv)*, obtém-se

$$x \wedge y = (x \wedge y)'' = \left(x' \vee y'\right)'$$

e

$$x \vee y = (x \vee y)'' = \left(x' \wedge y'\right)'.$$

(vi) Sejam $x, y \in B$.

Suponha-se, primeiramente, que $x \leq y$. Então, $x = x \wedge y$. Assim, por *(iv)*,

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

Logo, $y' \leq x'$.

Admita-se, agora, que $y' \leq x'$. Então,

$$x \wedge y' \leq x \wedge x' = 0.$$

Logo, $x \wedge y' = 0$.

Seguidamente, se $x \wedge y' = 0$, então

$$\left(x \wedge y'\right)' = 0',$$

donde, por *(iv)*, *(i)* e *(ii)*,

$$x' \vee y = 1.$$

Assuma-se, agora, que $x' \vee y = 1$. Então,

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

pelo que

$$\left(x \wedge x'\right) \vee (x \wedge y) = x,$$

ou seja,

$$0 \vee (x \wedge y) = x,$$

donde

$$x \wedge y = x.$$

Logo, $x \leq y$.

(vii) Sejam $x, y, z \in B$. Ora,

$$\begin{aligned} x \wedge y \leq z &\implies (x \wedge y) \vee y' \leq z \vee y' \\ &\implies \left(x \vee y'\right) \wedge \left(y \vee y'\right) \leq z \vee y' \\ &\implies \left(x \vee y'\right) \wedge 1 \leq z \vee y' \\ &\implies x \vee y' \leq z \vee y' \\ &\implies x \leq z \vee y'. \qquad \text{[uma vez que } x \leq x \vee y'\text{]} \end{aligned}$$

De forma semelhante se prova que

$$x \leq z \vee y' \implies x \wedge y \leq z.$$

Logo,

$$x \wedge y \leq z \iff x \leq z \vee y'.$$

Argumentos semelhantes provam que

$$z \leq x \vee y \iff z \wedge y' \leq x.$$

Conclui-se assim a demonstração do Lema 2.1.4. □

As condições da alínea *(iv)* do Lema 2.1.4 são conhecidas como *leis de De Morgan*.

Os conceitos que se seguem não são mais do que especificações dos que já foram estudados na Secção 0.2.

**Definição 2.1.5.** Sejam $(B; \wedge, \vee, ')$ uma álgebra de Boole e $A \subseteq B$. Uma álgebra $(A; \wedge, \vee, ')$, onde as operações $\wedge$, $\vee$, $'$ são as mesmas que as respetivas operações de $B$ restritas a $A$, diz-se uma *subálgebra de* $(B; \wedge, \vee, ')$ se

- $(A; \wedge, \vee)$ é um sub-reticulado de $(B; \wedge, \vee)$;
- para qualquer $x \in A$, $x' \in A$.

**Definição 2.1.6.** Sejam $(B; \wedge^B, \vee^B, ')$ e $(C; \wedge^C, \vee^C, ^*)$ álgebras de Boole e $f$ uma aplicação de $B$ em $C$. Diz-se que $f$ é um *homomorfismo de álgebras de Boole* se

- $f$ preserva ínfimos e supremos: para quaisquer $x, y \in B$,

$$f(x \wedge^B y) = f(x) \wedge^C f(y)$$
$$f(x \vee^B y) = f(x) \vee^C f(y);$$

- $f$ preserva complementos: para qualquer $x \in B$,

$$f(x') = (f(x))^*.$$

Tendo em conta a definição anterior e o que já foi estudado na Secção 0.2, é simples entender como se definem os termos *monomorfismo/ epimorfismo/ isomorfismo de álgebras de Boole*.

No lema seguinte, encontram-se algumas propriedades destes homomorfismos, que mostram que as condições da Definição 2.1.6 não são independentes entre si.

**Lema 2.1.7** (cf. [4], Secção 4.17)**.** *Sejam $(B; \wedge^B, \vee^B, ')$ e $(C; \wedge^C, \vee^C, ^*)$ álgebras de Boole e $f$ uma aplicação de $B$ em $C$.*

*(i) Se $f$ preserva ínfimos e supremos, então as seguintes condições são equivalentes:*

*(a) $f$ preserva complementos;*

*(b) $f$ preserva mínimos e máximos:*

$$f(0_B) = 0_C \quad e \quad f(1_B) = 1_C.$$

*(ii) Se $f$ preserva complementos, então $f$ preserva ínfimos se e só se $f$ preserva supremos.*

*Demonstração.* (i) Suponha-se que $f$ preserva ínfimos e supremos.

Primeiramente, se *(a)* for válida, então

$$\begin{aligned} f(0_B) &= f(0_B \wedge^B 0_B{}') \\ &= f(0_B) \wedge^C f(0_B{}') && \text{[hipótese]} \\ &= f(0_B) \wedge^C (f(0_B))^* && \text{[(a)]} \\ &= 0_C. \end{aligned}$$

Dualmente se prova que $f(1_B) = 1_C$.

Inversamente, suponha-se que se verifica *(b)*. Seja $x \in B$. Uma vez que $f(x') \in C$, para concluir que $f(x') = (f(x))^*$, basta mostrar que

$$f(x') \wedge^C f(x) = 0_C \quad \text{e} \quad f(x') \vee^C f(x) = 1_C.$$

Ora,

$$\begin{aligned} f(x') \vee^C f(x) &= f(x' \vee^B x) && \text{[hipótese]} \\ &= f(1_B) \\ &= 1_C. && \text{[(b)]} \end{aligned}$$

Por dualidade, tem-se $f(x') \wedge^C f(x) = 0_C$.

(ii) Admita-se que $f$ preserva complementos e ínfimos. Então, para quaisquer $x, y \in B$,

$$\begin{aligned} f(x \vee^B y) &= f((x' \wedge^B y')') && \text{[Lema 2.1.4 (v)]} \\ &= (f(x' \wedge^B y'))^* && \text{[$f$ preserva complementos]} \\ &= (f(x') \wedge^C f(y'))^* && \text{[$f$ preserva ínfimos]} \\ &= ((f(x))^* \wedge^C (f(y))^*)^* && \text{[$f$ preserva complementos]} \\ &= f(x) \vee^C f(y). && \text{[Lema 2.1.4 (v)]} \end{aligned}$$

Portanto, $f$ também preserva supremos.

Analogamente se prova que, se $f$ preserva complementos e supremos, então também preserva ínfimos. □

**Proposição 2.1.8.** *(i) Qualquer subálgebra de uma álgebra de Boole é uma álgebra de Boole.*

*(ii) Qualquer imagem homomorfa de uma álgebra de Boole é uma álgebra de Boole.*

*Demonstração.* *(i)* Seja $(B; \wedge, \vee, ')$ uma álgebra de Boole e $(S; \wedge, \vee, ')$ uma sua subálgebra.

Uma vez que $(B; \wedge, \vee)$ é um reticulado distributivo, e $(S; \wedge, \vee)$ é um sub-reticulado de $(B; \wedge, \vee)$, então $(S; \wedge, \vee)$ é um reticulado distributivo.

O reticulado $(S; \wedge, \vee)$ é limitado. De facto, como $S \neq \emptyset$, existe $x \in S$. Como $S$ é fechado para as operações $\wedge$, $\vee$ e $'$, segue que $0_B = x \wedge x' \in S$ e $1_B = x \vee x' \in S$.

Como $0_B, 1_B \in S$ e $S$ é fechado para a operação $'$, claramente, cada elemento de $S$ é complementado em $S$.

Logo, $(S; \wedge, \vee, ')$ é uma álgebra de Boole.

*(ii)* Sejam $(B; \wedge^B, \vee^B, ')$ uma álgebra de Boole e $(H; \wedge^H, \vee^H, ^*)$ uma sua imagem homomorfa. Então, $H = \varphi(B)$, para algum epimorfismo $\varphi$ de $(B; \wedge^B, \vee^B, ')$ em $(H; \wedge^H, \vee^H, ^*)$.

Pretende-se, primeiramente, mostrar que $(H; \wedge^H, \vee^H)$ é um reticulado de Boole.

Como $(B; \wedge^B, \vee^B)$ é um reticulado distributivo, então, por *(iii)* da Proposição 1.1.6, também $(H; \wedge^H, \vee^H)$ é um reticulado distributivo.

Prove-se que o reticulado $(H; \wedge^H, \vee^H)$ é limitado. Para tal, mostre-se que $\varphi(0_B)$ e $\varphi(1_B)$ são, respetivamente, o elemento mínimo e máximo de $H$. Seja $x \in H$. Então, $x = \varphi(y)$, para certo $y \in B$. Ora,

$$\begin{aligned} x \wedge^H \varphi(0_B) &= \varphi(y) \wedge^H \varphi(0_B) \\ &= \varphi(y \wedge^B 0_B) && [\varphi \text{ é um homomorfismo}] \\ &= \varphi(0_B). \end{aligned}$$

Analogamente se mostra que

$$x \vee^H \varphi(1_B) = \varphi(1_B).$$

Logo, $\varphi(0_B) = 0_H$ e $\varphi(1_B) = 1_H$.

Prove-se, agora, que $(H; \wedge^H, \vee^H)$ é um reticulado complementado. Seja $x \in H$. Então, tem-se $x = \varphi(y)$, para certo $y \in B$. Mostre-se que $\varphi(y')$ é o complemento de $x$ em $H$. Claramente, $\varphi(y') \in H$. Além disso,

$$\begin{aligned} x \wedge^H \varphi(y') &= \varphi(y) \wedge^H \varphi(y') \\ &= \varphi(y \wedge^B y') && [\varphi \text{ é um homomorfismo}] \\ &= \varphi(0_B) \\ &= 0_H. \end{aligned}$$

Analogamente se mostra que $x \vee^H \varphi(y') = 1_H$.

Portanto, $(H; \wedge^H, \vee^H)$ é um reticulado de Boole.

Falta demonstrar que $^*$ é a operação de complementação em $H$, ou seja, mostrar que, para cada $x \in H$, $x^*$ é o complemento de $x$ em $H$. Seja $x \in H$. Então, como $\varphi$ é um epimorfismo $\varphi$ de $(B; \wedge^B, \vee^B, ')$ em $(H; \wedge^H, \vee^H, ^*)$, $x = \varphi(y)$, para certo $y \in B$. Assim,

$$\begin{aligned}
x \wedge^H x^* &= \varphi(y) \wedge^H (\varphi(y))^* \\
&= \varphi(y) \wedge^H \varphi(y') & [\varphi : (B; \wedge^B, \vee^B, ') \to (H; \wedge^H, \vee^H, ^*)] \\
&= \varphi(y \wedge^B y') & [\varphi : (B; \wedge^B, \vee^B, ') \to (H; \wedge^H, \vee^H, ^*)] \\
&= \varphi(0_B) \\
&= 0_H.
\end{aligned}$$

Analogamente se prova que $x \vee^H x^* = 1_H$.

Termina, assim, a demonstração. □

As demonstrações dos seguintes dois resultados podem ser consultadas em [2], pp. 82–83.

**Teorema 2.1.9** (cf. [2], Theorem 6.8, p. 82)**.** *Seja $(B; \wedge, \vee, ')$ uma álgebra de Boole tal que $(B; \wedge, \vee)$ é um reticulado completo. Então, para qualquer $x \in B$ e para qualquer família $(y_i)_{i \in I}$ de elementos de $B$, onde $I$ é um conjunto, tem-se*

$$x \wedge \bigvee_{i \in I} y_i = \bigvee_{i \in I} (x \wedge y_i) \quad e \quad x \vee \bigwedge_{i \in I} y_i = \bigwedge_{i \in I} (x \vee y_i).$$

**Corolário 2.1.10** (cf. [2], Corollary, p. 83)**.** *Seja $(B; \wedge, \vee, ')$ uma álgebra de Boole tal que $(B; \wedge, \vee)$ é um reticulado completo. Então, para qualquer família $(x_i)_{i \in I}$ de elementos de $B$, onde $I$ é um conjunto, tem-se*

$$\left(\bigwedge_{i \in I} x_i\right)' = \bigvee_{i \in I} x_i' \quad e \quad \left(\bigvee_{i \in I} x_i\right)' = \bigwedge_{i \in I} x_i'.$$

## 2.2 Teoremas de caraterização e de representação

Nesta secção, são estabelecidos resultados que fornecem formas de caraterizar e/ou representar álgebras de Boole.

Pelo Teorema 1.2.11, sabe-se que um reticulado é distributivo se e só se é isomorfo a um anel de conjuntos. No caso das álgebras de Boole, obtém-se uma caraterização semelhante, estabelecida no Teorema 2.2.2. Para tal, introduz-se, primeiramente, a definição de corpo de conjuntos.

**Definição 2.2.1.** Dá-se a designação de *corpo de conjuntos* a qualquer subálgebra de uma álgebra de Boole $(\wp(X); \cap, \cup, ')$, para algum conjunto $X$.

**Teorema 2.2.2** (cf. [2], Theorem 6.11, p. 86). *Qualquer álgebra* $(B; \wedge, \vee, ^*)$ *de tipo* $(2,2,1)$ *é uma álgebra de Boole se e só se* $B$ *é isomorfa a algum corpo de conjuntos.*

*Demonstração.* Seja $(B; \wedge, \vee, ^*)$ uma álgebra de tipo $(2,2,1)$.

Suponha-se, primeiramente, que $B$ é isomorfa a algum corpo de conjuntos, isto é, $B$ é isomorfa a alguma subálgebra $(\mathcal{C}; \cap, \cup, ')$ de uma álgebra de Boole $(\wp(X); \cap, \cup, ')$, para algum conjunto $X$. Então, por *(i)* da Proposição 2.1.8, $(\mathcal{C}; \cap, \cup, ')$ é também uma álgebra de Boole. Logo, $B$ é imagem homomorfa de uma álgebra de Boole, donde, por *(ii)* da mesma proposição, se chega à conclusão de que $B$ é uma álgebra de Boole.

Suponha-se, agora, que $(B; \wedge, \vee, ^*)$ é uma álgebra de Boole. Para cada $x \in B$, defina-se

$$\mathcal{I}(x) = \{P \in \mathrm{Esp}(B) \mid x \notin P\},$$

onde $\mathrm{Esp}(B)$ é o conjunto dos ideais primos do reticulado $(B; \wedge, \vee)$. Considere-se o conjunto

$$\mathcal{I} = \{\mathcal{I}(x) \mid x \in B\}$$

e sejam $\cap$, $\cup$, $'$ as operações usuais de interseção, união e de complementação em $\wp(\mathrm{Esp}(B))$. O objetivo é mostrar que $(\mathcal{I}; \cap, \cup, ')$ é subálgebra de $(\wp(\mathrm{Esp}(B)); \cap, \cup, ')$. Na demonstração do Teorema 1.2.11, já foi provado que $(\mathcal{I}; \cap, \cup)$ é uma subálgebra de $(\wp(\mathrm{Esp}(B)), \cap, \cup)$ e, portanto, é um anel de conjuntos. Assim, para provar que $(\mathcal{I}, \cap, \cup, ')$ é um corpo de conjuntos, resta provar que $\mathcal{I}$ é fechado para a operação de complementação de $(\wp(\mathrm{Esp}(B)), \cap, \cup, ')$. Para tal, falta ver que, para cada $x \in B$, $(\mathcal{I}(x))' = \mathrm{Esp}(B) \setminus \mathcal{I}(x) \in \mathcal{I}$. Mostre-se que, para cada $x \in B$, se tem

$$(\mathcal{I}(x))' = \mathcal{I}(x^*),$$

isto é,

$$\mathrm{Esp}(B) \setminus \mathcal{I}(x) = \mathcal{I}(x^*).$$

Ora, se $J \in \mathrm{Esp}(B) \setminus \mathcal{I}(x)$, então $x \in J$. Sendo $J$ um ideal primo de $B$, segue que $x^* \notin J$. De facto, se $x^* \in J$, então

$$1_B = x \vee x^* \in J,$$

pelo que, para qualquer $y \in B$, $y \in J$, donde $J = B$, o que é absurdo. Logo, $J \in \mathcal{I}(x^*)$. Reciprocamente, se $J \in \mathcal{I}(x^*)$, então $J \in \mathrm{Esp}(B)$ e $x^* \notin J$. Como $J$ é um ideal primo e $x \wedge x^* = 0_B \in J$, então $x \in J$; consequentemente, $J \in \mathrm{Esp}(B) \setminus \mathcal{I}(x)$. Para cada $x \in B$, $x^* \in B$, e, portanto,

$$\mathrm{Esp}(B) \setminus \mathcal{I}(x) = \mathcal{I}(x^*) \in \mathcal{I}.$$

Portanto, $(\mathcal{I}, \cap, \cup, ')$ é um corpo de conjuntos.

Na demonstração do Teorema 1.2.11, também já foi provado que a aplicação $\varphi$ de $B$ em $\mathcal{I}$ definida por

$$\varphi(x) = \mathcal{I}(x),\ \forall\, x \in B,$$

é um isomorfismo de reticulados de $(B, \wedge, \vee)$ em $(\mathcal{I}, \cap, \cup)$, ou seja, $\varphi$ preserva ínfimos e supremos. Verifique-se que $\varphi$ também preserva complementos. Com efeito, foi mostrado anteriormente que, para qualquer $x \in B$,

$$\mathcal{I}(x^*) = (\mathcal{I}(x))',$$

pelo que,

$$\varphi(x^*) = (\varphi(x))'.$$

Portanto, a aplicação $\varphi$ é um isomorfismo de $(B; \wedge, \vee, {}^*)$ em $(\mathcal{I}, \cap, \cup, ')$. □

Pelo teorema anterior, sabe-se que toda a álgebra de Boole é isomorfa a algum corpo de conjuntos, isto é, a uma subálgebra de uma álgebra de Boole $(\wp(X); \cap, \cup, ')$, sendo $X$ um conjunto. Contudo, uma álgebra de Boole nem sempre é isomorfa a uma álgebra de Boole $(\wp(X); \cap, \cup, ')$, para algum conjunto $X$. Por exemplo, uma álgebra de Boole que não seja completa não pode ser isomorfa a uma álgebra de Boole $(\wp(X); \cap, \cup, ')$, onde $X$ seja um conjunto, visto esta última ser completa. Por isso, o objetivo do que se segue é estabelecer condições que auxiliem na identificação das álgebras de Boole que sejam isomorfas a alguma álgebra de Boole $(\wp(X); \cap, \cup, ')$, para algum conjunto $X$.

**Teorema 2.2.3** (cf. [2], Theorem 6.12, pp. 86–87)**.** *Seja $(B; \wedge, \vee, {}^*)$ uma álgebra de Boole. Então, as seguintes condições são equivalentes:*

*(i)* $(B; \wedge, \vee, {}^*) \cong (\wp(X); \cap, \cup, ')$, *para algum conjunto* $X$*;*

*(ii)* $(B; \wedge, \vee)$ *é um reticulado completo e atómico.*

*Demonstração.* Suponha-se, primeiramente, que $(B; \wedge, \vee, {}^*) \cong (\wp(X); \cap, \cup, ')$, para algum conjunto $X$. É claro que $(\wp(X); \cap, \cup)$ é um reticulado completo e, pelo Exemplo 0.3.43, também é atómico. Portanto, $(B; \wedge, \vee)$ é também um reticulado completo e atómico.

Admita-se, agora, que $(B; \wedge, \vee)$ é um reticulado completo e atómico.

Seja $\mathrm{At}(B)$ o conjunto de átomos do reticulado $(B; \wedge, \vee)$. Dado $x \in B$ tal que $x \neq 0$, seja

$$X = \mathrm{at}(x) = \{y \in \mathrm{At}(B) \mid y \leq x\}$$

e $z = \bigvee X$ (é garantido que $\bigvee X$ existe, visto que o reticulado $B$ é completo). É claro que $z \leq x$. Prove-se que, na verdade, $z = x$. Por absurdo, suponha-se que $z < x$. Como $(B; \wedge, \vee)$ é um reticulado distributivo complementado, então, pela Proposição 1.2.26, $B$ é um reticulado relativamente complementado. Assim, o intervalo $[0, x]$ de $B$ é complementado, pelo que $z$ possui um complemento relativo nesse intervalo, ou seja, existe $w \in [0, x]$ tal que $w \neq 0$ que satisfaz $x = z \vee w$ e $z \wedge w = 0$. Como $(B; \wedge, \vee)$ é um reticulado atómico, existe $a \in \mathrm{At}(B)$ tal que $a \leq w$. Assim, $a \leq z \vee w = x$. Logo, $a \in X$, pelo que $a \leq z$, donde $a \leq z \wedge w = 0$, o que é uma contradição. Portanto, $x = \bigvee X$.

Definam-se as aplicações $\varphi : B \longrightarrow \wp(\mathrm{At}(B))$ por

$$\varphi(x) = \begin{cases} \mathrm{at}(x), & \text{se } x \neq 0; \\ \emptyset, & \text{caso contrário;} \end{cases}$$

e $\psi : \wp(\mathrm{At}(B)) \longrightarrow B$ por

$$\psi(X) = \begin{cases} \bigvee X, & \text{se } X \neq \emptyset; \\ 0, & \text{caso contrário.} \end{cases}$$

O objetivo é provar que $\psi$ é um isomorfismo de álgebras de Boole de $(\wp(\mathrm{At}(B)); \cap, \cup, ')$ em $(B; \wedge, \vee, ^*)$.

Comece-se por mostrar que $\psi$ é uma aplicação bijetiva. Não é difícil verificar que $\psi \circ \varphi = \iota_B$. Ora, claramente, $(\psi \circ \varphi)(0) = 0$. Mais, para qualquer $x \in B$ tal que $x \neq 0$,

$$\begin{aligned} (\psi \circ \varphi)(x) &= \psi(\varphi(x)) \\ &= \psi(\mathrm{at}(x)) && [x \neq 0] \\ &= \bigvee \mathrm{at}(x) && [\mathrm{at}(x) \neq \emptyset, \text{ uma vez que } B \text{ é atómico e } x \in B \setminus \{0\}] \\ &= x && [\text{pelo que foi provado anteriormente}] \\ &= \iota_B(x). \end{aligned}$$

De facto, verifica-se que $\psi \circ \varphi = \iota_B$, donde se conclui que a aplicação $\psi$ é sobrejetiva. Prove-se, agora, que a aplicação $\psi$ é injetiva. Sejam $X, Y \in \wp(\mathrm{At}(B))$ tais que $\psi(X) = \psi(Y)$. Se $\psi(X) = \psi(Y) = 0$, então $X = \emptyset = Y$. Se $\psi(X) \neq 0$ e $\psi(Y) \neq 0$, então $\bigvee X = \bigvee Y$. Seja $y \in Y$. Então, $y \leq \bigvee Y = \bigvee X$. Por conseguinte,

$$\begin{aligned} y &= y \wedge \bigvee X \\ &= \bigvee (y \wedge X), && [\text{Teorema 2.1.9}] \end{aligned}$$

onde $y \wedge X = \{y \wedge x \mid x \in X\}$. Como $y \in \mathrm{At}(B)$, existe $x \in X$ tal que $0 < y \wedge x \leq y$. De facto, se tivéssemos $y \wedge x = 0$, para qualquer $x \in X$, então $y \wedge X = \{0\}$, pelo que

$$y = \bigvee \{0\} = 0,$$

o que não é possível visto que $y$ é um átomo de $B$. Como $0 \prec y$, então $y \wedge x = y$, donde $y \leq x$. Como $x \in X \subseteq \mathrm{At}(B)$, $0 \prec x$, pelo que $y = x \in X$. Logo, $Y \subseteq X$. Analogamente se obtém $X \subseteq Y$. Portanto, $X = Y$, donde se conclui que $\psi$ é injetiva, sendo, por isso, bijetiva. Uma vez que $\psi$ é bijetiva, então $\psi$ é invertível. Uma vez que $\psi \circ \varphi = \iota_B$, tem-se $\psi^{-1} = \varphi$.

Mostre-se, agora, que $\psi$ é isótona. Sejam $X, Y \in \wp(\mathrm{At}(B))$ tais que $X \subseteq Y$. Se $X = Y = \emptyset$, então

$$\psi(X) = 0 = \psi(Y),$$

pelo que $\psi(X) \leq \psi(Y)$. Se $X = \emptyset$ e $Y \neq \emptyset$, então

$$\psi(X) = 0 \leq \bigvee Y = \psi(Y).$$

Se $X \neq \emptyset$ e $Y \neq \emptyset$, então, como $\bigvee X \leq \bigvee Y$, tem-se $\psi(X) \leq \psi(Y)$. Confirma-se, assim, que $\psi$ é isótona.

Prove-se que $\varphi$ também é isótona. Sejam $x, y \in B$ tais que $x \leq y$. Ora, se $x = y = 0$, então

$$\varphi(x) = \emptyset = \varphi(y),$$

pelo que $\varphi(x) \subseteq \varphi(y)$. Se $x = 0$ e $y \neq 0$, então

$$\varphi(x) = \emptyset \subseteq \mathrm{at}(y) = \varphi(y).$$

Se $x \neq 0$ e $y \neq 0$, então

$$\varphi(x) = \mathrm{at}(x) \subseteq \mathrm{at}(y) = \varphi(y).$$

Portanto, $\varphi$ é, de facto, isótona.

Como $\psi$ é isótona, invertível e a sua inversa, $\varphi$, é também isótona, conclui-se, atendendo às Proposições 0.1.24 e 0.3.6, que $\psi$ é um isomorfismo de reticulados de $(B; \wedge, \vee)$ em $(\wp(\mathrm{At}(B)); \cap, \cup)$.

Verifique-se, agora, que $\psi$ preserva complementos. Seja $X \in \wp(\mathrm{At}(B))$. Para provar que

$$\psi(X') = (\psi(X))^*,$$

basta mostrar que $\psi(X') \in B$ (o que é óbvio) e que

$$\psi(X) \wedge \psi(X') = 0 \quad \text{e} \quad \psi(X) \vee \psi(X') = 1.$$

Ora,

$$\begin{aligned}
\psi(X) \wedge \psi(X') &= \psi(X \cap (\mathrm{At}(B) \setminus X)) \\
&= \psi(\emptyset) \\
&= 0
\end{aligned}$$

e

$$\begin{aligned}
\psi(X) \vee \psi(X') &= \psi(X \cup (\mathrm{At}(B) \setminus X)) \\
&= \psi(\mathrm{At}(B)) \\
&= \bigvee \mathrm{At}(B) \\
&= 1.
\end{aligned}$$

Verifique-se que, de facto, $\bigvee \mathrm{At}(B) = 1$. Para tal, suponha-se, por absurdo, que existe um majorante $z$ de $\mathrm{At}(B)$ tal que $z < 1$. Como $(B; \wedge, \vee)$ é um reticulado atómico, então existe $a \in \mathrm{At}(B)$ tal que $a \leq z^*$. Assim, $0 < a \leq z \wedge z^*$, o que é um absurdo.

Portanto, $\psi$ é um isomorfismo de álgebras de Boole, pelo que

$$(B; \wedge, \vee, {}^*) \cong (\wp(\mathrm{At}(B)); \cap, \cup, {}').$$

Fica, assim, concluída a demonstração. □

**Corolário 2.2.4** (cf. [2], Corollary, pp. 87–88)**.** *Seja $(B; \wedge, \vee, {}^*)$ uma álgebra de Boole finita. Então, $B$ tem $2^n$ elementos, onde $n \in \mathbb{N}$ é o número de átomos de $B$.*

*Demonstração.* É simples notar que $(B; \wedge, \vee)$ é um reticulado completo e atómico. Logo, pelo teorema anterior, $(B; \wedge, \vee, {}^*) \cong (\wp(X); \cap, \cup, {}')$, para algum conjunto $X$. Uma vez que $B$ é finito, $X$ é finito. Assuma-se, sem perda de generalidade, que $X = \{x_1, \ldots, x_n\}$, para certo $n \in \mathbb{N}$. Denote-se por $\mathbf{2}$ a cadeia de dois elementos $\{0, 1\}$ e considere-se a aplicação $f : \wp(X) \to \mathbf{2}^n$ definida por

$$f(Y) = (y_1, \ldots, y_n),$$

onde, para cada $i \in \{1, \ldots, n\}$,

$$y_i = \begin{cases} 1, & \text{se } x_i \in Y; \\ 0, & \text{caso contrário.} \end{cases}$$

É óbvio que $f$ está bem definida.

Suponha-se que a aplicação $f$ é bijetiva. Então o conjunto $\wp(X)$ tem o mesmo número de elementos que o conjunto $\mathbf{2}^n$, tendo este último $2^n$ elementos. Sabe-se que $X$ tem $n$ elementos, o que significa que $\wp(X)$ possui exatamente $n$ conjuntos singulares, os quais correspondem aos átomos de $(\wp(X); \cap, \cup)$. Logo, como $B \cong \wp(X)$, conclui-se que $B$ possui $2^n$ elementos, sendo $n$ o número de átomos de $B$.

Resta, portanto, provar que $f$ é uma aplicação bijetiva.

Inicialmente, mostre-se que $f$ é injetiva. Para tal, verifique-se que, para quaisquer $Y, Z \in \wp(X)$,

$$Y \subseteq Z \iff f(Y) \sqsubseteq f(Z).$$

Sejam $Y, Z \in \wp(X)$. Então,

$$f(Y) = (y_1, \ldots, y_n) \quad \text{e} \quad f(Z) = (z_1, \ldots, z_n),$$

para certos $(y_1, \ldots, y_n), (z_1, \ldots, z_n) \in \mathbf{2}^n$. Tem-se $Y \subseteq Z$ se e só se, para cada $i \in \{1, \ldots, n\}$, $x_i \in Y$ implica $x_i \in Z$; ou seja, $Y \subseteq Z$ se e só se, para cada $i \in \{1, \ldots, n\}$, $y_i = 1$ implica $z_i = 1$. Assim, $Y \subseteq Z$ se e só se

$$f(Y) = (y_1, \ldots, y_n) \sqsubseteq (z_1, \ldots, z_n) = f(Z).$$

Logo, $f$ é um mergulho de ordem de $(\wp(X); \subseteq)$ em $(\mathbf{2}^n; \sqsubseteq)$ e, portanto, $f$ é injetiva.

Mostre-se, agora, que $f$ é sobrejetiva. Seja $w = (w_1, \ldots, w_n) \in \mathbf{2}^n$. Considerando

$$W = \{x_i \in X \mid i \in \{1, \ldots, n\}, w_i = 1\},$$

tem-se claramente que

$$f(W) = w.$$

Portanto, $f$ é sobrejetiva.

Conclui-se assim o que era pretendido. □

# Bibliografia


[1] Balbes, R. & Dwinger, P. (1974). *Distributive lattices*. University of Missouri Press.

[2] Blyth, T. S. (2005). *Lattices and ordered algebraic structures*. Springer-Verlag London.

[3] Burris, S. & Sankappanavar, H. P. (1981). *A course in universal algebra*. Springer-Verlag New York.

[4] Davey, B. A. & Priestley, H. A. (2002). *Introduction to lattices and order* (2nd). Cambridge University Press.

[5] Dilworth, R. P. (1950). *A Decomposition Theorem for Partially Ordered Sets*. Annals of Mathematics, *51*, 161–166.

[6] Fan, K. (1972). *On Dilworth's Coding Theorem*. Mathematische Zeitschrift, *127*, 92–94.

[7] Grätzer, G. (2011). *Lattice theory: Foundation*. Birkhäuser Basel.

[8] Grätzer, G. & Schmidt, E. T. (1958). *Ideals and Congruence Relations in Lattices*. Acta Mathematica Academiae Scientiarum Hungarica, *9*, 137–175.

[9] Roman, S. (2008). *Lattices and ordered sets*. Springer-Verlag New York.