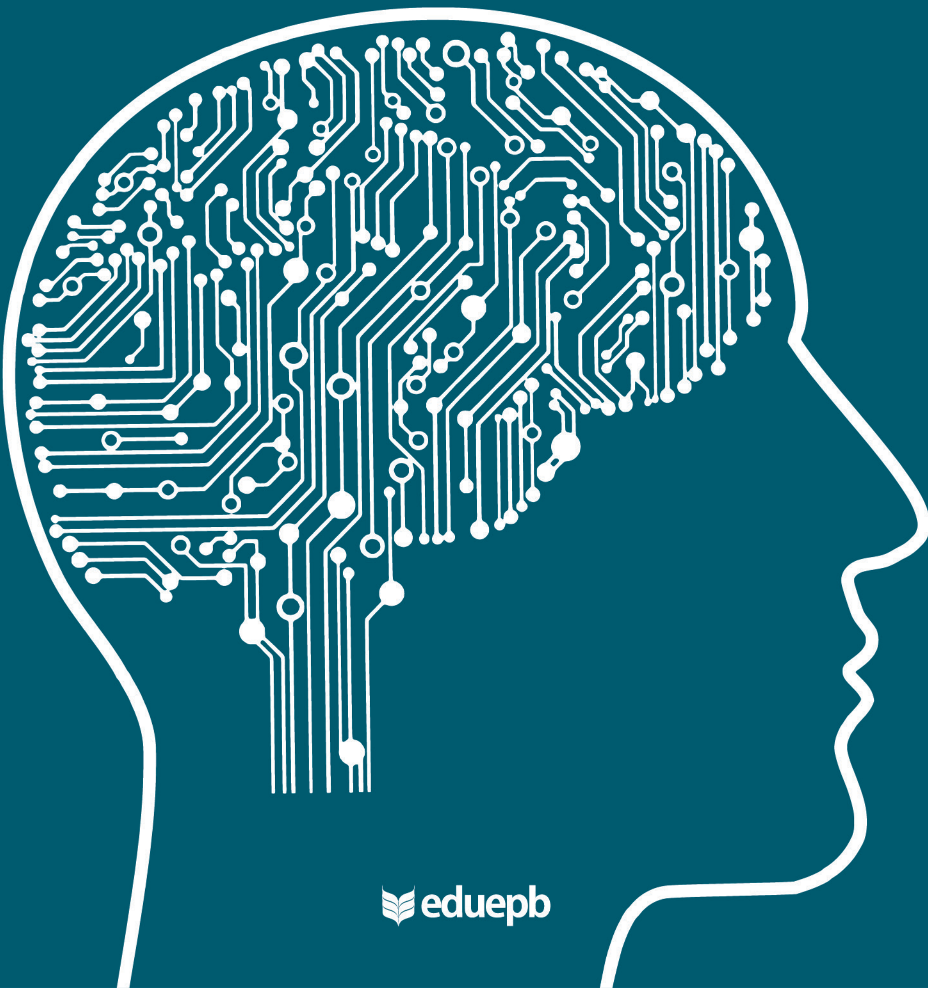
Rodrigo Costa Ferreira

LÓGICA E TEORIA DAS CATEGORIAS

Um curso introdutório de lógica proposicional categórica



eduepb

Editora indexada no SciELO desde 2012

Associação Brasileira
das Editoras Universitárias
Editora filiada a ABEU

EDITORA DA UNIVERSIDADE ESTADUAL DA PARAÍBA
Rua Baraúnas, 351 - Bairro Universitário - Campina Grande-PB - CEP 58429-500
Fone/Fax: (83) 3315-3381 - http://eduepb.uepb.edu.br - email: eduepb@uepb.edu.br

Rodrigo Costa Ferreira

Lógica e Teoria das Categorias:

Um curso introdutório de lógica proposicional categórica

eduepb

Campina Grande - PB
2022

Estado da Paraíba

João Azevêdo Lins Filho | *Governador*
Ana Lígia Costa Feliciano | *Vice-governadora*

Nonato Bandeira | *Secretário da Comunicação Institucional*
Claudio Benedito Silva Furtado | *Secretário da Educação e da Ciência e Tecnologia*
Damião Ramos Cavalcanti | *Secretário da Cultura*

EPC - Empresa Paraibana de Comunicação

Naná Garcez de Castro Dória | *Diretora Presidente*
William Pereira Costa | *Diretor de Mídia Impressa*
Alexandre Macedo | *Gerente da Editora A União*
Albiege Léa Fernandes | *Diretora de Rádio e TV*

EDITORA
A UNIÃO
BR 101 - KM 03 - Distrito Industrial - João Pessoa-PB - CEP: 58.082-010

Depósito legal na Câmara Brasileira do Livro - CDL

F383l Ferreira, Rodrigo Costa.
Lógica e teoria das categorias : um curso introdutório de lógica proposicional categórica / Rodrigo Costa Ferreira. – Campina Grande : EDUEPB, 2022.
134 p. : il. ; 15 x 21 cm ; 2,8 MB.

ISBN: 978-85-7879-788-1 (Impresso)
ISBN: 978-85-7879-792-8 (E-book)

1. Relações matemáticas. 2. Estruturas matemáticas. 3. Lógica matemática. I. Título.

21. ed. CDD 511.3

Ficha catalográfica elaborada por Fernanda Mirelle de Almeida Silva – CRB-15/483

Ao mestre Giovanni (*In Memoriam*)

Agradeço ao lógico, matemático e filósofo Giovanni da Silva de Queiroz por ter me iniciado nos estudos da lógica e da teoria das categorias. Sou-lhe muito grato também pela amizade e pelas valiosas lições de vida.

Gostaria de expressar também o meu mais sincero agradecimento ao editor-chefe prof. Cidoval Morais de Sousa, ao professor Antônio de Brito e demais membros da equipe editorial pela edição dessa obra.

SUMÁRIO

PREFÁCIO

A teoria das categorias é uma teoria matemática elegante e generalista que faz uso de uma linguagem abstrata cheia de gráficos e de uma axiomática intuitiva. Essa teoria, em linhas gerais, permite expor de forma mais clara estruturas e relações matemáticas, bem como possibilita correlacionar os mais distintos ramos da matemática. Não é de se estranhar que o lógico atento a essa poderosa ferramenta matemática proponha no mínimo duas questões, a saber: (1) Como a teoria das categorias "funciona" associada à lógica moderna (uma lógica matemática)?; (2) O uso de estruturas matemáticas da teoria das categorias é vantajoso aos estudos da lógica moderna?

Ao longo do presente livro tentamos responder (1) e (2), ainda que de modo incipiente e a partir de um contexto mais modesto de investigação: o da lógica proposicional. Com esse intuito, oferecemos ao leitor um curso introdutório de "lógica proposicional categórica": uma lógica proposicional (clássica) que se vale das técnicas matemáticas da teoria das categorias.

O nosso curso não existiria sem a valiosa orientação e incursões (exemplos e demonstrações) do lógico e matemático Giovanni da Silva de Queiroz. Esse livro vem a público em sua homenagem.

Desde já não é demais esclarecer ao leitor que muitas das lições de lógica categórica oferecidas no nosso curso foram extraídas, observadas poucas modificações, da obra *Topoi: The Categorial Analysis of Logic*, escrita pelo matemático e lógico Robert Goldblatt. Outras tantas motivações e exemplos trabalhados por nós estão presentes no *Categoy Theory* de Steve Awodey.

Como organizamos o nosso curso? Detalhes sobre as origens e os desenvolvimentos da lógica e teoria das categorias, e a posterior aplicação daquela nesta, são apresentados já no primeiro capítulo.

O domínio da teoria das categorias demanda bastante esforço e dedicação. Para amenizar essas dificuldades, tratamos da axiomática e de algumas estruturas importantes da teoria das categorias no segundo capítulo.

Como pretendemos entrelaçar a teoria das categorias com a lógica proposicional, no terceiro capítulo buscamos expor de modo claro alguns conceitos básicos e avançados da lógica proposicional como uma espécie de lógica matemática.

No último momento do nosso curso, mostramos como é possível traduzir os conectivos lógicos (negação, implicação, disjunção e conjunção) em termos categóricos. Com isso, na sequência, estabelecemos certas condições que permitem modelar uma semântica categórica capaz de interpretar as fórmulas bem formadas do cálculo proposicional proposto.

Ao final, avaliamos as propriedades da completude e da correção sob essa nova perspectiva.

Bons estudos!
Rainha da Borborema, 23 Março de 2020.
Rodrigo Costa Ferreira

CAPÍTULO 1
UM POUCO DE HISTÓRIA

1.1 TEORIA DAS CATEGORIAS COMO UM CAPÍTULO IMPORTANTE DA HISTÓRIA DA LÓGICA MATEMÁTICA

Já no século IV a.C., as geniais incursões de Aristóteles acerca da demonstração (ou, em geral, sobre o raciocínio humano) consolidam a lógica como uma disciplina filosófica. Entretanto, o escopo da atual lógica (uma lógica matemática) não se limita ao clássico estudo dos princípios da inferência válida, estendendo-se hoje a tópicos como teoria da prova, teoria dos modelos, teoria da recursão, fundamentos da teoria dos conjuntos, entre outros. Essa revolução no conteúdo da lógica só se deu com a sua matematização no século XIX.

No século XIX ocorreu com a lógica um fenômeno semelhante ao ocorrido com a física no século XVII: a sua matematização. Após a aproximação com a matemática houve um grande avanço na forma de se "fazer lógica" até então não vivenciado. A lógica ao mesmo tempo em que herda e aprimora o formalismo matemático, influencia a matemática com os seus métodos, os quais são utilizados por lógicos e matemáticos para examinar, por exemplo, os fundamentos da matemática e os seus procedimentos de prova. Surge, nesse momento, a moderna "lógica matemática". Daí, dizemos hoje que a lógica além de ser uma disciplina filosófica é também uma disciplina matemática.

Porém, já no século XVII o filósofo e matemático alemão Gottfried Wilhelm Leibniz (1646-1716) desenvolveu uma série de aproximações entre a álgebra e a lógica. Infelizmente, os resultados de seus trabalhos só seriam mais bem difundidos e desenvolvidos a partir do século XIX.

Leibniz, como é possível observar na sua *De Arte Combinatória*, escrita em 1666, compreende que a lógica, com os seus termos, proposições e silogismos, apresenta certa semelhança com a álgebra. Por isso, procurou elucidar vários aspectos da lógica por meio do cálculo algébrico de sua época. Ainda nessa obra introdutória, o filósofo alemão tenta implantar a ambiciosa construção de uma *lingua philosophica* com *characteristica universalis*, uma espécie de sistema exato e universal de notação concebido para expressar de forma precisa o pensamento humano. Em paralelo, propõe o desenvolvimento de um *calculus ratiocinator* (cálculo da razão): uma espécie de cálculo que permitiria inferir das premissas representadas na *lingua philosophica* (um tipo de linguagem formal), por conclusão, todas as coisas pensadas. Apesar do programa lógico-matemático de Leibniz, na forma como foi introduzido no século XVII, não ser teoricamente exequível, o *calculus ratiocinator* representa, no mínimo, uma condição inspiradora à metodologia da lógica matemática moderna.

Passados dois séculos da proposta de Leibniz, a lógica matemática tem uma formulação formal mais concisa no ano de 1847 com a publicação do livro *The Mathematical Analysis of Logic* de George Boole (1815-1864). Neste trabalho inovador Boole situa a lógica matemática como uma espécie de cálculo lógico de classes. No mesmo ano, Augustus De Morgan (1806-1871) publica o tratado *Formal Logic*, no qual desenvolve importantes estudos sobre a lógica das relações. No ano de 1854, George Boole publica *An Investigation into the Laws of thought on which are Founded the Mathematical Theories of Logic and Probability* complementando os estudos da sua *The Mathematical Analysis of Logic*. Anos depois, com Ernst Schröder (1841-1902), no volumoso tratado *Vorlesungen über die Algebra der Logic,* publicado entre 1890 e 1895, as noções lógicas booleanas recebem um refinamento notável.

Uma abordagem simbólica moderna à lógica é encontrada nos trabalhos do alemão Gottlob Frege (1848-1925), em particular, no *Begriffsschrift* de 1879, no *Grundgesetze der Arithmetik*, publicado entre 1879 e 1903, e nas pesquisas de Giuseppe Peano (1858-1932) com o extenso *Formulaire de Mathématiques* de 1894. Ao longo dessas obras, Frege tenta fundamentar logicamente o “raciocínio matemático” (ou a demonstração matemática) a partir de uma linguagem artificial precisa capaz de tornar mais explícito os seus processos de inferência. Essa linguagem formal de notação complexa lhe permitiu estabelecer as bases modernas do cálculo proposicional e do cálculo de primeira ordem – uma das grandes inovações, nesse sentido, foi a do uso de símbolos que expressam quantificadores, variáveis e funções. Uma das grandes contribuições de Peano, por sua vez, consiste em ter melhorado a notação simbólica de Frege, sendo a notação de Peano usada ainda hoje para expressar o cálculo lógico.

Os trabalhos iniciados por Frege e Peano impulsionaram a construção da monumental *Principia Mathematica* publicada entre os anos de 1910 e 1913 por Alfred North Whitehead (1861-1947) e Bertrand Russell (1872-1970). A identificação de grande parte da matemática com a lógica é a ideia básica dessa obra. Ao longo dos seus estudos, os conceitos e teoremas matemáticos são traduzidos em noções lógicas. Essa investigação tem início com o cálculo das proposições; e passa, na sequência, a elucidar aspectos importantes da teoria das classes e teoria das relações.

No período entre 1934 e 1939 aparece o abrangente *Grundlagen der Mathematik* de David Hilbert (1862-1943) e Paul Bernays (1888-1977). O ambicioso programa formalista de Hilbert e Bernays tem como objetivo fundamentar logicamente toda a matemática mediante a aplicação de sistemas formais baseados no método axiomático. Importantes contribuições para a teoria da prova são dadas nesse momento.

Os anos que se sucederam às pesquisas de Bernarys e Hilbert são seguidos por inúmeros outros importantes trabalhos em lógica matemática, entre os quais, para citar alguns, o artigo *Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme I* (1931) do matemático Kurt Gödel

(1906-1978) e os trabalhos *On Some Fundamental Concepts of Metamathematics* (1930) e *The Concept of Truth in Formalized Languages* (1935), *Boolean Algebras with Operators* (1952) do lógico polonês Alfred Tarski (1901-1983). Além do surpreendente resultado da incompletude de Gödel, ocorre o desenvolvimento de pontos importantes da teoria da representação e da teoria dos modelos (consequência importante da definição semântica de verdade de Tarski).

Conceitos fundamentais da álgebra moderna (ou abstrata), tipologia e espaços vetoriais foram estabelecidos entre 1920 e 1940. Nos vinte anos seguintes é possível observar uma verdadeira revolução nos métodos da topologia algébrica homológica. A álgebra homológica é um desenvolvimento da álgebra abstrata que trata de resultados válidos em diversos tipos de espaços matemáticos. Um dos frutos desse avanço ocorre com a introdução em 1942 por Eilenberg e Mac Lane das noções de funtor e categoria. Essas contribuições marcam o início da *teoria das categorias*.

No ano de 1942, Samuel Eilenberg (1913-1998) e Saunders Mac Lane (1909-2005) propõem novos métodos para o cálculo de grupos homólogos. Na ocasião constatam que grande parte dos grupos estudados estão relacionados de modo a exibirem uma determinada propriedade universal denotada por eles como "natural". Essa compreensão os conduz à criação e à aplicação dos "isomorfismos naturais" para um tratamento mais geral dos grupos algébricos. Além da noção de isomorfismo natural, formulam o importante conceito de funtor: no sentido de determinar um significado mais exato àquilo que é compartilhado pelas estruturas algébricas abstratas. Eilenberg e Mac Lane, cientes da necessidade de uma construção axiomática mais geral às suas pesquisas, anunciam, ainda em 1942, a realização de estudos futuros. Um trabalho detalhado da axiomática dos isomorfismos naturais só é publicado no ano de 1945, sob o título de *General Theory of Natural Equivalences*.

A publicação da *Teoria Geral das Equivalências Naturais* marca oficialmente o nascimento da *teoria das categorias*. Com essa teoria pretendem, inicialmente, fundamentar uma axiomática geral na qual a noção de isomorfismo natural associada aos conceitos de funtor e de categoria possibilitam capturar propriedades universais pertencentes a diferentes estruturas matemáticas. Mediante algumas dificuldades teóricas, Eilenberg e Mac Lane acrescentam à axiomática das equivalências naturais os conceitos de funtor e de categoria.

A categoria, a princípio, é entendida por Eilenberg e Mac Lane como como um conceito auxiliar à definição de funtor, ou seja, como algo útil apenas para solucionar certos problemas decorrentes da aplicação da noção de funtor. Mac Lane e Eilenberg, depois de introduzirem em 1945 algumas noções categóricas importantes, acreditavam ter produzido uma linguagem eficaz aos interesses dos topologistas e de outros, uma vez que essa permite oferecer uma visão conceitual ampla de inúmeras partes da matemática.

Na primavera de 1956, Daniel Kan introduziu o importante conceito de funtor adjunto à teoria das categorias. O matemático trabalhava na teoria homotópica, desenvolvendo o que é chamado, hoje, de teoria homotópica combinatória. De imediato, Kan percebeu que poderia usar a noção de funtor adjunto para unificar vários dos resultados obtidos por ele em pesquisas anteriores. Em 1958, o matemático publica uma versão unificada desses resultados no artigo *Functors Involving Complexes*. Ainda sobre os resultados obtidos em suas pesquisas, Kan escreve o artigo *Adjoint Functors,* tratando particularmente da ideia de funtores adjuntos. Ao escrever esse artigo que Kan descobre como a definição de funtor adjunto é geral e importante para se definir outras noções essenciais à teoria das categorias, tais como a de limite e colimite.

Em 1957, Alexander Grothendieck (1928-2014) procurou generalizar não apenas o trabalho de Eilenberg e Mac Lane, mas também alguns resultados particulares da álgebra abstrata ao definir as "categorias abelianas". A axiomática das categorias abelianas levou em conta apenas características estruturais compartilhadas, na medida em que objetos abelianos foram definidos como uma condição teórica primitiva em função do conceito de categoria. Tal terminologia permite a Grothendieck caracterizar um tipo de estrutura existente entre objetos, sem que, para tanto, fosse necessário especificar ao certo tais objetos.

A "lógica categórica" (uma lógica matemática que faz uso das estruturas da teoria das categorias) tem início na década de 60 com os trabalhos de Francis William Lawvere. Em 1963, o matemático Francis William Lawvere (1937-), na sua tese de doutorado *Functorial Semantics of Algebraic*, define uma semântica funtorial capaz de interpretar uma teoria algébrica em outra teoria algébrica por meio de um funtor. Passados alguns anos, nos trabalhos *Theories as Categories and the Completeness Theorem* (1967) e *Quantifiers and Sheaves* (1970), Lawvere faz uso da estrutura funtor para determinar os adjuntos de Kan (aqueles de imagem inversa) como quantificadores lógicos, bem como introduz uma nova axiomática aos topos de Grothendieck, buscando generalizá-los sob uma perspectiva topológica e categórica. Tal fato o levou, posteriormente, a desenvolver uma definição de topos capaz de fornecer um tratamento categórico à lógica de primeira ordem.

Por influência dos trabalhos de Lawvere, a partir das décadas de 1960 e 1970 há um maior interesse na aplicação da teoria das categorias nas lógicas algébricas. Tal interesse se mantém vivo, sendo a lógica categórica atualmente abordada como um importante objeto de pesquisa no desenvolvimento de novos sistemas lógicos.

CAPÍTULO 2
TEORIA DAS CATEGORIAS: PRIMEIROS PASSOS

2.1 DEFINIÇÃO AXIOMÁTICA DE CATEGORIA

A axiomática de uma categoria qualquer $\mathscr{C}$ é definida a seguir. Toda categoria tem como primitivos os conceitos de objeto e morfismo (ou setas), devendo os morfismos satisfazerem, em especial, as propriedades de composição e identidade.

DEFINIÇÃO 2.1 (AXIOMÁTICA DE UMA CATEGORIA QUALQUER) UMA CATEGORIA QUALQUER $\mathscr{C}$ COMPREENDE:

(1) *Obj* ($\mathscr{C}$): uma coleção de objetos;

(2) *Hom* ($\mathscr{C}$): uma coleção de morfismos;

(3) *D; CD*: duas operações denominadas domínio e codomínio. Para cada morfismo *f* de *Hom* ($\mathscr{C}$) com $a = D(f)$ e $b = CD$

(f), escrevemos *f:a* $\longrightarrow$ *b*; *f:* $\langle A, B \rangle$ ou $a \xrightarrow{f} b$;

(4) $\circ$: uma operação de composição. Sejam *f: a* $\longrightarrow$ *b, g: b* $\longrightarrow$ *c, h: c* $\longrightarrow$ *d* morfismos de *Hom* ($\mathscr{C}$), temos a composição *(h* $\circ$ *g)* $\circ$ *f = h* $\circ$ *(g* $\circ$ *f): a* $\longrightarrow$ *b*, de forma que o diagrama abaixo comute

$$
\begin{tikzcd}
a \arrow[r, "f"] \arrow[d, dotted, "g \circ f"'] \arrow[dr, dotted] & b \arrow[dl, "g"] \arrow[d, dotted, "h \circ g"] \\
c \arrow[r, "h"'] & d
\end{tikzcd}
;
$$

(5) *id*: uma operação chamada identidade. Para cada objeto *a* e *b* de Obj ($\mathscr{C}$) ocorrem morfismos identidade *ida: a* $\longrightarrow$ *a* e *idb: b* $\longrightarrow$ *b,* tal que, dado um morfismo qualquer *f: a* $\longrightarrow$ *b* de *Hom* ($\mathscr{C}$), o diagrama comute

$$
\begin{tikzcd}
a \arrow[r, "f"] \arrow[d, "id_a"'] \arrow[dr, "f"] & b \arrow[d, "id_b"] \\
a \arrow[r, "f"'] & b,
\end{tikzcd}
$$

isto é, $f \circ ida = idb \circ f = f$.

Uma categoria $\mathscr{C}$ é uma estrutura do tipo $\langle Obj\ (\mathscr{C}),\ Hom\ (\mathscr{C}),\ D,\ CD,\ id,\ \circ \rangle$.

2.2 ALGUMAS CATEGORIAS

Com o objetivo de tornar a definição de uma categoria qualquer (Definição 2.1) mais clara ao leitor, tratamos adiante de algumas expécies de categoria: categoria dos conjuntos (SET), categoria das funções ($\mathrm{SET}^{\rightarrow}$), categoria dos conjuntos parcialmente ordenados (POSET), categoria dos monóides (MON) e categoria dos grupos (GRU). As categorias MON e GRU podem ser facilmente compreendidas após a elucidação de alguns conceitos importantes da álgebra abstrata: monóide, grupo e homomorfismo.

2.2.1 CATEGORIA DOS CONJUNTOS (SET)

Definição 2.2 (Axiomática da Categoria dos Conjuntos) $SET = \langle Obj\ (SET),\ Hom\ (SET),\ D,\ CD,\ id,\ \circ \rangle$ é uma categoria se, somente se, as seguintes condições são satisfeitas:

(1) *Obj* (SET) são conjuntos;

(2) *Hom* (SET) são funções entre conjuntos;

(3) *D, CD*: *Hom* (SET) $\longrightarrow$ *Obj* (SET) são operações denominadas domínio A e codomínio B, ou seja, *A* = *D (f)* e B = *CD (f)* para qualquer função *f* entre conjuntos;

(4) $\circ$: *Hom* (SET)2 $\longrightarrow$ *Hom* (SET) é a composição de funções entre conjuntos;

(5) *id*: *Obj* (SET) $\longrightarrow$ *Hom* (SET) é a operação identidade, na qual a cada conjunto A é associado a função identidade *idA*: A $\longmapsto$ A e a cada conjunto B é conferida a função identidade *idB*: B $\longmapsto$ B.

As proposições a seguir validam a **Definição 2.2**

Proposição 2.1 A operação composição é associativa em SET.

Demonstração:

Para as funções $f: A \longmapsto B$, $g: B \longmapsto C$ e $h: C \longmapsto A$, e para qualquer que seja aA, temos:

$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))) = h(g \circ f(a)) =$
$(h \circ (g \circ f)))(a)$

$\square$

Proposição 2.2 Em SET vale a identidade.

Exercício 2.1 Provar a **Proposição 2.2**

Exemplo:

A categoria SET $^{\mathbb{Z}}$ possui infinitos morfismos que, por definição, são números inteiros $\mathbb{Z} = \{\ldots 3, 2, 1, 0, -1, -2, -3 \ldots\}$. Os morfismos dessa categoria têm um mesmo domínio e codomínio, já que na categoria SET$^{\mathbb{Z}}$ há um único objeto chamado $\mathbb{Z}$.

Da composição dos morfismos m e n (números quaisquer) deriva um número distinto $n \cdot m$ (multiplicação). Se $n \circ m = n \cdot m$, então o diagrama abaixo comuta

$$
\begin{tikzcd}
\mathbb{Z} \arrow[r, "n"] \arrow[dr, "n \cdot m"'] & \mathbb{Z} \arrow[d, "m"] \\
& \mathbb{Z}
\end{tikzcd}
.
$$

A multiplicação em SET $^{\mathbb{Z}}$ é associativa: $m \cdot (n \cdot k) = (m \cdot n) \cdot k$, sendo essa válida para qualquer número inteiro *n*, *m* e *k*. Nesses termos, o diagrama

$$
\begin{tikzcd}
\mathbb{Z} \arrow[r, "n"] \arrow[d, "m \circ n"'] \arrow[dr, dotted] & \mathbb{Z} \arrow[d, "k \circ m"] \arrow[dl, "m"] \\
\mathbb{Z} \arrow[r, "k"'] & \mathbb{Z}
\end{tikzcd}
$$

comuta, pois $m \circ (n \circ k) = (m \circ n) \circ k = m \cdot (n \cdot k) = (m \cdot n) \cdot k$.

O morfismo identidade $id_{\mathbb{Z}}$ de $\mathbb{Z}$ é o número 1, já que o diagrama a seguir comuta

$$
\begin{tikzcd}
\mathbb{Z} \arrow[r, "m"] \arrow[d, "m"'] & \mathbb{Z} \arrow[d, "n"] \arrow[dl, "0"] \\
\mathbb{Z} \arrow[r, "n"'] & \mathbb{Z},
\end{tikzcd}
$$

na medida em que $1 \cdot m = m$ e $n \cdot 1 = n$.

2.2.2 CATEGORIA DAS FUNÇÕES (SET$^{\rightarrow}$)

Definição 2.3 (Axiomática da Categoria das Funções) $SET^{\rightarrow} = \langle Obj\,(SET^{\rightarrow}),\ Hom\,(SET^{\rightarrow}),\ D,\ CD,\ id,\ \circ \rangle$ é uma categoria se, somente se, as seguintes condições são satisfeitas:

(1) *Obj (*SET$^{\rightarrow}$*)* são funções*;*

(2) *Hom* (SET$^{\rightarrow}$) são pares de funções;

(3) *D, CD: Hom* (SET$^{\rightarrow}$) $\longrightarrow$ *Obj (*SET$^{\rightarrow}$*)* é a operação do par de funções com domínio *D (f)* = $\langle i, j \rangle$ e o codomínio *CD (f)* = $\langle h, k \rangle$, de forma que *f*: $\langle i, j \rangle \longrightarrow \langle h, k \rangle$*;*

(4) $\circ$: *Hom* (SET$^{\rightarrow}$)2 $\longrightarrow$ *Hom* (SET$^{\rightarrow}$) é a composição

que ocorre quando os morfismos em *Hom* ($\mathrm{SET}^{\rightarrow}$) comutam, isto é, $\langle i, j\rangle \circ \langle h, k\rangle = \langle i \circ h, j \circ k\rangle$;

(5) *id: Obj* ($\mathrm{SET}^{\rightarrow}$) $\longrightarrow$ *Hom* ($\mathrm{SET}^{\rightarrow}$) é o par $\langle id_A, id_B\rangle$ das funções identidades.

As proposições a seguir validam a **Definição 2.3**

Proposição 2.3 A operação composição é associativa em $\mathrm{SET}^{\rightarrow}$.

EXERCÍCIO 2.2 PROVE A **PROPOSIÇÃO 2.3**

Proposição 2.4 Em $\mathrm{SET}^{\rightarrow}$ vale a identidade.

Demonstração:

Dado o diagrama

$$\begin{tikzcd} A \arrow[r, "id_A"] \arrow[d, "f"'] & A \arrow[d, "f"] \\ B \arrow[r, "id_B"'] & B \end{tikzcd},$$

podemos definir para o morfismo $A \xrightarrow{f} B$ a identidade $id_f = \langle id_A, id_B \rangle$.

Conforme o diagrama

$$
\begin{tikzcd}
A \arrow[r, "id_A"] \arrow[d, "f"'] & A \arrow[r, "h"] \arrow[d, "f"'] & C \arrow[d, "g"] \\
B \arrow[r, "id_B"'] & B \arrow[r, "k"'] & D
\end{tikzcd} ,
$$

segue

$\langle h, k \rangle \circ \langle id_A, id_B \rangle = \langle h \circ id_A, k \circ id_B \rangle = \langle h, k \rangle,$

bem como temos

$$\langle id_A, id_B \rangle \circ \langle h, k \rangle = \langle id_A \circ h, id_B \circ k \rangle = \langle h, k \rangle \ .$$

$\square$

2.2.3 CATEGORIA DOS CONJUNTOS PARCIALMENTE ORDENADOS (POSET)

Definição 2.4 (Axiomática da Categoria dos Conjuntos Parcialmente Ordenados) $POSET = \langle Obj\ (POSET), Hom\ (POSET), D, CD, id, \circ \rangle$ é uma categoria se, somente se, as seguintes condições são satisfeitas:

(1) *Obj* (*POSET*) são conjuntos parcialmente ordenados;

(2) *Hom* (*POSET*) são funções monotônicas que preservam certa ordem, ou seja, para conjuntos ordenados A e B em que *a, b* A, com $a \leq b$, a função $f: A \longmapsto B$ implica $f(a) \leq f(b)$ em B;

(3) *D, CD: Hom* (*POSET*) $\longrightarrow$ *Obj* (*POSET*) é a operação em que dada a função $f: A \longmapsto B$, temos o domínio $A = D$ e o codomínio $B = CD$;

(4) $\circ$: *Hom* $(POSET)^2 \longrightarrow$ *Hom* (*POSET*) é a operação de composição entre funções monotônicas que preservam certa ordem;

(5) *id: Obj* (*POSET*) $\longrightarrow$ *Hom* (*POSET*) é a operação identidade, segundo a qual ao conjunto A é associado a função identidade $id_A: A \longmapsto A$ e ao conjunto B é conferida a função identidade $id_B: B \longmapsto B$.

As proposições a seguir validam a **Definição 2.4**

Proposição 2.5 A operação composição é associativa em POSET.

Demonstração:

Dadas as funções $f: A \longmapsto B$, $g: B \longmapsto C$ e $h: C \longmapsto D$, com $a, b \ A$:

1. Para $a \leq b$ é possível exprimir $f(a) \leq f(b)$, uma vez que f é monotônica em B;

2. Dado $f(a) \leq f(b)$, temos $g(f(a)) \leq g(f(b))$, já que g é monotônica em C;

3. Como $g(f(a)) \leq g(f(b))$, podemos escrever $h(g(f(a))) \leq h(g(f(b)))$, pois h é monotônica em D;

4. Logo, se $a \leq b$ em A, então $h(g(f(a))) \leq h(g(f(b)))$ em D.

Por outro lado,

1. Se $a \geq b$, então $f(a) \geq f(b)$, uma vez que f é monotônica em B;

2. Dado que $f(a) \geq f(b)$, podemos escrever a equação anterior como $g(f(a)) \geq g(f(b))$, pois g é monotônica em C;

3. Como $g\ (f(a)) \geq g(f(b))$, segue $h\ (g(f(a))) \geq h\ (g\ (f(b)))$, pois h é monotônica em *D;*

4. Portanto, se $a \geq b$ em A, então $h\ (g(f(a))) \geq h\ (g\ (f(b)))$ em D.

Se $a \leq b$ e $a \geq b$, então $a = b$ em A. Conforme os passos 1-4, segue $h\ (g(f(a))) \leq h\ (g\ (f(b)))$ e $h\ (g(f(a))) \geq h\ (g\ (f(b)))$ em D. Dado o exposto, podemos concluir que o seguinte diagrama comuta

$$
\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, dotted, "g\circ f"'] \arrow[dr, dotted] & B \arrow[dl, "g"] \arrow[d, dotted, "h\circ g"] \\
C \arrow[r, "h"'] & D
\end{tikzcd},
$$

isto é, $(h \circ g) \circ f = h \circ (g \circ f)$.
□

Proposição 2.6 Em POSET vale a identidade.

EXERCÍCIO 2.3 PROVE A **PROPOSIÇÃO 2.6**

2.2.4 CATEGORIA DOS MONÓIDES (MON)

Definição 2.5 (Monóide) A matriz $\langle M, \oplus, e \rangle$ é um monóide, na qual:

(1) $\langle M, \oplus \rangle$ é um semi-grupo em que M é um conjunto, não vazio, denominado "conjunto suporte", e $\oplus : A \times A \longmapsto A$ é uma operação binária associativa, definida em M, de forma que para quaisquer *a, b, c* $\in$ *A* subsista a igualdade

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c \ ;$$

(2) Dizemos que *e M* é um elemento neutro da operação $\oplus$ se, somente se, para qualquer *a M*, temos

$$a \oplus e = e \oplus a = a \ .$$

Em um monóide a operação binária não é necessariamente comutativa, já que pode existir *a, b M*, tais que $a \oplus b \neq b \oplus a$. Um monóide é denominado abeliano quando possui operação comutativa.

Exemplo:

São monóides abelianos os semi-grupos aditivo $\langle \mathbb{N}, + \rangle$ e multiplicativo $\langle \mathbb{N}, \cdot \rangle$ com os elementos neutros 0 e 1, já que as operações de adição e de multiplicação em $\mathbb{N}$ (conjunto dos números naturais) são associativas e comutativas. Por isso, são monóides $\langle \mathbb{N}, +, 0 \rangle$ e $\langle \mathbb{N}, \cdot, 1 \rangle$.

Definição 2.6 (Homomorfismo entre Monóides) Sejam $\langle M, \oplus, a\rangle$e $\langle N, \triangleright, e\rangle$ dois monóides. O homomorfismo $f(\oplus): \ \langle M, \oplus, a\rangle \longmapsto \langle N, \triangleright, e\rangle$ de *M* em *N* é toda função $f(\oplus): M \longmapsto N,$ tal que preserva as operações e os elementos identificados. Quaisquer que sejam os elementos *m* e *n* do conjunto *M* e seus elementos neutros, denominados *a* e *e*, seguem as igualdades:

$$\begin{tikzcd}
(m,n) \arrow[r, "\oplus"] \arrow[d, "f"'] \arrow[dr, dotted, "f \circ \oplus = \triangleright \circ f"] & m \oplus n \arrow[d, "f"] \\
(f(m), f(n)) \arrow[r, "\triangleright"'] & f(m \oplus n) = f(m) \triangleright f(n)
\end{tikzcd}$$

$$f(\oplus): \langle M, \oplus, e\rangle \longmapsto \langle N, \triangleright, d\rangle$$

$$f(m \oplus n) = f(m) \triangleright f(n)$$

$$
\begin{tikzcd}
 & \{*\} \arrow[dl, "e"'] \arrow[dr, "a"] & \\
M \arrow[rr, "f"'] & & N
\end{tikzcd}
$$

$$f : \{a\} \longmapsto \{e\}$$

$$f(a) = e$$

A composição de homomorfismos $f \circ \oplus = \triangleright \circ f$ equivale a *f*($\oplus$)) = $\triangleright$(*f*). Ao atribuirmos *m* e *n* à expressão anterior, temos *f*($\oplus$(*m*,*n*))= $\triangleright$(*f*(*m*,*n*)). Ou seja, *f*($\oplus$(*m*,*n*))= $\triangleright$(*f*(*m*), *f*(*n*)) que equivale a *f*(*m*$\oplus$*n*) = *f*(*m*)$\triangleright$*f*(*n*). $\square$

Exemplo:

Dados os monóides $\langle \mathbb{Z}_+, +, 0 \rangle$ e $\langle A, \times, 1 \rangle$, temos o conjunto $A = \{2^n \mid n \in \mathbb{Z}_+\}$A função $f : \mathbb{Z}_+ \longmapsto A$, definida por *f*(*x*) = 2*x*, é um homomorfismo de $\langle \mathbb{Z}_+, +, 0 \rangle$em $\langle A, \times, 1 \rangle$ para quaisquer que sejam os inteiros positivos *a* e *b*:

1. Para os elementos neutros 0 e 1, obtemos:

f(0) = 20 =1;

2. Para quaisquer que sejam os inteiros positivos *a* e *b* do conjunto $\mathbb{Z}_+$ em *f*(*a* + *b*) = 2^a+*b*, segue:

$f(a+b) = 2^{a+b} = 2^a \times 2^b = f(a) \times f(b)$

Definição 2.7 (Axiomática da Categoria dos Monóides) $MON = \langle Obj\,(MON),\ Hom\,(MON),\ D,\ CD,\ id,\ \circ \rangle$ é uma categoria se, somente se, as seguintes condições são satisfeitas:

(1) *Obj* (*MON*) são monóides na forma $\langle M, \oplus,\ e \rangle$;

(2) *Hom* (*MON*) são homomorfismos entre monóides do tipo $h : \langle M, \oplus,\ e \rangle \longrightarrow \langle N, \triangleright,\ d \rangle$, tal que $h: M \longrightarrow N$ preserve as estruturas;

(3) $D, CD: Hom\,(MON) \longrightarrow Obj\,(MON)$ é uma operação em que dada $f: M \longrightarrow N$, temos o domínio $D(f) = \langle M, \oplus,\ e \rangle$ e o codomínio $CD(f) = \langle N, \triangleright,\ d \rangle$, de forma que $f: \langle M, \oplus,\ e \rangle \longrightarrow \langle N, \triangleright,\ d \rangle$.

(4) $\circ$: $Hom\,(MON \rightarrow MON)^2 \longrightarrow Hom\,(MON \rightarrow MON)$ é a composição de homomorfismos;

(5) $id: Obj\,(MON) \longrightarrow Hom\,(MON)$ é a operação identidade entre homomorfismos, segundo a qual ao conjunto *M* é associado a identidade $id_M : \langle M, \oplus,\ e \rangle \longrightarrow \langle M, \oplus,\ e \rangle$ e ao conjunto *N* é indicada a identidade $id_N : \langle N, \triangleright,\ d \rangle \longrightarrow \langle N, \triangleright,\ d \rangle$.

As proposições a seguir validam a **Definição 2.7**

Proposição 2.7 A operação composição é associativa em MON.

Exercício 2.4 Prove a **Proposição 2.7**

Proposição 2.8 Em MON vale a identidade.

DEMONSTRAÇÃO:

*P*ara quaisquer dos homomorfismos entre monóides *f: M* $\longmapsto$ *N*, sendo *a M* e dado *e N*, tal que *f(a) = e*, temos:

$$(f \circ idM)(a) = f(idM\,(a)) = f(a) = e = idN\,(e) = idN\,(f(e)) = (idN \circ f)(a)\,.$$

$\square$

2.2.5 CATEGORIA DOS GRUPOS (GRU)

Definição 2.8 (Grupo) A estrutura $\langle G, \ominus,\ e, ^{-1} \rangle$ é um grupo no qual:

(1) $\langle G, \ominus \rangle$ é um semi-grupo em que *G* é um conjunto, não vazio, denominado "conjunto suporte", e $\ominus : A \times A \longmapsto A$ é uma operação binária associativa, definida em *G*, tal que para quaisquer *a, b, c* $\in$ *A* temos

$$a \ominus (b \ominus c) = (a \ominus b) \ominus c \;;$$

(2) Dizemos que *e G* é um elemento neutro da operação $\ominus$ se, e somente se, para qualquer *a G*, temos

$$a \ominus e = e \ominus a = a \,;$$

(3) O elemento *e G* admite um elemento inverso (único) $a^{-1} \in$ *G* se, somente se, para *a G*, segue

$$a \ominus a^{-1} = a^{-1} \ominus a = e.$$

No item 3 da definição acima o inverso é sempre único. É fácil perceber isso, supondo *a' e a''* dois inversos de *a,* então $a'' \ominus (a \ominus a') = (a'' \ominus a) \ominus a' = e \ominus a' = a'$. □

Exemplo:

São grupos abelianos os semi-grupos aditivo $\langle \mathbb{R}, + \rangle$ R e multiplicativo $\langle \mathbb{R}, \cdot \rangle$ com elementos neutros 0 e 1 e elementos inversos – a e $\frac{1}{a}$ de $\mathbb{R}$ (conjunto de números reais), de forma que a $\neq$ 0, já que as operações de adição e de multiplicação em $\mathbb{R}$, números reais, são associativas e comutativas. Logo, são grupos $\langle \mathbb{R}, +, -a \rangle$ e $\left\langle \mathbb{R}, \cdot, \frac{1}{a} \right\rangle$.

Definição 2.9 (Homomorfismo entre Grupos) Sejam $\langle G, \ominus, e, ^{-1} \rangle$ e $\langle H, \triangleright, d, ^{-1} \rangle$ dois grupos. O homomorfismo $g(\ominus) : \langle G, \ominus, e, ^{-1} \rangle \longmapsto \langle H, \triangleright, d, ^{-1} \rangle$ de *G* em *H é* toda função $g(\ominus) : G \longmapsto H$ que preserva as operações e os elementos identificados. Ou seja, para *a* e *b* no conjunto *G*, os seguintes diagramas comutam:

$$
\begin{tikzcd}
(a,b) \arrow[r, "*"] \arrow[d, "g"'] \arrow[dr, dotted, "g \circ \ominus = \diamond \circ g"] & a \ominus b \arrow[d, "g"] \\
(g(a), g(b)) \arrow[r, "\diamond"'] & g(a \ominus b) = g(a) \diamond g(b)
\end{tikzcd}
$$

$$
\begin{gathered}
g(\ominus) : \langle G, \ominus, e \rangle \longmapsto \langle H, \diamond, d \rangle \\
g(a \ominus b) = g(a) \diamond g(b)
\end{gathered}
$$

$$
\begin{tikzcd}
 & \{*\} \arrow[dl, "d"'] \arrow[dr, "e"] & \\
G \arrow[rr, "g"'] & & H
\end{tikzcd}
$$

$$
\begin{gathered}
g : \{e\} \longmapsto \{d\} \\
f(e) = d
\end{gathered}
$$

$$\begin{tikzcd}
g(a) \arrow[rr, "g^{-1}"] & & g(g(a))^{-1} \\
a \arrow[u, "g"] \arrow[urr, "g^{-1} \circ g"'] & &
\end{tikzcd}$$

$$g(a^{-1}) = g(g(a))^{-1}$$

Sabemos que $a \ominus a^{-1} = e$ e que $a^{-1} \ominus a = e$. Ao aplicarmos a função g aos membros: se $g(a \ominus a^{-1}) = g(e)$, então $g(a) \ominus g(a^{-1}) = g(a^{-1}) \ominus g(a) = g(e) = d$. Pela unicidade do inverso, obtemos $g(a^{-1}) = (g(a))^{-1}$. $\square$

Exemplo de Homomorfismo entre Grupos:

Definição 2.10 (Álgebra de Boole) Uma Álgebra de Boole $\mathscr{B}$ é uma estrutura do tipo $\mathscr{B} = \langle \boldsymbol{B}, \sqcup, \sqcap, -, 0, 1 \rangle$ na qual:

(1) B é um conjunto não-vazio;

(2) $\sqcup$, $\sqcap$ são duas operações binárias sobre B;

(3) – é um operador unário sobre B;

(4) 0 e 1 são dois elementos distintos de B;

Para quaisquer x, y, z, 0 e 1 pertencentes a B, vale o seguinte:

($Ax_{\mathscr{B}}$ 1) $x \sqcap y = y \sqcap x$ (Comutatividade);
($Ax_{\mathscr{B}}$ 2) $x \sqcup y = y \sqcup x$ (Comutatividade);
($Ax_{\mathscr{B}}$ 3) $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$ (Distributiva);
($Ax_{\mathscr{B}}$ 4) $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$ (Distributiva);
($Ax_{\mathscr{B}}$ 5) $x \sqcup 0 = 0 \sqcup x = x$ (Identidade);
($Ax_{\mathscr{B}}$ 6) $x \sqcap 1 = 1 \sqcap x = x$ (Identidade);
($Ax_{\mathscr{B}}$ 7) $x \sqcap -x = 0$ (Complementariedade);
($Ax_{\mathscr{B}}$ 8) $x \sqcup -x = 1$ (Comutatividade);

Teorema 2.1 (Princípio da Dualidade) Todo resultado dedutível dos axiomas da álgebra de Boole permanece válido se nele trocamos $\sqcup$ por $\sqcap$ e 0 por 1, e vice-versa.

Demonstração:

Ao tomarmos $\sqcup$ e $\sqcap$ como operações binárias, $-$ como um elemento inverso e 0 e 1 como elementos neutros, podemos definir as estruturas booleanos $\langle \mathbf{B}, \sqcap, -, 0 \rangle$ e $\langle \mathbf{C}, \sqcup, -, 1 \rangle$ como grupos. Portanto, se o homomorfismo *f*: $\mathbf{B} \longmapsto \mathbf{C}$ preserva as operações binárias e os elementos inversos e neutros, então para quaisquer que sejam os elementos *a* e *b* do conjunto **B** são válidas as igualdades:

$$f(x \sqcap y) = f(x) \sqcup f(y)$$
$$f(0) = 1$$
$$f(-x) = -(f(x))$$

$\square$

Essa característica homomórfica da álgebra booleana corresponde ao *teorema da dualidade*. Segundo este teorema, todo resultado dedutível dos axiomas de uma álgebra de Boole permanece válido se nele trocarmos $\sqcup$ por $\sqcap$ e 0 por 1, e vice-versa, pois pela simetria da definição de uma álgebra de Boole entre os operadores $\sqcap$ e $\sqcup$ os elementos 0 e 1, tanto esses como aqueles podem ser intercambiados, conduzindo outros resultados também verdadeiros.

Definição 2.11 (Axiomática da Categoria dos Grupos) $GRU = \langle Obj\ (GRU),\ Hom\ (GRU),\ D,\ CD,\ id,\ \circ \rangle$ é uma categoria se, somente se, as seguintes condições são satisfeitas:

(1) *Obj* (*GRU*) são grupos;

(2) *Hom* (*GRU*) são homomorfismos entre grupos do tipo $h : \langle G, \ominus,\ e,^{-1} \rangle \longrightarrow \langle H, \triangleright, d,^{-1} \rangle$, tal que a função *h: G* $\longrightarrow$ *H* preserve as estruturas;

(3) *C, CD: Hom* (*GRU*) $\longrightarrow$ *Obj* (*GRU*) são tais que *f: G* $\longrightarrow$ *H*, com $D\ (f) = \langle G, \ominus,\ e,^{-1} \rangle$, $CD\ (f) = \langle H, \triangleright,\ d,^{-1} \rangle$ e $f : \langle G, \ominus,\ e,^{-1} \rangle \longrightarrow \langle H, \triangleright,\ d,^{-1} \rangle$;

(4) $\circ$: *Hom* (*GRU* $\rightarrow$ *GRU*)2 $\longrightarrow$ *Hom* (*GRU* $\rightarrow$ *GRU*) é a operação de composição de homomorfismos;

(5) *id: Obj* (*GRU*) $\longrightarrow$ *Hom* (*GRU*) é a operação identidade entre homomorfismos, segundo a qual ao conjunto *G* é associado a identidade $id_G : \langle G, \ominus,\ e,^{-1} \rangle \longrightarrow \langle G, \ominus,\ e,^{-1} \rangle$ e ao conjunto *H* é indicada a identidade $id_H : \langle H, \triangleright,\ d,^{-1} \rangle \longrightarrow \langle H, \triangleright,\ d,^{-1} \rangle$.

As proposições a seguir validam a **Definição 2.11**

Proposição 2.9 A operação composição é associativa em GRU.

Demonstração:

O seguinte diagrama

$$\begin{tikzcd}
M \arrow[rr, "f"] \arrow[dd, dotted, "g\circ f"'] \arrow[ddrr, dotted] & & N \arrow[ddll, "g"] \arrow[dd, dotted, "h\circ g"] \\
& & \\
G \arrow[rr, "h"'] & & H
\end{tikzcd}$$

indica os homomorfismos entre os grupos $\langle M, \oplus, a,^{-1} \rangle$, $\langle N, \triangleright, e,^{-1} \rangle$, $\langle G, \odot, o,^{-1} \rangle$ e $\langle H, \diamond, u,^{-1} \rangle$. Os homomorfismos são:

1. Se *m,n M*, tal que *f: M* $\longmapsto$ *N*, então há o homomorfismo $f(m \oplus n) = f(m) \triangleright f(n)$, $f(a) = e$, e $f(m^{-1}) = f(f(m))^{-1}$;

2. Se *p,q N*, dado *g: N* $\longmapsto$*G*, temos o homomorfismo $g(p \triangleright q) = g(p) \odot g(q)$ e $g(e) = o$, e $g(p^{-1}) = g(g(p))^{-1}$;

3. Como *r,s G*, e *h: G* $\longmapsto$*H*, obtemos o homomorfismo $h(r \odot s) = h(r) \diamond h(s)$ e $h(o) = u$, *e* $h(r^{-1}) = h(h(r))^{-1}$;

4. Se *m,n M*, e *g* $\circ$ *f: M* $\longmapsto$*G*, logo temos o homomorfismo $g \circ f(m \oplus n) = g \circ f(m) \odot g \circ f(n)$ e $g \circ f(a) = o$ e $g \circ f(m^{-1}) = g \circ f(g \circ f(m))^{-1}$;

5. Se *p,q N*, e temos *h* $\circ$ *g: N* $\longmapsto$ *H*, então ocorre o homomorfismo $h \circ g(p \triangleright q) = h \circ g(p) \diamond h \circ g(q)$, $h \circ g(e) = u$ e $h \circ g(p^{-1}) = h \circ g(h \circ g(m))^{-1}$;

6. Como *m,n M*, e $(h \circ g) \circ f = h \circ (g \circ f) : M \longmapsto H$, segue $h \circ (g \circ f)\ (m \oplus n) = h \circ (g \circ f)(m) \diamond h \circ (g \circ f)(n)$, e, consequentemente, $h \circ (g \circ f)(a) = u$ e $h \circ (g \circ f)(m^{-1}) = h \circ (g \circ f)(h \circ (g \circ f)(m))^{-1}$;

O elemento neutro do grupo $\langle M, \oplus, a,^{-1} \rangle$ pode ser escrito na forma $m \oplus m^{-1} = m^{-1} \oplus m = a$. Ao plicarmos a função *f* a todos os membros da equação anterior, obtemos $f(m \oplus m^{-1}) = f(a)$. Seja *f(a)* = *e*, segundo o passo 1, temos $f(m \oplus m^{-1}) = e$. Mas, pelo passo 5, se $h \circ g(e) = u$, então $h \circ g(f(m \oplus m^{-1}))$ = $(h \circ g) \circ f(m \oplus m^{-1})$)= *u*. Como *u* = *h*○ *(g* ○*f) e m* ⊕ *m*–1, segue *u* = *h*○*(g* ○*f)(m* ⊕ *m*–1*)*. Logo, a propriedade associativa ocorre, pois *(h*○*g)*○*f* *(m* ⊕ *m*–1) = *u* = *h*○ *(g*○*f)(m* ⊕ *m*–1*)*.

□

Proposição 2.10 Em GRU vale a identidade.

Demonstração:

Para qualquer um dos homomorfismos entre os grupos *f: M* ⟼ *N*, tal que *a M* e para *e N*, como *f(m* ⊕ *m*–1 *)* = *f(a)* = *e*, temos:

(f ○ *idM)(a)* = *f(idM (a))* = *f(a)* = *e* = *idN(e)* = *idN(f(e))* = *(idN* ○ *f)(a)*

□

2.3 ALGUMAS ESTRUTURAS CATEGÓRICAS

2.3.1 MONOMORFISMO, EPIMORFISMO E ISOMORFISMO

A seguir são analisadas as estruturas categóricas monomorfismo, epimorfismo e isomorfismo. Motivamos os nossos estudos sob as seguintes definições da teoria dos conjuntos: 1. função injetora – conceito generalizado pela noção de monomorfismo; 2. função sobrejetora – definição generalizada pela noção de epimorfismo; e 3. função bijetora – generalizada pela noção de isomorfismo.

2.3.1.1 MONOMORFISMO

Motivações em SET:

Definição 2.11 (Função Injetiva) Uma função $f: A \longmapsto B$ é injetiva se, somente se, para todo $\{x1, x2\}$ A temos: se $f(x1) \neq f(x2)$, então $x1 \neq x2$. Mas, se para todo $\{x1, x2\}$ A ocorre $f(x1) = f(x2)$, uma vez que $x1 = x2$.

Proposição 2.10 Uma função $f: A \longmapsto B$ é injetiva se, somente se, para todo par de "funções paralelas" $g, h: C \rightrightarrows A$, $f \circ g = f \circ h$, temos $g = h$ (uma função f é injetiva se houver cancelamento à esquerda).

Demonstração:

Sejam os diagramas

$$
\begin{tikzcd}
A \arrow[r, "f"] & B \\
C \arrow[u, shift left, "h"'] \arrow[u, shift right, "g"] \arrow[ur, "f\circ h=f\circ g"'] &
\end{tikzcd}
$$

, isto é,

$$
\begin{tikzcd}
C \arrow[r, "h"] \arrow[d, "g"'] & A \arrow[d, "f"] \\
A \arrow[r, "f"'] & B
\end{tikzcd},
$$

e $f: A \longmapsto B$ uma função injetiva. As funções $g, h: C \rightrightarrows A$ são tais que $f \circ g =$ $f \circ h$. Vamos provar que $g = h$.

Se x C e ambas as funções g e h têm domínio em C, então $f \circ g = f \circ h$. Por conseguinte, $(f \circ g)(x) = f(g(x)) = f(h(x))$. Como f é injetiva $g(x) = h(x)$, $g = h$.

Por outro lado, vamos provar que para $\{x_1, x_2\}$ A, se temos $f(x_1) = f(x_2)$, então $x_1 = x_2$.

Definirmos g, h de um conjunto $C = \{*\}$, tal que $g,h: \{*\} \rightrightarrows A$. Vamos agora supor que f e g convertem os elementos de C em x_1 e x_2, de forma que $g(*) = x_1$ e $h(*) = x_2$.

A hipótese $f(x_1) = f(x_2)$ pode ser escrita na forma $f(g(*)) = f(h(*))$. Dessa expressão, obtemos $f \circ g(*) = f \circ h(*)$ e $f \circ g = f \circ h$.

Pela hipótese da proposição, concluímos que $g = h$. Logo, $g(*) = h(*)$, isto é, $x_1 = x_2$.

$\square$

Definição 2.13 (Monomorfismo) Um morfismo $f: A \longrightarrow B$ em categoria qualquer $\mathscr{C}$ é um monomorfismo se para todo par de "morfismos paralelos" $g,h: C \rightrightarrows A$, tal que $f \circ g = f \circ g$ implica $g = h$ (f cancelável à esquerda). Notação: f:

$A \rightarrowtail B$.

Exemplo em SET:

Na categoria dos números naturais $SET^{\mathbb{N}}$ os morfismos são monomorfismos, pois se $m + n = m + p$, então $n = p$ (m cancelável à esquerda).

2.3.1.2 EPIMORFISMO

Motivações em SET:

Definição 2.14 (Função Sobrejetiva) Uma função $f: A \longmapsto B$ é sobrejetiva se, somente se, $Im\,(f) = CD\,(f)$, isto é, para todo y B, então existe x A tal que $f(x) = y$.

Proposição 2.12 Uma função $f: A \longmapsto B$ é sobrejetiva se, somente se, para todo par de "funções paralelas" do tipo g,h: $B \rightrightarrows C$, tal que $f \circ g = f \circ g$ implica $g = h$ (uma função f é sobrejetiva se houver cancelamento à direita).

Demonstração:

Sejam os diagramas

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "g\circ f = h\circ f"'] & B \arrow[d, shift right, "g"'] \arrow[d, shift left, "h"] \\ & C \end{tikzcd}$$

, isto é,

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "f"'] & B \arrow[d, "g"] \\ B \arrow[r, "h"'] & C \end{tikzcd},$$

f: *A* $\longmapsto$ *B* e *g*,*h*: *B* $\rightrightarrows$ *C* são funções que comutam $g \circ f = h \circ f$. Queremos provar que $g = h$, isto é, para todo *x B*, $g(x) = h(x)$.

Se *x B* e *f* é sobrejetiva, então existe *z A,* tal que $f(z) = x$. Logo, escrevemos $g(x) = g(f(z)) = (g \circ f)(z)$. Mas, por hipótese, $(g \circ f)(z) = (h \circ f)(z) = h(f(z)) = h(x)$.

Por outro lado, como *x* A e *y B*, tais que $f(x) = y$, devemos provar que se $g = h$, então $g \circ f = h \circ f$.

Definimos *g*, *h* para certo conjunto C = {$*$}, de forma que *g*,*h*: *B* $\longmapsto$ {$*$}. Vamos supor que *f* e *g* convertem os elementos de *B* em $*_1$ e $*_2$, logo temos:

$f(x) = y$;

2. $h(y), g(y) = \begin{cases} g(y) = *_1 \\ h(y) = *_2 \end{cases}$

Se $g = h$ ocorre, então $*_1 = *_2$. Por conseguinte, a hipótese anterior pode ser escrita na forma $g(y) = h(y)$, ou seja, se $g(f(x)) = h(f(x))$, então $(g \circ f)(x) = (h \circ f)(x)$. Pela hipótese da proposição, concluímos que $g \circ f = h \circ f$.

$\square$

Definição 2.15 (Epimorfismo) Um morfismo $f: A \longmapsto B$ em categoria qualquer $\mathscr{C}$ é um epimorfismo se para todo par de "morfismos paralelos" do tipo $g,h: B \rightrightarrows C$, implica $g = h$ (f cancelável à direita). Denotação: $f: A \twoheadrightarrow B$.

Exemplo em SET:

Na categoria dos números naturais SET$^{\mathbf{N}}$ os morfismos são epimorfismos, pois como $n + m = p + m$, então $n = p$ (m cancelável à direita).

2.3.1.3 ISOMORFISMO

Motivação em SET:

Definição 2.16 (Função Bijetiva) Uma função $f: A \longmapsto B$ é bijetiva se, somente se, verificamos:

(1) se para todo y B, então existe x A tal que $f(x) = y$;

(2) se $f(x1) \neq f(x2)$, *então* $x1 \neq x2$ *para todo* $\{x1, x2\}$ A.

Proposição 2.13 Uma função $f: A \longmapsto B$ é bijetiva se, somente se, existe $g: B \longmapsto A$ tal que $f \circ g = idB$ e $g \circ f = idA$.

Demonstração:

Sejam os diagramas

id *g* *id*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "id_A"'] & B \arrow[d, "g"] \\ & A \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] & B \\ B \arrow[u, "g"] \arrow[ur, "id_B"'] & \end{tikzcd}$$

$$g \circ f = id_A \qquad\qquad f \circ g = id_B\,.$$

Como *f: A* $\longmapsto$ *B* é bijetiva, temos:

1. como *f é* uma função, para todo *x A* e existe um único *y* B, temos *f(x) = y*;

2. como *f* é bijetiva, todo *y B* e existe (pois é sobrejetiva) um único (pois é injetiva) *x A* tal que *g(y) = x*. Logo, *g(y) = x* se, e somente se *f(x) = y*.

Se *y B, (f* $\circ$ *g)(y) = f(g(y))=f(x) = y = idB(y)*, então *f* $\circ$ *g = idB*. Do mesmo modo, *(g* $\circ$ *f) (x) = g (f (x)) = g(y) = x = idA*. Portanto, *g* $\circ$ *f = idA*.

Lema 2.1 (Unicidade de g) *g = g'*, se, e somente se, *g'* (uma função inversa) satisfaz as seguintes propriedades: (1) *g'* $\circ$ *f = idA* e (2) *f* $\circ$ *g' = idB*.

Demonstração:

Para qualquer *y* B, com *y = f(x)*, segue *g'(y) = g'(f(x)) = (g'* $\circ$

$f)\ (x) = idA\ (x) = x$. Além do mais, se $g(y) = g(f(x)) = (g \circ f)\ (x) = idA\ (x) = x$, então $g = g'$. Ou seja, temos $g' = idA \circ g' = (g \circ f) \circ g' = g \circ (f \circ g') = g \circ idB = g$. Sendo g' única, g' é chamada "inversa de f" e é denota por f^{-1}. Logo, f^{-1} satisfaz $f^{-1} \circ f = idA$ e $f \circ f^{-1} = idB$.
□

Por outro lado, devemos provar que f é bijetiva, ou seja, que f é *monomorfismo* e *epimorfismo*.

1. f é monomorfismo se, somente se, dado $f \circ g = f \circ h$, temos $g = h$. Compondo f^{-1} a ambos os membros, temos a equação $f^{-1} \circ (f \circ g) = f^{-1} \circ (f \circ h)$. Pela associatividade, $(f^{-1} \circ f) \circ g = (f^{-1} \circ f) \circ h$. Já pela identidade, segue $idA \circ g = idA \circ h$. Com isso, concluímos que $g = h$.

2. f é epimorfismo se, somente se, dado $g \circ f = h \circ f$, temos $g = h$. Compondo f^{-1} a ambos os membros, obtemos $(g \circ f) \circ f^{-1} = (h \circ f) \circ f^{-1}$. Pela associatividade, temos $g \circ (f \circ f^{-1}) = h \circ (f \circ f^{-1})$. Já pela identidade, segue $g \circ idB = h \circ idB$. Dado o exposto, concluímos que $g = h$.

Conforme os passos 1 e 2, provamos que f é bijetiva.
□

Definição 2.17 (Definição de Isomorfismo) Um morfismo $f\colon A \longrightarrow B$ em uma categoria qualquer $\mathscr{C}$ é um isomorfismo se existe um morfismo $f^{-1}\colon B \longrightarrow A$ tal que $f^{-1} \circ f = idA$ e $f \circ f^{-1} = idB$. Notações: $f\colon A \cong B$ ou $f\colon A \rightarrowtail\!\!\twoheadrightarrow B$.

Exemplo em SET:

Na categoria dos números naturais $SET^{\mathbb{N}}$ os morfismos são monomorfismos e epimorfismos. Nessa categoria, para $m + n = 0$, isto é, $m \circ n = id_{\mathbb{N}}$ há um inverso para m, por definição n. Como m e n apenas admitem números naturais, então $m = n = 0$. Logo, o morfismo $0: \mathbb{N} \longrightarrow \mathbb{N}$ é o único isomorfismo na categoria $SET^{\mathbb{N}}$.

Exemplo em POSET:

Em uma POSET, se o seu morfismo $f: p \longrightarrow q$ admite o inverso f -1: $q \longrightarrow p$, então $p \leq q$ e $q \leq p$, isto é, pela antissimetria, temos $p = q$. No entanto, sendo f único, temos $idp: p \longrightarrow p$. Aqui, todo morfismo é monomórficos e epimórficos, mas apenas os morfismos identidades são isomórficos.

2.3.2 OBJETO INICIAL E OBJETO TERMINAL

Nesta subseção vamos estudar as construções categóricas de *objeto inicial* e *objeto terminal*. Motivamos as demonstrações das proposições sugeridas nas seguintes noções da teoria dos conjuntos: 1. *conjunto vazio* – conceito generalizado pela definição categórica de objeto inicial; e 2. *conjunto unitário* – conceito generalizado pela definição categórica de objeto terminal.

Definição 2.18 (Objeto Inicial) Seja 0 um objeto inicial de uma categoria qualquer $\mathscr{C}$, para um único objeto *a Obj* ($\mathscr{C}$) existe um único morfismo denotado *!o: o* $\longrightarrow$ *a*.

Motivação em SET:

Proposição 2.14 *A* é objeto inicial em SET se, somente se, $A = \emptyset$.

Exercício 2.5 Prove a **Proposição 2.14**

Exemplo em Álgebra de Boole:

Definição 2.19 Seja *A* um conjunto não vazio. Uma pré-ordem em *A* é uma relação binária $\leq$ definida em *A* que satisfaz as seguintes condições:

(1) $\leq$ é reflexiva, isto é, $p \leq p$, para todo *p A;*

(2) $\leq$ é transitiva, isto é, se $p \leq q$ *e* $q \leq r$, então $p \leq r$, para todo {*p, q, r*} *A*.

Na pré-ordem $\langle A, \leq \rangle$, um objeto inicial é um elemento o A com $o \leq x$ para todo *x* A. O objeto inicial equivale na álgebra de Boole $\mathscr{B}$ ao *minimum,* no qual para todo *x* em **B**, temos $o \leq x$.

Na álgebra de Boole o *minimum* é teorema. Podemos prová-lo da seguinte forma: se *x* e *y* são elementos de uma álgebra de Boole, dizemos que $x \geq y$ se, somente se, $x \sqcap y = y$.

Como, pelo $Ax_{\mathscr{B}}$ 5, se vale $x \sqcap 0 = 0$, então $0 \leq x$ ocorre.

$\square$

Definição 2.20 (Objeto Terminal) Seja 1 um objeto terminal de uma categoria qualquer $\mathscr{C}$, para um único objeto *a* *Obj* ($\mathscr{C}$) existe um único morfismo do tipo $!1: a \longrightarrow 1$.

Motivações em SET:

Proposição 2.15 *A* é objeto terminal em SET se, somente se, A é um conjunto unitário, isto é, $A = \{*\}$.

Demonstração:

Seja $A = \{*\}$ e *B* um conjunto qualquer, consideremos os seguintes casos:

$B = \emptyset$, então existe uma única função $f: B \longmapsto A$ que é a função vazia;

$B \neq \emptyset$, então existe uma única função $f: B \longmapsto \{*\}$, isto é, a função constante $f(z) = *$ para todo z B.

Por outro lado, tratemos dos seguintes casos:

Se $A = \emptyset$, então *A* só admite uma função com domínio vazio. Nesse caso, essa função seria $\emptyset: \emptyset \longmapsto \emptyset$ e, assim, *A* não seria objeto terminal;

Por outro lado, se existem *x, y A,* tal que $x \neq y$, presumimos que dado qualquer conjunto $B \neq \emptyset$, podemos definir, pelo menos, duas funções distintas *f, g: B* $\longmapsto$ *A*. Logo, *A* não seria objeto terminal.

Conforme o exposto, *A* é um conjunto unitário e, portanto, um objeto terminal.

$\square$

Exemplo em Álgebra de Boole:

Na pré-ordem $\langle A, \leq \rangle$, um objeto terminal é um elemento *1* *A* que satisfaz $x \leq 1$ para todo *x A*. O objeto terminal equivale na álgebra de Boole $\mathscr{B}$ ao *maximum*, no qual para todo *x* em **B**, temos $x \leq 1$.

Na álgebra de Boole o *maximum* é teorema. Podemos prová-lo da seguinte forma: se *x* e *y* são elementos de uma álgebra de Boole, dizemos que $x \leq y$ se, somente se, $x \sqcup y = y$. Como, pelo $\mathbf{Ax}_{\mathscr{B}}$ 6, vale $x \sqcup 1 = 1$, segue $x \leq 1$. $\square$

2.3.3 PRODUTO E COPRODUTO

Nesta subseção introduzimos os conceitos de produto e coproduto. Motivamos as demonstrações das proposições sugeridas nas seguintes noções da teoria dos conjuntos: 1. *produto cartesiano* ($A \times B$) – conceito generalizado pela noção de *produto*; e 2. *união disjuntiva* ($A + B$) – conceito generalizado pela noção de *coproduto*.

2.3.3.1 PRODUTO

Construção em SET:

Definição 2.21 (Produto Cartesiano) Dados dois conjuntos A e B, o produto cartesiano de A e B é definido como

$A \times B = \{(x, y) \mid x \in A \; e \; y \in B\}$.

Proposição 2.16 No produto cartesiano $A \times B$ as projeções $pA: A \times B \longmapsto A$ e $pb: A \times B \longmapsto B$ fatoraram o par de funções $f: C \longmapsto A$ *e* $g: C \longmapsto B$. A projeção $p: C \longmapsto A \times B$ existe e é única, tal que o diagrama

$$\begin{tikzcd} & C \arrow[dl, "f"'] \arrow[d, dashed, "p"] \arrow[dr, "g"] & \\ A & A \times B \arrow[l, "p_A"] \arrow[r, "p_B"'] & B \end{tikzcd}$$

comuta, isto é, $f = pA \circ p$ *e* $g = pB \circ p$.

Demonstração:

As funções pA e pB que permitem a fatoração indicada são projeções do tipo:

$$\begin{aligned} p_A : A \times B &\longmapsto A \\ (x, y) &\longmapsto x \end{aligned} \qquad \begin{aligned} p_B : A \times B &\longmapsto B \\ (x, y) &\longmapsto y\,. \end{aligned}$$

Vamos demonstrar que *pA* e *pB* têm a propriedade da fatoração. As funções $f: C \longmapsto A$ e $g: C \longmapsto B$ podem ser fatoradas através de *pA* e *pB* mediante uma única projeção *p*.

Definidas $f: C \longmapsto A$ e $g: C \longmapsto B$, segue:

1. Existência da projeção *p*;

Observado o exposto, obtemos:

$$\begin{aligned} p : C &\longmapsto A \times B \\ x &\longmapsto \langle f(x), g(x) \rangle. \end{aligned}$$

Dado $(pA \circ p)(x) = pA(p(x)) = pA(f(x), g(x)) = f(x)$, para todo x *de* C, temos o seguinte $pA \circ p = f$. A função *p*, tal como definida, permite a fatoração desejada.

2. Unicidade da projeção *p*.

Supondo outra função $q: C \longmapsto A \times B$ que faz comutar o diagrama. Vamos provar que $q = p$, isto é, para todo x de C, $p(x) = q(x)$, temos

$$\begin{aligned} q : C &\longmapsto A \times B \\ x &\longmapsto (q_1(x),\ q_2(x)). \end{aligned}$$

Se o diagrama acima comuta, podemos escrever $(q1(x)) = pA(q1(x), q2(x)) = pA(q(x)) = (pA \circ q)(x) = f(x)$. Por outro lado, $(q2(x)) = pB(q1(x), q2(x)) = pB(q(x)) = (pB \circ q)(x) = g(x)$. Por conseguinte, $q(x) = (q1(x), q2(x)) = (f(x), g(x)) = p(x)$.

Portanto, a função $p: C \longmapsto A \times B$ existe e é única no produto cartesiano $A \times B$.

$\square$

Definição 2.22 (Produto) Seja $\mathscr{C}$ uma categoria qualquer e *a, b* e *c* objetos de $Obj(\mathscr{C})$, um produto de *a e b* é um objeto em $\mathscr{C}$ denotado $a \times b$, o qual admite dois morfismos do tipo $pa{:}a \times b \longrightarrow a$ e $pb{:}\ a \times b \longrightarrow b$, tais que para qualquer *c*, dado $f{:}\ c \longrightarrow a$ e $g{:}\ c \longrightarrow b$, *existe* um único morfismo $p{:}\ c \longrightarrow a \times b$ que comuta o diagrama

$$\begin{tikzcd}
 & c \arrow[dl, "f"'] \arrow[d, dashed, "p"] \arrow[dr, "g"] & \\
a & a \times b \arrow[l, "p_a"] \arrow[r, "p_B"'] & b
\end{tikzcd},$$

isto é, $f = pa \circ p$ e $g = pa \circ p$.

Proposição 2.17 Seja D um conjunto para o qual existe a função $p{:}\ D \longmapsto A$ e a função $q{:}\ D \longmapsto B$ que satisfazem a propriedade de fatoração, dizemos D e $A \times B$ como isomórficos, de forma que denotamos $D \cong A \times B$.

Demonstração:

Consideremos o seguinte diagrama

$$
\begin{tikzcd}
 & D \arrow[dl, "p"'] \arrow[dr, "q"] \arrow[d, dashed, "p\times q"] & \\
A & A\times B \arrow[l, "p_A"] \arrow[r, "p_B"'] \arrow[d, dashed, "p_A\times p_B"] & B \\
 & D \arrow[ul, "p"] \arrow[ur, "q"'] &
\end{tikzcd}
.
$$

O diagrama acima é a justaposição dos seguintes diagramas:

$$
\begin{tikzcd}
 & D \arrow[dl, "p"'] \arrow[dr, "q"] \arrow[d, dashed, "p\times q"] & \\
A & A\times B \arrow[l, "p_A"] \arrow[r, "p_B"'] & B
\end{tikzcd}
\qquad
\begin{tikzcd}
A & A\times B \arrow[l, "p_A"'] \arrow[r, "p_B"] \arrow[d, dashed, "p_A\times p_B"] & B. \\
 & D \arrow[ul, "p"] \arrow[ur, "q"'] &
\end{tikzcd}
$$

(I) (II)

1. (I) é consequência de supor $A \times B$ como o produto de A e B;

2. (II) é consequência de supor D como o produto de A e B, considerando $A \times B$ como um domínio qualquer.

Como $p \times q$ e $pA \times pB$ são únicas, a composta $(pA \times pB) \circ (p \times q)$ é também única e vai de D em D e, assim, coincide com idD. Portanto, $(pA \times pB) \circ (p \times q)= idD$.

Analogamente, $(p \times q) \circ (pA \times pB) = idA \times B = idD$. Por conseguinte, $p \times q: D \longmapsto A \times B$ é um isomorfismo. Ao final, concluímos $D \cong A \times B$.

$\square$

Exemplo em Álgebra de Boole:

Definição 2.23 Seja A um conjunto não vazio, uma ordem parcial em *A* é uma relação binária $\leq$, definida em A, que satisfaz as seguintes condições:

(1) $\leq$ é reflexiva, isto é, $p \leq p$, para todo p A;

(2) $\leq$ é transitiva, isto é, se $p \leq q$ e $q \leq r$, então $p \leq r$, para todo p, q, r A;

(3) $\leq$ é antissimétrica, isto é, se $s \leq t$ e $s \leq t$, então $s = t$, para todo s, t A.

Proposição 2.18 O produto $p \times q$ coincide com o ínfimo $p \sqcap q$ quando tomamos $\langle A, \leq \rangle$, tal que p A, uma ordem parcial, como um *POSET*.

EXERCÍCIO 2.6 PROVE A **PROPOSIÇÃO 2.18**

2.3.3.2 COPRODUTO

Definição 2.24 (Coproduto) Seja $\mathscr{C}$ uma categoria qualquer e *a*, *b* e *c* objetos de $Obj(\mathscr{C})$, um coproduto de *a* e *b* é um objeto em $\mathscr{C}$ denotado *a* + *b*, com dois morfismos do tipo *ia: a* + *b* $\longrightarrow$ *A e ib: a* + *b* $\longrightarrow$ *b*, tais que para qualquer *c*, dado *f: a* $\longrightarrow$ *c* e *g: b* $\longrightarrow$ *c*, existe um único morfismo *q: a* + *b* $\longrightarrow$ *c* que comuta o diagrama

$$\begin{tikzcd}
a \arrow[r, "i_a"] \arrow[dr, "f"'] & a+b \arrow[d, dashed, "q"] & b \arrow[l, "i_b"'] \arrow[dl, "g"] \\
& c &
\end{tikzcd},$$

isto é, $f = q \circ ia$ e $g = q \circ ib$.

Motivação em SET:

Definição 2.25 (União Disjunta) Dados dois conjuntos *A e B,* a união disjunta de *A* e *B* é definida como

$$A+B=\{(x,1)\mid x\in A\ \cup\ (y,0)\mid y\in B\}.$$

Proposição 2.19 Seja *A* e *B* dois conjuntos quaisquer, o coproduto de *A* e *B* em *SET* é a união disjunta de *A* e *B*, isto é, *A* + *B*.

Exercício 2.7 Provar a **Proposição 2.19**

Exemplo em Álgebra de Boole:

Proposição 2.20 A noção de coproduto $p + q$ coincide com o supremo $p \sqcup q$ quando tomamos $\langle A, \leq \rangle$, tal que $p, q\ A$, uma ordem parcial, como um POSET.

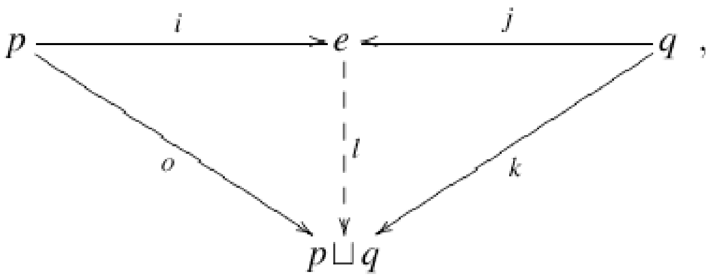
Demonstração:

O *supremo* é uma noção de ordem. Observados os dois elementos p e q, denotamos o *supremo* de p e q como $\mathrm{p} \sqcup \mathrm{q} = sup\{\mathrm{p}, \mathrm{q}\}$.

Temos $p + q$ como coproduto de p e q se existe um morfismo $m: q \longrightarrow p + q$ e um monomorfismo $n: p \longrightarrow p + q$, tais que para $i: p \longrightarrow e$ e $j: q \longrightarrow e$ existe um único morfismo $h: p + q \longrightarrow e$; e o diagrama a seguir comuta

$$\begin{tikzcd}
p \arrow[r, "m"] \arrow[dr, "i"'] & p+q \arrow[d, dashed, "h"] & q \arrow[l, "n"'] \arrow[dl, "j"] \\
& e\,. &
\end{tikzcd}$$

Em POSET, temos os morfismos: $m: p \leq p + q$; $n: q \leq p + q$; $h: p + q \leq e$; $i: p \leq e$; $j: q \leq e$. Os morfismos m e n podem ser escritos na forma $m: (p + q) \sqcup p = p + q$ e $n: (p + q) \sqcup q = p + q$. Ao acrescentarmos o termo '$\sqcup$q' a ambos os membros da expressão anterior, obtemos: dado $(p + q \sqcup p) \sqcup q = (p + q) \sqcup q$, e ao final $(p + q) \sqcup (p \sqcup q) = (p + q) \sqcup q$. O último membro dessa equação equivale à expressão anterior de n, logo: $(p + q)$



$\sqcup$ 1).

Po

observamos o morfismo $l: e \leq p \sqcup q$. Pela transitiva de l e h, temos $p + q \leq p \sqcup q$ (2). Portanto, conforme as equações (1) e (2) dizemos que $p + q$ é o *supremo* de p e q, isto é, $p + q = p \sqcup q$. $\square$

2.3.4 EQUALIZADORES

Motivação em SET:

Para um par de funções $f, g: A \rightrightarrows B$ em SET, podemos admitir D como um subconjunto de A, tal que $D = \{x \mid x \; A$ e $f(x) = g(x)\}$. A função injetiva $i: D \rightarrowtail A$ é chamada de equalizador de f e g, de modo que $f \circ i = g \circ i$.

Se $h: C \longrightarrow A$ é algum outro tipo de equalizador de f e g, então $f \circ h = g \circ h$. Em gráfico, temos:

$$\begin{tikzcd}
C \arrow[dr, dashed, "k"] \arrow[drr, bend left, "h"] \arrow[ddr, bend right, "h"'] & & \\
& D \arrow[r, tail, "i"] \arrow[d, "i"'] & A \arrow[d, "g"] \\
& A \arrow[r, "f"'] & B ,
\end{tikzcd}$$

como h que "fatora" unicamente $i: D \longrightarrow A$, e a função $k: C \longrightarrow A$ tal que $i \circ k = h$.

Definição 2.26 (Equalizador) Seja $\mathscr{C}$ uma categoria qualquer e i, f, g morfismos de $Hom\ (\mathscr{C})$, o morfismo $i: e \longrightarrow a$ é um equalizador dos morfismos $f, g: a \longrightarrow b$ em $\mathscr{C}$ se, somente se, satisfaz as seguintes propriedades:

(1) comuta o seguinte diagrama

$$
\begin{tikzcd}
d \arrow[dr, dashed, "k"] \arrow[drr, bend left, "h"] \arrow[ddr, bend right, "h"'] & & \\
& e \arrow[r, "i"] \arrow[d, "i"'] & a \arrow[d, "g"] \\
& a \arrow[r, "f"'] & b ,
\end{tikzcd}
$$

isto é, $g \circ i = f \circ i$;

(2) garante a existência de um único morfismo $k: c \longrightarrow e$, tal que $i \circ k = h$.

Exemplo:

Sejam f,g: $\mathbb{R}^2 \longmapsto \mathbb{R}$ as funções $f(\langle x, y\rangle) = x^2 + y^2$ e $g(\langle x, y\rangle) = 1$, tais que para todo $\langle x, y\rangle \in \mathbb{R}^2$. Isto é,

$$
\begin{tikzcd}
e \arrow[r, "i"] \arrow[d, "i"'] & \mathbb{R}^2 \arrow[d, "x^2+y^2"] \\
\mathbb{R}^2 \arrow[r, "1"'] & B.
\end{tikzcd}
$$

Temos $f(\langle x, y\rangle) \circ i = g(\langle x, y\rangle) \circ i$ de forma que $i(f(\langle x, y\rangle)) = i(g(\langle x, y\rangle))$. Se $g(\langle x, y\rangle) = 1$, então $i(1) = i(f(\langle x, y\rangle)$. Ao supormos $i(x) = x$ como uma função constante, podemos escrever $x2+y2 = 1$.

Portanto, o objeto resultante do equalizador de f e g é o subconjunto de $\mathbb{R}^2$ que constitui a circunferência de raio 1, ou seja, é o conjunto de todos os pares $\langle x, y\rangle \in \mathbb{R}^2$.

Proposição 2.21 Para uma categoria qualquer $\mathscr{C}$, se $i: e \longrightarrow a$ é um equalizador de $f, g: a \longrightarrow b$, então '$i$' é um monomorfismo.

Demonstração:

Devemos provar que se $i \circ u = i \circ v$, então $u = v$. Dado o diagrama

$$\begin{tikzcd}
c \arrow[dr, shift left, "u"] \arrow[dr, shift right, "v"'] & & \\
& e \arrow[r, "i"] \arrow[d, "i"'] & a \arrow[d, "g"] \\
& a \arrow[r, "f"'] & b
\end{tikzcd},$$

em $u, v: c \longrightarrow e$, temos $i \circ u = i \circ v$. Existe um único $k: c \longrightarrow e$ de forma que $i \circ v = i \circ k$. Pela unicidade de k, segue $v = k$ e, consequentemente, por uma análise semelhante, $k = u$. Logo, $u = v$, o que implica 'i' como monomorfismo.

□

Proposição 2.22 Para uma categoria qualquer $\mathscr{C}$, todo equalizador que seja epimorfismo é um isomorfismo.

Exercício 2.8 Prove a **Proposição 2.22**

2.3.5 Coequalizadores

Definição 2.27 (Coequalizadores) Seja $\mathscr{C}$ uma categoria qualquer e *q, f e g* morfismos de *Hom* ($\mathscr{C}$), o morfismo *i: e* $\longrightarrow$ *a* é um coequalizador dos morfismos *f, g: a* $\longrightarrow$ *b em* $\mathscr{C}$ se, somente se, satisfaz as seguintes propriedades:

(1) comuta o seguinte diagrama

$$\begin{tikzcd}
a \arrow[r, "g"] \arrow[d, "f"'] & b \arrow[d, "q"] \arrow[ddr, bend left, "p"] & \\
b \arrow[r, "q"'] \arrow[drr, bend right, "p"'] & d \arrow[dr, dashed, "h"] & \\
& & e
\end{tikzcd},$$

ou seja, $q \circ f = q \circ g$;

(2) garante a existência de um único morfismo *h: d* $\longrightarrow$ *e,* tal que $h \circ q = p$.

Proposição 2.23 Em $\mathscr{C}$, se *h: b* $\longrightarrow$ *d* é um coequalizador de $f, g: a \longrightarrow b$, então h é um epimorfismo.

Demonstração:

Vamos provar o seguinte: se $u \circ h = v \circ h$, então $u = v$. Dado o diagrama a seguir

$$\begin{tikzcd}
a \arrow[r, "g"] \arrow[d, "f"'] & b \arrow[d, "h"] & \\
b \arrow[r, "h"'] & d \arrow[dr, bend left, "u"] \arrow[dr, bend right, "v"'] & \\
& & e
\end{tikzcd},$$

temos $u,v: d \longrightarrow e$, tal que $u \circ h = v \circ h$. Existe um único $k: d \longrightarrow e$ de modo que $v \circ = k \circ h$. Segundo a unicidade de h, $v = k$ e $k = u$. Logo, $u = v$, o que implica afirmar que h é epimorfismo.

□

Exemplo em SET:

Em SET, uma relação de equivalência traduz bem o "funcionamento" de um coequalizador. Vejamos.

Definição 2.28 (Relação de Equivalência) Uma relação R num conjunto A é um subconjunto R *de* $A \times A$. Uma relação R é chamada relação de equivalência, se e somente se, satisfaz as seguintes condições:

(1) Para todo $x\ A$, $(x, x)\ R$;

(2) Se para todo $x, y\ A$, $(x, y)\ R$, então $(y, x)\ R$;

(3) Se para todo $x,y,z\ \ A$, $(x, y)\ \ R$ *e* $(y, z)\ \ R$, então $(x, z)\ \ R$.

R é uma relação de equivalência se, somente se, for reflexiva, simétrica e transitiva.

Se R é uma relação de equivalência em A, então a classe de equivalência de qualquer elemento $x\ \ A$, representada por $[x]$, é o conjunto de elementos com os quais x está em relação:

$[x] = \{y \mid (x, y)\ R\}$, ou seja, $[x] = \{y \mid xRy\}$.

Por intemédio da relação R, podemos construir o conjunto quociente A/R que é a coleção de todas as classes de equivalência quando x percorre A:

$A/R = \{[x] \mid x \ A\}$.

O conjunto quociente possui as seguintes propriedades:

Teorema 2.2 Seja R uma relação de equivalência em A *e* $[x]$ a classe de equivalência de $x \ A$, então:

(1) $x \ A$ para todo $[x] \ A$;

(2) $[x] = [y]$ se, somente se, $\langle x, y \rangle \ R$, ou seja, xRy;

(3) *Se* $[x] \neq [y]$, então $[x]$ *e* $[y]$ são disjuntas, isto é, $[x] \ [y] \neq \emptyset$.

Exercício 2.9 Prove o **Teorema 2.2**

As classes de equivalência formam uma partição disjunta do conjunto A, de forma que ao conjunto quociente A/R está associado a seguinte função: $fR: A \longmapsto A/R$, dada por $fR(x) = [x]$, para todo $x \ A$. É perceptível que fR é sempre sobrejetiva. Em razão disso é chamada de "projeção canônica" (cada x é projetado sobre sua classe de equivalência).

Proposição 2.24 Seja A um conjunto qualquer, R uma relação de equivalência em A e $p1, p2: R \longmapsto A$, representadas pelas funções $p_1(x,y) = x$ e $p_2(x, y) = y$, concluímos que $f_R: A \longmapsto A/R$ é um coequalizador de p_1 *e* p_2.

Demonstração:

Consideremos o seguinte diagrama

$$\begin{tikzcd}
R \arrow[r, "p_1"] \arrow[d, "p_2"'] & A \arrow[d, "f_R"] \\
A \arrow[r, "f_R"'] & A/_R .
\end{tikzcd}$$

Temos $(x, y)\ R$, ou seja, xRy. *É* fácil notar que isso implica em $[x] = [y]$. Consequentemente, $(f_R \circ p_1)(x, y) = f_R(p_1(x, y)) = f_R(x) = [x] = [y] = f_R(y) = f_R(p_2(x, y)) = (f_R \circ p_2)(x, y)$. Ou seja, f_R equaliza p_1 e p_2.

Para verificar se f_R existe e é única, vamos supor que outra função, por exemplo, h faz o mesmo que f_R, isto é, $h \circ p_1 = h \circ p_2$. Observado o diagrama

$$\begin{tikzcd}
R \arrow[r, "p_1"] \arrow[d, "p_2"'] & A \arrow[d, "f_R"] \arrow[ddr, bend left, "h"] & \\
A \arrow[r, "f_R"'] \arrow[drr, bend right, "h"'] & A/_R \arrow[dr, dashed, "k"] & \\
 & & B,
\end{tikzcd}$$

devemos definir k: $A/R \longmapsto B$, tal que $h = k \circ fR$ e k como única. Disso segue que $k([x]) = h(x)$. Temos que determinar ainda se k está bem definida, isto é, se k independe dos representantes quando $[x] = [y]$, ou seja, $h(x) = h(y)$.

Se $[x] = [y]$, então $(x, y)\ R$. Logo, $h(x)=h(p1(x, y))=(h \circ p1)(x, y)=(h \circ p2)(x, y)=h(p2(x, y))=h(y)$. Por conseguinte, temos $k \circ fR = h$; $(k \circ fR)(x) = k(fR(x)) =$ $k([x])= h(x)$.

Por fim, resta-nos provar se k é única. Ao supor que l: $A/R \longmapsto B$, de forma que $h = l \circ fR$, provamos $l = k$; $l([x]) = l(fR(x)) = (l \circ fR)(x) = h(x) = k(x)$. Conclusão: k é única. $\square$

2.3.6 PULLBACKS

Definição 2.29 (Pullback) Seja $\mathscr{C}$ uma categoria qualquer e *k, f, g, f ' e g'* morfismos de *Hom* ($\mathscr{C}$), um pullback de *f* e *g* com codomínio em comum ocorre se, somente se, os morfismos *f ' e g'* satisfazem as seguintes propriedades:

(1) comutam o seguinte diagrama

$$
\begin{tikzcd}
e \arrow[dr, dashed, "h"] \arrow[drr, bend left, "j"] \arrow[ddr, bend right, "i"'] & & \\
& d \arrow[r, "g'"] \arrow[d, "f'"'] & b \arrow[d, "f"] \\
& a \arrow[r, "g"'] & c ,
\end{tikzcd}
$$

ou seja, $f \circ g' = g \circ f'$;

(2) garantem a existência de um único $h: e \longrightarrow d$, tal que $f' \circ h = i$ e $g' \circ h = j$.

Exemplo em SET:

Dada a função $f: A \longmapsto B$ *e* C um subconjunto de B *(isto é,* $C \subseteq B$*)*, conforme a teoria dos conjuntos, podemos definir a imagem inversa de C sobre f da seguinte forma $f -1(C) = \{ x\ A \mid f(x)\ C\}$. Em teoria das categorias, o diagrama

$$
\begin{tikzcd}
f^{-1}(C) \arrow[r, "f^*"] \arrow[d, "id_{f^{-1}(C)}"'] & C \arrow[d, "id_C"] \\
A \arrow[r, "f"'] & B
\end{tikzcd}
$$,

descreve tal situação.

Assim, *f −1 (C)* pode ser construída como um pullback, desde que cumpra com as seguintes propriedades:

(1) Comuta o diagrama anterior. Temos *idC* ∘ *f* = *f* ∘ $id_{f^{-1}(C)}$. Logo, *x f −1(C)*, então *(idC* ∘ *f)(x) = idC (f(x)) = f(x) =* $f(id_{f^{-1}(C)}(x)) = (f \circ id_{f^{-1}(C)})(x)$;

(2) Garante que E existe e é único. No seguinte diagrama

$$
\begin{tikzcd}
E \arrow[r, "k"] \arrow[d, "h"'] & C \arrow[d, "id_C"] \\
A \arrow[r, "f"'] & B ,
\end{tikzcd}
$$

devemos construir o morfismo *h: E* $\longmapsto$ *f −1(C)* como único, tal que o seguinte diagrama

$$
\begin{tikzcd}
E \arrow[dr, dashed, "l"] \arrow[drr, bend left, "k"] \arrow[ddr, bend right, "h"'] & & \\
& f^{-1}(C) \arrow[r, "f^*"] \arrow[d, "id_{f^{-1}(C)}"'] & C \arrow[d, "id_C"] \\
& A \arrow[r, "f"'] & B ,
\end{tikzcd}
$$

comute, isto é, $id_{f^{-1}(C)} \circ l = h$ e $f^* \circ l = k$.

Seja *x E,* tal que *l(x) f −1(C), (f* ∘ h) (x) = (idC ∘ k) (x),* isto é, *f*(h(x)) = idC (k (x)) = k(x) C.* Então, *h(x) f−1 (C).* Como *f −1*

(C) = {z A | f(z) C. temos *l(x) = h(x)*. Logo, *(*$id_{f^{-1}(C)} \circ$ *l) (x) =* $id_{f^{-1}(C)}$*(l (x)) =* $id_{f^{-1}(C)}$*(h (x)) = h (x)*, isto é, $id_{f^{-1}(C)} \circ$ *l = h*. Do mesmo modo, *(f** $\circ$ *l) (x) = f*(l(x)) = f*(h(x)) = k (x)*. Por fim, temos *f** $\circ$ *l = k*.

□

Exemplo em Álgebra de Boole:

Proposição 2.29 Dada uma pré-ordem $\langle A, \leq \rangle$,vista como uma *POSET*, com *p, q A,* o seguinte diagrama é um pullback se, somente se, *s = p* $\times$ *q = p* $\sqcap$ *q*.

$$\begin{tikzcd} s \arrow[r] \arrow[d] & q \arrow[d] \\ p \arrow[r] & r \end{tikzcd}$$

Demonstração:

Ao supormos *s = p* $\sqcap$ *q* (ínfimo de *p* e *q*), podemos escrever o diagrama

$$
\begin{tikzcd}
p \sqcap q \arrow[r] \arrow[d] & q \arrow[d] \\
p \arrow[r] & r ,
\end{tikzcd}
$$

no qual temos os morfismos:

(1) $p \sqcap q \longrightarrow q$, isto é, $p \sqcap q \leq q$;

(2) $p \sqcap q \longrightarrow p$, isto é, $p \sqcap q \leq p$.

Observemos que $q \leq r$ e $p \leq r$, o que sugere $p \sqcap q \leq r$. Por conseguinte, o referido diagrama comuta.

Dado agora o diagrama

$$
\begin{tikzcd}
t \arrow[dr] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& p \sqcap q \arrow[r] \arrow[d] & q \arrow[d] \\
& p \arrow[r] & r,
\end{tikzcd}
$$

podemos mostrar que existe um único $t \longrightarrow p \sqcap q$. Dado $t \leq q$ e $t \leq p$ e $p \sqcap q$ um ínfimo, segue $t \leq p \sqcap q$.

Por outro lado, se o diagrama anterior é um pullback, devemos provar que $s = p \sqcap q$. A existência dos morfismos indicados garante que $s \leq p$ e $s \leq q$, ou seja, temos o seguinte $s \leq p \sqcap q$. Como $t \leq p$ e $t \leq q$, devemos ainda provar $t \leq s$. Dado que no pullback há um único morfismo $t \longrightarrow s$, segue $t \leq s$.

$\square$

2.3.7 EXPONENCIAÇÃO

Definição 2.30 (Exponenciação) Seja $\mathscr{C}$ uma categoria qualquer e *a, b, ba, c,* $ba \times a$ e $c \times a$ objetos de *Obj* ($\mathscr{C}$), uma exponenciação ocorre em $\mathscr{C}$ se, somente se, temos:

(1) um produto entre quaisquer dois objetos de *Obj* ($\mathscr{C}$);

(2) para os objetos *a ,b e ba* associado ao "morfismo avaliação" v*: ba* $\times$ *a* $\longrightarrow$ *b* e um objeto *c* no morfismo *g: c* $\times$ *a* $\longrightarrow$ *b*, existe um único morfismo $\hat{g}$*: c* $\longrightarrow$ *b a* tal que o diagrama a seguir comuta

$$\begin{tikzcd}
b^a \times a \arrow[rr, "v"] & & b \\
c \times a \arrow[u, "\hat{g}\times id_a"] \arrow[urr, "g"'] & &
\end{tikzcd},$$

ou seja, $v \circ (g \times ida) = g$.

Motivação em SET:

Proposicão 2.30 Em SET, temos o isomorfismo $\wp(A) \cong 2A$.

Demonstração:

Sejam A e B conjuntos em SET, o objeto de SET *BA* representa todas as funções que admitem domínio A e codomínio B. Definimos a exponenciação como $AB = \{f: B \longmapsto A\}$.

Denotamos ainda a seguinte função χ: $\wp(A) \longmapsto 2A$.

Por conseguinte, seja $B \subseteq A$, isto é, B $\wp(A)$, enunciamos que χB (x): A $\longmapsto$ {0, 1} na forma

$$\chi_B(x) = \begin{cases} 1 & se \;\; x \in B \\ 0 & se \;\; x \notin B \,. \end{cases}$$

Assim, χB é a *função característica* do conjunto *B*, isto é, para cada $B \subseteq A$, dispomos χB (x): A $\longmapsto$ {0, 1} como definida acima. Logo, temos:

(1) χ é injetiva: se χB = χC, então *B* = *C*. Supondo χB = χC, para todo *x A*, temos χB *(x)* = χC*(x)*. Por outro lado, ao supormos, por absurdo, que *B* ≠ *C*, dizemos que existe pelo menos um *x* tal que *x* B e *x* $\notin$*C*. Por conseguinte, χ*B* = *1*, mas χC *(x)* = 0, ou seja, χB *(x)* ≠ χC*(x)*, o que é uma contradição. Portanto, *B* = *C*;

(2) Se χ é sobrejetiva, estão para *f* *2A* existe *B* $\wp$*(A)* tal que temos χB = *f*. Se isto ocorre, podemos definir *B* = {*x* $\in$ *A* | *f(x)* = *1*}, logo para todo *x A*, temos χ*B (x)* = *1* se, e somente se, *f(x)* = *1*.

Provamos, pelo exposto, que χ é um isomorfismo em SET.

□

CAPÍTULO 3
INTRODUÇÃO À LÓGICA PROPOSICIONAL

Com a matematização da lógica, a partir do século XIX, ocorreu uma verdadeira revolução na forma como os lógicos passaram a estudar temas ligados ao raciocínio humano: princípios da inferência válida, uso e representação das linguagens formais e naturais, a questão da verdade, meios de demonstração *etc*.

Como já observamos no primeiro capítulo, um grande avanço da lógica matemática se deu com os trabalhos do filósofo e matemático alemão Gottlob Frege, mais precisamente, com o livro *Begriffsschrift* (Escrita Conceitual) de 1879. Frege está preocupado em realizar uma investigação sistemática do raciocínio matemático, ou seja, ele pretendia encontrar uma representação precisa do que seja uma demonstração matemática. Para tanto, ele cria uma linguagem simbólica que o permite expor de modo mais explícito as estruturas e procedimentos da prova matemática. Essa linguagem que contém uma avançada sintática com quantificadores, funções, variáveis e regras gramaticais para a formação de fórmulas bem formadas é utilizada por Frege para elaborar o cálculo proposicional e o cálculo de predicados (ou cálculo de primeira ordem) como o concebemos ainda hoje.

Giuseppe Peano no seu *Aritmetics Principia: Novo Methodo Exposita* de 1889 expõe uma linguagem formal com notação mais simples do que a proposta por Frege e a usa com objetivo de representar formalmente as provas em aritmética. Mesmo que Russell e Whitehead tenham adotado em grande maioria as ideias lógicas de Frege, preferiram utilizar na sua grande *Principia Mathematica* (1910-1913) a notação e regras formais de prova de Peano. A proposta filosófica básica da *Principia* consiste na tentativa de redução da matemática à lógica. Com esse intuito os conceitos e teoremas matemáticos passam a ser transcritos com o auxílio de ideias lógicas. Axiomas, por exemplo, expressam verdades lógicas básicas, e outras verdades lógicas (teoremas, por exemplo) derivam deles por regras de inferência *modus ponens* e de generalização universal, regras essas já sugeridas por Frege.

Russell e Whitehead ao estabelecerem a teoria dos tipos para evitarem certos paradoxos de uma "linguagem formal muito expressiva" dividem os objetos do discurso matemático em níveis. Com isso, o cálculo lógico é dividido em uma série de cálculos: cálculo proposicional (nível zero ou ordem zero da linguagem); cálculo de primeira ordem (nível um ou primeira ordem da linguagem) e cálculo de ordens superiores (demais níveis da linguagem).

A partir da década de 1920 a abordagem Frege-Peano-Russell tornou-se bem aceita, em especial, por influência de

David Hilbert e seus colaboradores. Em obras como *Os Fundamentos da Matemática* (1922), *Uma Nova Fundamentação da Matemática* (1922) e *Fundamentos da Matemática* (1939) estabelecem pressupostos teóricos importantes ao método axiomático, segundo o qual uma prova deve começar de pontos iniciais chamados axiomas e proceder, por intermédio de um mecanismo de síntese que faz uso de regras de inferência, até os teoremas. O cálculo proposicional (CP) a ser tratado a seguir é apresentado nos moldes dessa tradição: a abordagem Frege-Peano-Russell-Hilbert.

Hoje, o CP é entendido como um sistema formal que deve cumprir as seguintes condições:

1. Ter um alfabeto (catálogo de símbolos ou vocabulário) pertencente a uma linguagem proposicional;

2. Apresentar uma gramática (ou regras de formação) que identifica quais são as combinações de símbolos do vocabulário que são aceitáveis como "fórmulas bem formadas" (fbfs);

3. Possuir "esquemas de axioma", isto é, um conjunto finito de fbfs (intercambiáveis) aceitas sem demonstração;

4. Estabelecer regra(s) de inferência (ou regras de transformação ou regras de produção) que indiquem como inferir novas fbfs a partir de axiomas e/ou outras fbfs já deduzidas (chamadas teoremas).

Uma semântica é uma estrutura que permite interpretar fbfs de um CP. A seguir, enunciamos uma semântica ao CP proposto, a qual será reinterpretada (ou traduzida) em termos categóricos no último capítulo.

3.1 SINTAXE DA LÓGICA PROPOSICIONAL

3.1.1 LINGUAGEM E AXIOMÁTICA

Definição 3.1 (Linguagem do CP) Consideremos $\mathscr{L}$ a linguagem do CP. A linguagem proposicional $\mathscr{L}$ tem o seguinte alfabeto de símbolos primitivos:

(1) uma coleção de variáveis proposicionais: A, B, C,... (letras latinas maiúsculas);

(2) conectivos lógicos: $\neg$ (negação); $\wedge$ (conjunção); $\vee$ (disjunção); $\supset$ (implicação);

(3) sinais de pontuação: (,) (parênteses – símbolos auxiliares).

Definição 3.2 (Gramática) As fórmulas bem formadas (fbfs) do CP são sequências finitas de símbolos primitivos de $\mathscr{L}$ (expressões) construídas com base nas seguintes regras de formação:

(1) uma variável proposicional é uma fbf (atômica);

(2) se A é uma fbf, então $\neg$ A também o é;

(3) se A e B são fbfs, então (A $\vee$ B), (A $\wedge$ B) e (A $\supset$ B) são fbfs (moleculares);

(4) uma expressão de $\mathscr{L}$ é uma fbf se, somente se, for construída utilizando as regras de (1) – (3).

Definição 3.3 O conjunto de todas as fbfs no CP é denotado $\mathbb{FOR}$. Já Γ e Δ são subconjuntos de $\mathbb{FOR}$.

(Ax 1) $A \supset (B \supset A)$; no esquemas de

axi

(Ax 2) $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$;

(Ax 3) $(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$.

Definição 3.5 (Regra de Inferência) No CP proposto a única regra de inferência é a *modus ponens*: ao assumirmos que A $\supset$ B; dado A, então B (Notação: MP).

3.1.2 CONSEQUÊNCIA SINTÁTICA

Definição 3.6 (Demonstração) Uma demonstração de A no CP é uma sequência finita de fbfs $A_1, \ldots, A_i, \ldots, A_n$, tal que para todo i, $1 \leq i \leq n$, na qual A_i satisfaz as seguintes condições:

(1) A_i é um axioma (ou esquema de axioma);

(2) Ai vem de fbfs anteriores na sequência em razão da aplicação da MP;

(3) Ai = An = A.

Definição 3.7 (Teorema) A é um teorema no CP se, somente se, existir uma demonstração de A nesse cálculo (em símbolos $\vdash$A). Se A não é um teorema no CP, escrevemos $\nvdash$ A.

Definicao 3.8 Uma dedução de A a partir de Γ é uma sequência finita de fbfs A1, ..., Ai, ..., An, tal que para todo i, 1 $\leq$ i $\leq$ n, na qual Ai satisfaz uma das seguintes condições:

(1) Ai é um axioma (ou um esquema de axioma); ou

(2) Ai pertence a Γ;

(3) Ai é obtida de fórmulas anteriores por meio da MP;

(4) Ai = An = A.

Definição 3.9 (Consequência sintática) A fbf A é uma consequência sintática de Γ se, somente se, A é uma fbf numa dedução a partir de Γ (Notação: Γ $\vdash$ A). Sendo Γ vazio, em lugar da notação $\emptyset \vdash$A, denotamos $\vdash$A.

Corolário 3.1 Da noção de consequência decorrem as seguintes propriedades[1]:

(1) Se $\Gamma \subseteq \Delta$ e $\Gamma \vdash A$, então $\Delta \vdash A$;

(2) $\Gamma \vdash A$ se, somente se, existe Δ finito, $\Delta \subseteq \Gamma$, tal que $\Delta \vdash A$;

(3) Se $\Delta \vdash B$ e $B, \Gamma \vdash A$, então $\Delta, \Gamma \vdash A$.

Demonstração:

1. Dadas a hipótese 1 de $\Gamma \subseteq \Delta$ e a hipótese 2 de $\Gamma \vdash A$, dizemos pela segunda, que há uma sequência finita A1, ..., Ai, ..., An em que, para $1 \leq i \leq n$, ou Ai é axioma ou vem de fórmulas anteriores por MP ou, ainda, Ai Γ. Mas, se Ai Γ, então Ai Δ, pela definição de subconjunto. Logo, segue $\Delta \vdash A$. Portanto, como $\Gamma \subseteq \Delta$ e $\Gamma \vdash A$, temos, ao final, $\Delta \vdash A$.

2. Se $\Gamma \vdash A$, então há uma sequência finita de fórmulas A1, ..., Ai, ..., An que é uma dedução de A a partir de Γ, ou seja, existe Δ finito, $\Delta \subseteq \Gamma$ tal que $\Delta \vdash A$. Por outro lado, se $\Delta \subseteq \Gamma$ e $\Delta \vdash A$, então $\Delta \cup \Gamma \vdash A$. Mas, $\Delta \cup \Gamma = \Gamma$, pela definição de união e pela hipótese $\Delta \subseteq \Gamma$. Portanto, $\Gamma \vdash A$ se, somente se, existe Δ finito, $\Delta \subseteq \Gamma$, tal que $\Delta \vdash A$.

3. Por hipótese $B, \Gamma \vdash A$. Pela parte (1) dessa demonstração,

1 Abrevia-se, aqui, {*A1, ..., Ai, ..., An*} $\vdash$ *A*, escrevendo-se *A1, ..., Ai, ..., An* $\vdash$ *A*. Da mesma forma, abrevia-se $\Gamma \cup \{A\}$, escrevendo-se Γ, *A*.

segue $\Delta, B, \Gamma \vdash A$, mas como $\Delta \vdash B$ e $B, \Gamma \vdash A$, por hipótese, segue-se $\Delta, \Gamma \vdash A$.

$\square$

TEOREMA 3.1 (TEOREMA DA DEDUÇÃO) SE $\Gamma, A \vdash B$, ENTÃO $\Gamma \vdash A \supset B$.

EXERCÍCIO 3.1 PROVE O **TEOREMA 3.1**

3.2 SEMÂNTICA PROPOSICIONAL

Definição 3.10 (Semântica Proposicional) Uma semântica proposicional consiste nas condições que modelam a função-verdade (ou função interpretação) $\bar{v} : \mathbb{FOR} \longmapsto 2$, a qual atribuí a cada fbf pertencente ao conjunto de todas as fbfs do CP $\mathbb{FOR}$ um valor-verdade do conjunto $2 = \{\bot, \top\}$, tal que o valor-verdade $\top$ representa o verdadeiro e o valor-verdade $\bot$ denota o falso, conforme a matriz lógica de cada conectivo lógico. A valoração $\bar{v}$ satisfaz as seguintes condições:

($\neg$) $\bar{v}\ (\neg A) = \top$ *se, e somente se,* $\bar{v}\ (A) = \bot$;

($\vee$) $\bar{v}\ (A \vee B) = \top$ *se, e somente se,* $\bar{v}\ (A) = \top$ *ou* $\bar{v}\ (B) = \bot$;

($\wedge$) $\bar{v}\ (A \wedge B) = \top$ *se, e somente se,* $\bar{v}\ (A) = \bar{v}\ (B) = \top$;

($\supset$) $\bar{v}\ (A \supset B) = \top$ *se, e somente se,* $\bar{v}\ (A) = \bot$ *ou* $\bar{v}\ (B) = \top$.

Definição 3.11 Uma fbf qualquer A é válida se para toda valoração $\bar{v}$, temos $\bar{v}\ [A] = \top$. Denotamos A como uma fbf qualquer válida por $\models$A. Caso contrário, $\not\models$ A.

3.3 TEOREMAS DA COMPLETUDE E CORREÇÃO

A seguir, vamos mostrar que o CP é correto, ou seja, que todos os seus teoremas são válidos (ou verdadeiros) na semântica sugerida.

TEOREMA 3.2 (TOREMA DA CORREÇÃO). SE $\vdash$ A, ENTÃO $\models$A.

Demonstração:

Para demonstrarmos o teorema da correção devemos provar que todos os esquemas de axiomas do CP são válidos e que a regra *modus ponens* preserva a validade.

Devemos provar que o *Ax* **1** é verdadeiro, em símbolos, $\models A \supset (B \supset A)$. Essa igualdade vale desde que, observada a condição ($\supset$), tenhamos $\not\models$ A ou $B \supset A$. Suponhamos que $\models A$ e $\not\models B \supset A$. Mas $\not\models B \supset A$ se, somente se, $\models B$ e $\not\models A$, segundo ($\supset$). o que é uma contradição com a suposição que estabelece $\models A$. Logo, temos $\models A \supset (B \supset A)$.

Devemos provar que o *Ax* **2** é verdadeiro, isto é, em símbolos, temos o seguinte $\models (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$. Segundo a condição ($\supset$), $\models$ $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$ se, somente se, $\not\models A \supset (B \supset C)$ ou $\models (A \supset B) \supset (A \supset C)$.

Suponhamos que (1) $\models A \supset (B \supset C)$ e (2) $\not\models (A \supset B) \supset (A \supset C)$. Se (1) $\not\models (A \supset (B \supset C)$, então $\models A$ e $\not\models (B \supset$

$C)$. Já de (2) $\not\models (A \supset B) \supset (A \supset C)$, temos $\models A \supset B$ e $\not\models A \supset C$, observada a condição **($\supset$)**. Mas se $\models A \supset B$, obtemos $\not\models A$ *ou* $\models B$, o que é uma contradição com a suposição. Logo, $\models (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.

Devemos provar que o *Ax* **3** é verdadeiro. Nesse caso, $\models (\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$ se, somente se, $\not\models (\neg B \supset \neg A)$ ou $\models (\neg B \supset A) \supset B$.

Suponhamos que $\models \neg (\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$ se, somente se, (1) $\models \neg B \supset \neg A$ e (2) $\not\models (\neg B \supset A) \supset B$. Se $\models \neg B \supset \neg A$, então $\not\models \neg B$ ou $\models \neg A$, pela condição **($\supset$)**. Ainda, segundo a condição **($\neg$)**, temos $\not\models \neg B$, logo $\models B$. Mas para que (2) $\not\models (\neg B \supset A) \supset B$, conforme a condição **($\supset$)**, devemos ter $\not\models B$, o que é uma contradição com a hipótese. Logo, $\models (\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$.

A regra *modus ponens* preserva a validade desde que $\models ((A \supset B) \wedge A) \supset B$. Suponhamos que $\not\models ((A \supset B) \wedge A) \supset B$. Como $\not\models ((A \supset B) \wedge A) \supset B$, temos $\models (A \supset B) \wedge A$ e $\not\models B$. Se $\models (A \supset B) \wedge A$, então $\models A \supset B$ e $\models A$, segundo a condição **($\wedge$)**. Mas para $\models A \supset B$, observada a condição **($\supset$)**, concluímos que $\not\models A$ ou $\models B$, o que é uma contradição com a hipótese. Logo, a regra *modus ponens* preserva a validade.

$\square$

Teorema 3.3 (Teorema da Completude) Se $\models$ A, então $\vdash$ A.

Demonstração:

Adotaremos a prova de Kalmar (1935) do teorema da completude. A prova é por indução sobre o cumprimento da demonstração de A segundo o CP.

Seja *A* uma fbf e *p*1,..., *pk* variáveis proposicionais que ocorrem em A. Dada uma valoração $\bar{v}$ para a variável *pk*, $1 \leq i \leq k$, consideremos as atribuições de valor-verdade (1) *piv* $\equiv$ *pi*, se $\bar{v}$ (*pi*) = $\top$ e (2) *piv* $\equiv \neg$ *pi*, se $\bar{v}$ (*pi*) = $\perp$.

Em geral, se *Av* $\equiv$*A*, então $\bar{v}$ (*A*) = $\top$. Por outro lado, se *Av* $\equiv$ $\neg$*A*, então $\bar{v}$ (*A*) = $\perp$. Devemos provar que $p_1{}^v, \ldots, p_k{}^v \vdash A^v$, observando o número de conectivos que ocorrem em *A*.

Para o caso *n* = 0 em que *Av* $\equiv$ *p*, temos *p* $\vdash$ *p* e $\neg$ *p* $\vdash \neg$ *p*. Como *p* $\vdash$ *p* e $\neg$ *p* $\vdash \neg$ *p* são válidos no CP, então neste caso vale a expressão em questão. Para a hipótese de indução (HI) *k* < *n*, temos:

1. *A* $\equiv$ $\neg$*B*

1.1. Se $\bar{v}$ (*B*) = $\top$, então $\bar{v}(A) = \perp$; logo, *Bv* $\equiv$ *B* e *Av* $\equiv$ $\neg$ *A*.

1. $p_1{}^v, \ldots, p_k{}^v \vdash B$	HI aplicada a B
2. $p_1{}^v, \ldots, p_k{}^v \vdash B \supset \neg\neg B$	T. do CP: $A \supset \neg\neg A$
2. $p_1{}^v, \ldots, p_k{}^v \vdash B$	MP 1,2
3. $p_1{}^v, \ldots, p_k{}^v \vdash \neg A$	$A \equiv \neg B$
4. $p_1{}^v, \ldots, p_k{}^v \vdash A^v$	$A^v \equiv \neg A$.

1.2. Se $\bar{v}$ (B) = $\perp$, então $\bar{v}$ $(A) = \top$; logo, $Bv \equiv \neg B$ e $Av \equiv A$.

1. $p_1{}^v, \ldots, p_k{}^v \vdash B^v$	HI aplicada a B
2. $p_1{}^v, \ldots, p_k{}^v \vdash \neg B$	$B^v \equiv \neg B$
3. $p_1{}^v, \ldots, p_k{}^v \vdash A$	$A \equiv \neg B$
4. $p_1{}^v, \ldots, p_k{}^v \vdash A^v$	$A^v \equiv A$.

2. $A \equiv B \supset C$

2.1. Se $\bar{v}$ $(B) = \perp$, então $\bar{v}$ $(A) = \top$; logo, $B^v \equiv \neg B$ e $Av \equiv A$.

1. $p_1{}^v, \ldots, p_k{}^v \vdash \neg B$	HI aplicada a B e $B^v \equiv \neg B$
2. $p_1{}^v, \ldots, p_k{}^v \vdash \neg B \supset (B \supset C)$	T. do CP: $\neg A \supset (A \supset B)$
3. $p_1{}^v, \ldots, p_k{}^v \vdash B \supset C$	MP 1,2
4. $p_1{}^v, \ldots, p_k{}^v \vdash A$	$A \equiv B \supset C$
5. $p_1{}^v, \ldots, p_k{}^v \vdash A^v$	$A^v \equiv A$.

2.2. Se $\bar{v}$ (B) = $\top$ e $\bar{v}$ (C) = $\top$, então $\bar{v}$ (A) = $\top$; logo, $Cv \equiv C$ e $Av \equiv A$.

1. $p_1{}^v, \ldots, p_k{}^v \vdash C$ HI aplicada a C e $C^v \equiv C$
2. $p_1{}^v, \ldots, p_k{}^v \vdash C \supset (B \supset C)$ **Ax 1**
3. $p_1{}^v, \ldots, p_k{}^v \vdash B \supset C$ MP 1,2
4. $p_1{}^v, \ldots, p_k{}^v \vdash A^v$ $A \equiv B \supset C$ e $A^v \equiv A$.

2.3. Se $\bar{v}\ (B) = \top$ e $\bar{v}\ (C) = \bot$, então $\bar{v}\ (A) = \bot$; logo, $B^v \equiv B$, $C^v \equiv \neg C$ e $A^v \equiv \neg A$.

1. $p_1{}^v, \ldots, p_k{}^v \vdash B$ HI aplicada a B e $B^v \equiv B$
2. $p_1{}^v, \ldots, p_k{}^v \vdash \neg C$ HI aplicada a C e $C^v \equiv \neg C$
3. $p_1{}^v, \ldots, p_k{}^v \vdash B \supset (\neg C \supset \neg(B \supset C))$ T. do CP: $A \supset (\neg B \supset \neg(A \supset B))$
4. $p_1{}^v, \ldots, p_k{}^v \vdash \neg C \supset \neg(B \supset C)$ MP 1,3
5. $p_1{}^v, \ldots, p_k{}^v \vdash \neg(B \supset C)$ MP 2,4
6.. $p_1{}^v, \ldots, p_k{}^v \vdash A^v$ $A \equiv B \supset C$ e $A^v \equiv \neg A$.

Logo, para qualquer valoração as variáveis *p1,...,pk*, vale a expressão $p_1{}^v, \ldots, p_k{}^v \vdash A^v$.

Sejam *A* uma tautologia e *p1,...,pk* variáveis proposicionais que ocorrem em A. Como $A^v \equiv A$, temos $p_1{}^v, \ldots, p_k{}^v \vdash A$. Se $\bar{v}\ (p_k) = \bot$, então temos $p_1{}^v, \ldots, \neg p_k{}^v \vdash A$. Pelo TD, segue $p_1{}^v, \ldots, p_{k-1}{}^v \vdash \neg p_k \supset A$. Mas, se $\bar{v}\ (p_k) = \top$, então, pelo TD, temos $p_1{}^v, \ldots, p_{k-1}{}^v \vdash p_k \supset A$. Vejamos se é possível eliminar a variável *pk*.

1. $p_1{}^v, \ldots, p_{k-1}{}^v \vdash p_k \supset A$
2. $p_1{}^v, \ldots, p_{k-1}{}^v \vdash \neg p_k \supset A$
3. $p_1{}^v, \ldots, p_{k-1}{}^v \vdash (p_k \supset A) \supset ((\neg p_k \supset A) \supset A)$ T. do CP:$(A \supset B) \supset ((\neg A \supset B) \supset B)$
4. $p_1{}^v, \ldots, p_{k-1}{}^v \vdash (\neg p_k \supset A) \supset A$ MP 1,3
5. $p_1{}^v, \ldots, p_{k-1}{}^v \vdash A$ MP 2,4

Após $K - 1$ procedimentos semelhantes a este, eliminamos as variáveis $p_1, \ldots, p_{k-1}$ até obtermos $\vdash A$. $\square$

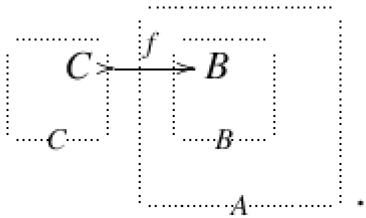
CAPÍTULO 4
CÁLCULO PROPOSICIONAL E TEORIA DAS CATEGORIAS

No presente capítulo correlacionamos algumas noções do CP com a categoria *TOPOS*. Definimos, inicialmente, o objeto matemático "classificador de sub-objetos" que compõe a estrutura da TOPOS. Em seguida, apresentamos essa categoria especial. Na sequência, interpretamos os conectivos lógicos da disjunção, conjunção, negação e implicação à luz da *TOPOS*. Ao final, expomos uma *semântica categórica* para o CP. Com o auxílio dessa semântica, encerramos o capítulo com as provas dos teoremas da correção e completude.

4.1 SUB-OBJETOS E CLASSIFICADOR DE SUB-OBJETOS

MOTIVAÇÃO EM SET:
Seja B um subconjunto de A e f injetora (um *monomorfismo*), dizemos que a função $f: C \rightarrowtail B$ define um subconjunto de A, tal que $Im\ (f) = \{f(x) \mid x\ C\}$. Portanto, f induz a uma bijeção

entre C e $Im(f)$. Em gráfico, temos:



Em *SET*, portanto, um sub-objeto de A é qualquer objeto tal que a função $f: C \rightarrowtail B$ seja injetiva, isto é, $Im(f)$ equivale a B. Nesses termos, denotamos $C \cong B$.

Definição 4.1 (Sub-objeto) Numa categoria qualquer $\mathscr{C}$ um sub-objeto do objeto d $Obj(\mathscr{C})$ é um monomorfismo $f: a \rightarrowtail d$ com domínio d.

Motivação em SET:

Na *teoria dos conjuntos* o conjunto potência $\wp(D)$ pode ser denotado como $2D$: uma coleção de todas as funções de D para $2 = \{0, 1\}$, isto é, $\wp(D) \longmapsto 2D$, já que há uma correspondência bijetiva entre os subconjuntos de D e as funções do tipo $D \longmapsto 2$. Com isso, dado um subconjunto $A \subseteq D$, definimos a *função característica* de A, isto é, $\chi_A: D \longmapsto 2$, pela seguinte lei

$$\chi_A(x) = \begin{cases} 1 & se \;\; x \in A \\ 0 & se \;\; x \notin A \,. \end{cases}$$

Definição 4.2 (Classificador de Sub-objeto) Seja $\mathscr{C}$ uma categoria qualquer com objeto terminal 1 e pullback(s), um classificador de sub-objetos é um objeto Ω Obj ($\mathscr{C}$) associado ao "morfismo verdade" $\top$: 1 $\longrightarrow$ Ω, tal que para d Obj ($\mathscr{C}$) e o sub-objeto *f*: *a* $\rightarrowtail$ *d* existe um único "morfismo característico de *f*" χ_f: *d* $\longrightarrow$ Ω que comuta o seguinte pullback

$$\begin{tikzcd} a \arrow[r, tail, "f"] \arrow[d, "!"'] & d \arrow[d, "\chi_f"] \\ 1 \arrow[r, "\top"'] & \Omega \,, \end{tikzcd}$$

isto é, $\chi_f \circ f = \top \circ \, !$.

Proposição 4.1 Sejam *f*: *a* $\rightarrowtail$ *d* e *g*: *b* $\rightarrowtail$ *d* dois sub-objetos de *d*, $f \cong g$ se, somente se, $\chi_f = \chi_g$.

Demonstração:

Por um lado, segundo o diagrama

$$\begin{tikzcd}
b \arrow[dr, "k"] \arrow[drr, bend left, "g"] \arrow[ddr, bend right, "!"'] & & \\
& a \arrow[r, tail, "f"] \arrow[d, "!"'] & d \arrow[d, "\chi_f"] \\
& 1 \arrow[r, "\top"'] & \Omega
\end{tikzcd},$$

k ocorre por ser pullback, então $f \circ k = g$. Nesse caso, como g é monomorfismo, temos $f \leq g$. Dessa forma, $\chi_f \circ f = \top \circ\, !$, já que o diagrama acima comuta.

Sabemos que k é monomorfismo, pois se $k \circ m = k \circ n$, então $f \circ k \circ m = f \circ k \circ n$. O que implica em $g \circ m = g \circ m = n$. Como $f \circ k = g$, temos $g \leq f$. De modo análogo, provamos que $f \leq g$; logo, $f \cong g$.

Por outro lado, vamos supor que $f \cong g$, então k no diagrama acima é isomorfismo. Reescrevendo o diagrama anterior, temos

$$\begin{tikzcd}
b \arrow[r, "g"] \arrow[d, "k"'] & d \arrow[dd, "\chi_g"] \\
a \arrow[ur, "f"] \arrow[d, "!"'] & \\
1 \arrow[r, "\top"'] & \Omega
\end{tikzcd}$$

Para provar $\chi_f = \chi_g$, temos que definir o diagrama acima como um Pullback. Dado

$$\begin{tikzcd}
e \arrow[drr, bend left, "h"] \arrow[dr, dashed, "l"] \arrow[ddr, dashed, "l'"'] \arrow[dddr, bend right, "!"'] & & \\
& b \arrow[r, "g"] \arrow[d, "k"] & d \arrow[dd, "\chi_f"] \\
& a \arrow[ur, "f"'] \arrow[d, "!"'] & \\
& 1 \arrow[r, "\top"'] & \Omega
\end{tikzcd}$$

temos $\chi_f \circ h = \top \circ !$.

Queremos provar ainda a existência de um único l, tal que

$g \circ l = h$. Nesse diagrama, como $\chi_f \circ h = \top \circ !$ e como o quadrilátero formado por f e χ_f é um Pullback, então existe um único $l': e \longrightarrow a$ tal que $f \circ l' = h$. Finalmente, o mesmo diagrama sugere definir $l' = k \circ l$, ou seja, $l = k-1 \circ l'$, já que k é isomorfismo, temos $g \circ l =$ $g \circ k-1 \circ l' = f \circ l' = h$.
$\square$

4.2 Conectivos Lógicos em Termos Categóricos

Definição 4.3 (Categoria TOPOS) TOPOS é uma categoria $\mathscr{E}$ que admite:

(1) *Objeto Terminal;*

(2) *Pullback;*

(3) *Exponenciação;*

(4) *Classificador de Sub-objetos.*

4.2.1 Negação

Motivação em SET:

Em SET, podemos estabelecer dois morfismos que vão de 1 = {0} para 2 = {1,0}. Um deles chamamos de "morfismo verdade", dito $\top(0) = 1$, enquanto o outro chamamos de "morfismo falso", definido como $\perp(0) = 0$. Deste modo, obtemos no codomínio 2 o seguinte conjunto vazio: $\emptyset = \{x \mid \perp(x) = 1\}$. Consequentemente, em *SET*, temos o seguinte pullback

$$
\begin{tikzcd}
\emptyset \arrow[r, tail, "!"] \arrow[d, "!"'] & 2 \arrow[d, "\perp"] \\
1 \arrow[r, tail, "\top"'] & 2 .
\end{tikzcd}
$$

A negação na categoria SET pode ser entendida como uma função $2 \longmapsto 2$, de forma que $\{x \mid \sim(x) = 1\} = \{0\} \subseteq 2$. A inclusão de zero ao conjunto 2, isto é, $\{0\} \subseteq 2 = \{1,0\}$, é determinada pela função $\perp$. Logo, em SET, vale o seguinte pulback

$$
\begin{tikzcd}
1 \arrow[r, tail, "\perp"] \arrow[d, "!"'] & 2 \arrow[d, "\sim"] \\
1 \arrow[r, tail, "\top"'] & 2 .
\end{tikzcd}
$$

Definição 4.4 (Conectivo Negação) O conectivo negação é um morfismo único expresso da seguinte forma $\sim : \Omega \longrightarrow \Omega$, dado pelo diagrama

$$\begin{tikzcd}
1 \arrow[r, "\perp"] \arrow[d, "!"'] & 2 \arrow[d, "\sim"] \\
1 \arrow[r, "\top"'] & 2 .
\end{tikzcd}$$

um pullback em $\mathscr{E}$, tal que $\sim = \chi_{\perp}$ e $\chi_{\perp} \circ \perp = = \top \circ !$.

4.2.2 CONJUNÇÃO

Motivação em SET:

Vejamos, a princípio, em SET o comportamento do conectivo lógico da conjunção. A função valor-verdade $\frown: \;\; 2 \times 2 \longmapsto 2$ é definida segundo a seguinte matriz lógica

A	B	$\overline{v}(A) \frown \overline{v}(B)$
0	0	0
0	1	0
1	0	0
1	1	1

.

O conjunto dos valores-verdade que valida a função-verdade da conjunção pode ser expresso na forma $\Theta = \{(1,1)\} \subseteq 2 \times 2$.

Tomando Θ como monomorfismo, isto é, $1 \overset{\Theta}{\rightarrowtail} 2 \times 2$, temos observado o diagrama

$$\begin{tikzcd}
1 \arrow[r, tail, "\Theta"] \arrow[d, "!"'] & 2 \times 2 \arrow[d, "\frown"] \\
1 \arrow[r, "\top"'] & 2
\end{tikzcd},$$

isto é, $\frown \circ \Theta = \top \circ\, !$. Por conseguinte, $\frown (\Theta(1,1)) = \frown (1,1) = 1$. Por outro lado, $\top \circ\, !(1,1) = \top(*) = 1$.

Como Θ é um conjunto unitário, então é possível identificá -lo com qualquer outro conjunto unitário $\{*\}$. Logo, podemos expressar o morfismo Θ segundo $h : \{*\} \longmapsto 2 \times 2$, dado *h* ($*$) = (1,1). Todavia, o morfismo $\langle \top, \top \rangle$ pode fazer o mesmo que *h* se tomarmos o elemento $*$ = 0, visto que em

$$\begin{tikzcd}
 & \{*\} \arrow[dl, "\top"'] \arrow[d, "\langle \top, \top \rangle"] \arrow[dr, "\top"] & \\
2 & 2 \times 2 \arrow[l] \arrow[r] & 2
\end{tikzcd},$$

ocorre $\langle \top, \top \rangle \circ \{*\} = \langle \top(*), \top(*) \rangle = (1,1)$.

Portanto, em *SET*, podemos definir a conjunção conforme o diagrama

$$\begin{tikzcd}
1 \arrow[r, "\langle \top, \top \rangle"] \arrow[d, "!"'] & 2 \times 2 \arrow[d, "\frown"] \\
1 \arrow[r, "\top"'] & 2 .
\end{tikzcd}$$

$\square$

Definição 4.6 (Conectivo Conjunção) O conectivo conjunção é um morfismo único expresso na forma $\frown : \Omega \times \Omega \longrightarrow \Omega$, dado o seguinte diagrama

$$\begin{tikzcd}
1 \arrow[r, tail, "\langle \top, \top \rangle"] \arrow[d, "!"'] & \Omega \times \Omega \arrow[d, "\frown"] \\
1 \arrow[r, "\top"'] & \Omega ,
\end{tikzcd}$$

em $\mathscr{E}$, tal que $\frown = \chi_{\langle \top, \top \rangle}$ e $\chi_{\langle \top, \top \rangle} \circ \langle \top, \top \rangle = \top \circ\, !$.

4.2.3 IMPLICAÇÃO

Motivação em SET:

Na lógica clássica o conectivo da implicação pode ser expresso segundo a função $\Rightarrow : 2 \times 2 \longmapsto 2$, a qual é modelada pela seguinte matriz lógica

A	B	$\overline{v}(A) \Rightarrow \overline{v}(B)$
0	0	1
0	1	1
1	0	0
1	1	1

.

Seja $\Psi = \{(0,0), (0,1), (1,1)\} \subseteq 2 \times 2$, dado o seguinte diagrama

$$\begin{tikzcd} \Psi \arrow[r, tail, "\Psi"] \arrow[d, "!"'] & 2 \times 2 \arrow[d, "\Rightarrow"] \\ 1 \arrow[r, "\top"'] & 2 \end{tikzcd},$$

Γ, visto como um morfismo, pode ser discriminado como um conjunto de pares ordenados, em decorrência da lei (x, y) Γ se, e somente se, $x \leq y = \leq (x, y)$. Nesses termos, temos:

1. $\Psi = \{(x,y) \subseteq 2 \times 2$ **tal que** $\leq (x,y)\}$;

2. $\Psi = \{(x,y) \subseteq 2 \times 2$ **tal que** $x \sqcap y = x\}$;

3. $\Psi = \{(x,y) \subseteq 2 \times 2$ **tal que** $\sqcap(x,y) = p_1(x,y)\}$.

Logo, com base nos passos anteriores, $\Psi \rightarrowtail 2 \times 2$ é o equalizador das projeções $\frown : 2 \times 2 \longmapsto 2$ e $p_1 : 2 \times 2 \longmapsto 2$, tal que o diagrama

$$
\begin{tikzcd}
d \arrow[dr, dashed, "k"] \arrow[drr, bend left, "h"] \arrow[ddr, bend right, "h"'] & & \\
& e \arrow[r, "i"] \arrow[d, "i"'] & 2 \times 2 \arrow[d, "\frown"] \\
& 2 \times 2 \arrow[r, "p_1"'] & 2
\end{tikzcd}
$$

comute, ou seja, $\frown \circ i = p_1 \circ i$ e $i \circ k = h$ exista e seja único. Portanto, se $\frown \circ i = p_1 \circ i$, então $p_1 = \frown$. Por conseguinte, $p_1(x, y) = \frown(x, y) = x$, isto é, $p_1(x, y) = x$.

□

Definição 4.7 (Conectivo Implicação) O conectivo implicação é um morfismo único expresso na forma $\Rightarrow : \Omega \times \Omega \longrightarrow \Omega$, definido pelo equalizador

$$
\begin{tikzcd}
d \arrow[dr, dashed, "k"] \arrow[drr, bend left, "h"] \arrow[ddr, bend right, "h"'] & & \\
& e \arrow[r, "i"] \arrow[d, "i"] & \Omega \times \Omega \arrow[d, "\frown"] \\
& \Omega \times \Omega \arrow[r, "p_1"'] & \Omega
\end{tikzcd}
$$

em $\mathscr{E}$, o qual pode ser expresso na forma

$$
\begin{tikzcd}
e \arrow[r, tail, "i"] \arrow[d, "!"'] & \Omega \times \Omega \arrow[d, "\Rightarrow"] \\
1 \arrow[r, "\top"'] & \Omega ,
\end{tikzcd}
$$

tal que $\Rightarrow : \ \Omega \times \Omega \underset{p_1}{\overset{\frown}{\rightrightarrows}} \Omega$, isto é, $\Rightarrow \ = \chi_i$ e $\chi_i \circ i = \top \circ \, !$.

4.2.4 DISJUNÇÃO

Motivação em SET:

Na lógica clássica o conectivo da disjunção é uma função do tipo $\smile : 2 \times 2 \longmapsto 2$ como indicado pela seguinte matriz lógica

A	B	$\overline{v}(A) \smile \overline{v}(B)$
0	0	0
0	1	1
1	0	1
1	1	1

.

A partir da matriz acima, estabelecemos o conjunto $\Xi = \{(1,1),(1,0),(0,1)\} \subseteq 2 \times 2$.

O conjunto Ξ pode ser escrito como a união de dois outros conjuntos, ou seja, $\Xi = \Sigma \cup \Pi$, tal que $\Sigma = \{(1,0),(1,1)\}$ e $\Pi = \{(0,1),(1,1)\}$. O conjunto Γ pode ser identificado como um monomorfismo do produto $\langle \top, id \rangle : 2 \longmapsto 2 \times 2$, de forma que $1 = \{x \mid x = 0 \text{ ou } x = 1\}$ e $\top(x) = 1$. De modo similar, ∏ é dito como $\langle id, \top \rangle$. Logo, segundo o coproduto

$$\begin{tikzcd}
2 \arrow[rr, "\Sigma"] \arrow[drr, "{\langle \top, id \rangle}"'] & & 2+2 \arrow[d, "f"] & & 2 \arrow[ll, "\Pi"'] \arrow[dll, "{\langle id, \top \rangle}"] \\
& & 2 \times 2 & &
\end{tikzcd},$$

temos $f \circ \Sigma = \langle \top, id \rangle$ e $f \circ \Pi = \langle id, \top \rangle$. Com isso, $f(\Sigma) = \langle \top, id \rangle$ gera (1,0) e (1,1), uma vez que

$$f(\Sigma) = \begin{cases} \langle \top(x), id(x) = (1,0) \ para \ x = 0 \\ \langle \top(x), id(x) \rangle = (1,1) \ para \ x = 1 \ . \end{cases}$$

Portanto, para $f = [\langle \top, id \rangle, \langle id, \top \rangle]$, temos a $Im\ (f) = f(2+2) = \Xi$ e vale a seguinte fatoração (epimorfismo-monomorfismo)

$$\begin{tikzcd}
2+2 \arrow[r, "f"] \arrow[dr, "f^*"'] & 2 \times 2 \\
& f(2+2) \arrow[u, hook]
\end{tikzcd} ,$$

isto é, $Im\ (f) = \{ f(x) \mid x \in \Xi \}$ e $f^*(x) = f(x)$, para todo $x \in \Xi$.

$\square$

Definição 4.8 (Conectivo Disjunção) O conectivo disjunção é um morfismo único expresso na forma $\smile : \Omega + \Omega \longrightarrow \Omega \times \Omega$, conforme o seguinte diagrama

$$\begin{tikzcd}
\Omega \arrow[r, tail, "{[\langle \top, id\rangle, \langle id, \top\rangle]}"] \arrow[d, "!"'] & \Omega + \Omega \arrow[d, "\smile"] \\
1 \arrow[r, "\top"'] & \Omega \times \Omega ,
\end{tikzcd}$$

em $\mathscr{E}$, dado que $\chi_{[\langle \top, id\rangle, \langle id, \top\rangle]} = \smile$ e $\chi_{[\langle \top, id\rangle, \langle id, \top\rangle]} \circ [\langle \top, id\rangle, \langle id, \top\rangle] = \top \circ !$.

4.3 SEMÂNTICA PROPOSICIONAL CATEGÓRICA

Definição 4.9 (Semântica Proposicional Categórica) Seja $\mathbb{FOR}$ uma coleção de fbfs do CP, uma dada $\mathscr{E}$-Valoração é um morfismo-verdade $\breve{v} : \mathbb{FOR} \longrightarrow \mathscr{E}(1, \Omega)$ que associa a uma fbf qualquer (**X**) o valor-verdade verdadeiro 1, isto é, $\breve{v}(\boldsymbol{X}) : 1 \longrightarrow \Omega$, tal que $\breve{\boldsymbol{v}}$ satisfaz as seguintes condições:

$$(\neg) \;\; \breve{v}(\neg A) = \sim \circ\, \breve{v}(A)$$

$$
\begin{tikzcd}
1 \arrow[r, "\breve{v}(A)"] \arrow[dr, "\sim\circ\breve{v}(A)"'] & \Omega \arrow[d, "\sim"] \\
& \Omega \, ;
\end{tikzcd}
$$

(∧) $\breve{v}(A \wedge B) = \frown \circ \langle \breve{v}(A), \breve{v}(B) \rangle$

$$
\begin{tikzcd}
& 1 \arrow[dl, "\breve{v}(A)"'] \arrow[d, "\langle \breve{v}(A), \breve{v}(B) \rangle"] \arrow[dr, "\breve{v}(B)"] & \\
\Omega & \Omega \times \Omega \arrow[l] \arrow[r] \arrow[d, "\frown"] & \Omega \\
& \Omega \, ; &
\end{tikzcd}
$$

(∨) $\breve{v}(A \vee B) = \smile \circ \langle \breve{v}(A), \breve{v}(B) \rangle$

$$
\begin{tikzcd}
 & 1 \arrow[dl, "\breve{v}(A)"'] \arrow[d, "\langle \breve{v}(A), \breve{v}(B) \rangle"] \arrow[dr, "\breve{v}(B)"] & \\
\Omega \arrow[r] & \Omega + \Omega \arrow[d, "\smile"] & \Omega \arrow[l] \\
 & \Omega \times \Omega\ ; &
\end{tikzcd}
$$

(⊃) $\breve{v}(A \supset B) = \Rightarrow \circ \langle \breve{v}(A), \breve{v}(B) \rangle$

$$
\begin{tikzcd}
 & 1 \arrow[dl, "\breve{v}(A)"'] \arrow[d, "\langle \breve{v}(A), \breve{v}(B) \rangle"] \arrow[dr, "\breve{v}(B)"] & \\
e & \Omega \times \Omega \arrow[l] \arrow[r] \arrow[d, "\Rightarrow"] & e \\
 & \Omega\ . &
\end{tikzcd}
$$

4.4 CORREÇÃO E COMPLETUDE

Definição 4.10 Na categoria $\mathscr{E}$, denotamos $\mathscr{E} \models A$ para todo A em $\mathbb{FOR}$ quando $\breve{v}(A) = \top : 1 \longrightarrow \Omega$, ou seja, A é uma fbf válida do CP.

Proposição 4.2 Como $\mathscr{E}$ admite $\top$ e $\perp$ como únicos para Ω, temos $\mathscr{E} \models A$ se, e somente se, $\vdash_{CP} A$.

Lema 4.1 Em TOPOS, os valores-verdade $\top$ e $\perp$ (verdadeiro e falso) têm comportamento clássico, isto é,

$$\begin{array}{c|c} & \sim \\ \hline \top & \perp \\ \perp & \top \end{array} \;;\quad \begin{array}{c|cc} \Rightarrow & \top & \perp \\ \hline \top & \top & \perp \\ \perp & \top & \top \end{array} \;;\quad \begin{array}{c|cc} \smile & \top & \perp \\ \hline \top & \top & \top \\ \perp & \top & \perp \end{array} \;;\quad \begin{array}{c|cc} \frown & \top & \perp \\ \hline \top & \top & \perp \\ \perp & \perp & \perp \end{array}\,.$$

Lema 4.2 Dados os diagramas do tipo

$$\begin{tikzcd} \bullet \arrow[r] \arrow[d] & \bullet \arrow[d] \\ \bullet \arrow[r] \arrow[d] & \bullet \arrow[d] \\ \bullet \arrow[r] & \bullet \end{tikzcd} \qquad \mathit{ou} \qquad \begin{tikzcd} \bullet \arrow[r] \arrow[d] & \bullet \arrow[r] \arrow[d] & \bullet \arrow[d] \\ \bullet \arrow[r] & \bullet \arrow[r] & \bullet \end{tikzcd},$$

dizemos:

(1) Se os quadrados internos são pullbacks, o quadrado externo também é pullback;

(2) Se o quadrado externo é pullback e o de baixo (ou à direita) também é pullback, então o quadrado de cima (ou à esquerda) é pullback.

Como ilustração, vamos provar o caso $\neg \circ \perp = \top$. A partir do **Lema 4.2**, obtemos:

$$
(1)\quad
\begin{tikzcd}
0 \arrow[r, "!"] \arrow[d, "!"'] & 1 \arrow[d, "\top"] \\
1 \arrow[r, "\perp"] \arrow[d, "!"'] & \Omega \arrow[d, "\sim"] \\
1 \arrow[r, "\top"'] & \Omega .
\end{tikzcd}
\qquad
(2)\quad
\begin{tikzcd}
0 \arrow[r] \arrow[d, "!"'] & 1 \arrow[d, "\sim\circ\perp"] \\
1 \arrow[r, "\top"'] & \Omega
\end{tikzcd}
$$

$$\Longrightarrow$$

Os diagramas (1) e (2) são pullbacks, pois $\top\circ\, ! = \perp\circ\, !$ e $\sim \circ\perp = \top\circ\, !$. Como o diagrama exterior também é pullback, logo se $\sim \circ\perp = \top(!)$, então $\sim \circ\perp = \top$.

$\square$

Demonstração:

Por um lado, para qualquer TOPOS admitimos que se $\mathscr{E} \models A$, então $\vdash_{CP} A$. Observado o *teorema da completude* acima, devemos provar que se $\mathscr{E} \models A$, então $\vdash A$.

Seja $\bar{v} : \mathbb{FOR} \longmapsto 2$, então A é uma tautologia quando $\bar{v}(A) = \top$. Ao escrevermos $\breve{v} : \mathbb{FOR} \longrightarrow \mathscr{E}(1, \Omega)$ em função de $\bar{v}$, temos:

$$\check{v}(A) = \begin{cases} 1 & se \quad \bar{v}(A) = \top \\ 0 & se \quad \bar{v}(A) = \bot \end{cases}.$$

Se $\mathscr{E} \models A$, então $\check{v}(A) = \top$ e, em particular, $\bar{v}(A) = 1$. Com fulcro no *teorema da completude* acima, dado o exposto, podemos afirmar que se $\mathscr{E} \models A$, então $\vdash A$.

Por outro lado, admitindo o *teorema da correção* como válido, dado $\vdash A$, temos A como tautologia, isto é, $\models A$. Seja $\check{v} : \mathbb{FOR} \longmapsto \mathscr{E}(1,\Omega) = \{\top, \bot\}$, podemos definir $\bar{v}$ usando $\bar{v}(A) = \begin{cases} \top & se \quad \check{v}(A) = 1 \\ \bot & se \quad \check{v}(A) = 0 \end{cases}.$

Se ocorre $\models A$, então, em particular, $\bar{v}(A) = \top$. Logo, $\check{v}(A) = 1$. Por fim, pelo *teorema da correção* se $\vdash A$, então $\mathscr{E} \models A$.

$\square$

RESPOSTAS DOS EXERCÍCIOS PROPOSTOS

EXERCÍCIO 1.1:

Dada uma função *f: A* $\longmapsto$ *B*, e para qualquer *a A* e *b B*, tais que *f(a) = b*, temos:

$$(f \circ idA)(a) = f(idA\,(a)) = f(a) = b = idB(b) = idB(f(a)) = (idB \circ f)(a)$$

$\square$

EXERCÍCIO 2.1:

No seguinte diagrama

$$
\begin{tikzcd}
A \arrow[r, "h"] \arrow[d, "f"'] & C \arrow[r, "i"] \arrow[d, "g"] & N \arrow[d, "l"] \\
B \arrow[r, "k"'] & D \arrow[r, "j"'] & M
\end{tikzcd} ,
$$

os pares de funções $\langle i, j \rangle$ e $\langle h, k \rangle$ comutam. Da composição de $\langle i, j \rangle \circ \langle h, k \rangle$, obtemos o novo diagrama

$$
\begin{tikzcd}
A \arrow[r, "i \circ h"] \arrow[d, "f"'] & N \arrow[d, "l"] \\
B \arrow[r, "j \circ k"'] & M
\end{tikzcd} .
$$

Logo, temos:
$\langle i, j \rangle \circ \langle h, k \rangle = \langle i \circ h, j \circ k \rangle$.

Observados os passos anteriores, determinamos a associatividade como segue

$$
\begin{gathered}
(\langle i, j\rangle \circ \langle h,k\rangle) \circ \langle f,g\rangle = \langle (i \circ h) \circ f, (j \circ k) \circ g\rangle = \\
\langle i \circ (h \circ f), j \circ (k \circ g)\rangle = \langle i, j\rangle \circ \langle h \circ f, k \circ g\rangle = \\
\langle i, j\rangle \circ (\langle h,k\rangle \circ \langle f,g\rangle).
\end{gathered}
$$

□

Exercício 2.3:

Para qualquer função monotônica *f: A* $\longmapsto$ *B*, com *a*, *b A*, *a* $\leq$ *b* implica *f (a)* $\leq$ *f (b)* em *B*. Pelo diagrama

$$
\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "id_A"'] \arrow[dr, dotted, "f"] & B \arrow[d, "id_B"] \\
A \arrow[r, "f"'] & B
\end{tikzcd},
$$

se *a* $\leq$ *b* em *A*, então pela nomotônica *idA: A* $\longmapsto$ *A*. Logo, temos *idA (a)* $\leq$ *idA (b)* em *A*. Como *f* é monotônica, obtemos *f (idA (a))* $\leq$ *f (idB (b))* em *B*.

Por outro lado, sendo a função *idB: B* $\longmapsto$ *B* também monotônica, segue *idB (f(a))* $\leq$ *idB (f(b))* em B. Mas, se *a* $\geq$ *b*, então *idA (a)* $\geq$ *idA (b)* ocorre em *A* e *f (idA (a))* $\geq$ *f (idB (b))* ocorre em *B*. Pelo exposto, o diagrama acima comuta, isto é, *idB* $\circ$ *f = f* $\circ$ *idA = f*.

□

EXERCÍCIO 2.4:

Para provarmos a propriedade da composição da categoria MON, pensemos no seguinte diagrama

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, dotted, "g\circ f"'] \arrow[dr, dotted] & N \arrow[dl, "g"] \arrow[d, dotted, "h\circ g"] \\
G \arrow[r, "h"'] & H
\end{tikzcd}$$

Esse diagrama representa os homomorfismos entre os seguintes monóides $\langle M, \oplus, a\rangle$, $\langle N, \triangleright, e\rangle$, $\langle G, \odot, o\rangle$ e $\langle H, \diamond, u\rangle$. Os homomorfismos são:

1. Se *m,n M*, tal que $f: M \longmapsto N$, então há o homomorfismo do tipo $f(m \oplus n) = f(m) \triangleright f(n)$ e $f(a) = e$;

2. Se *p,q N*, tal que $g: N \longmapsto G$, então temos o homomorfismo do tipo $g(p \triangleright q) = g(p) \odot g(q)$ e $g(e) = o$;

3. Se *r,s G*, tal que $h: G \longmapsto H$, então obtemos o homomorfismo do tipo $h(r \odot s) = h(r) \diamond h(s)$ e $h(o) = u$;

4. Se *m,n M*, tal que $g \circ f: M \longmapsto G$, então o homomorfismo $g \circ f(m \oplus n) = g \circ f(m) \odot g \circ f(n)$ e $g \circ f(a) = o$;

5. Se *p,q N*, tal que $h \circ g: N \longmapsto H$, então segue o

homomorfismo $h \circ g(p \triangleright q) = h \circ g(p) \diamond h \circ g(q)$ e $h \circ g(e) = u$;

6. Se m,n M, tal que $(h \circ g) \circ f = h \circ (g \circ f)$: $M \longmapsto H$, então há o homomorfismo $h \circ (g \circ f)(m \oplus n) = h \circ (g \circ f)(m) \diamond h \circ (g \circ f)(n)$ e $h \circ (g \circ f)(a) = u$;

Por um lado, o morfismo $g \circ f$ compreende o homomorfismo $g \circ f(a) = o$. Como $h \circ (g \circ f) = h(g \circ f)$, então $h(g \circ f(a)) = h(o) = u$, segundo o passo 3. Se $(h \circ g) \circ f = (h \circ g)(f)$ e $f(a) = e$, segundo o passo 1, então segue $(h \circ g)(f(a)) = (h \circ g)(e) = u$, segundo o passo 5. Conforme o exposto, concluímos que $(h \circ g) \circ f = h \circ (g \circ f)$.

Por outro lado, o passo 5, temos $h \circ g(e) = u$. Como $h(o) = u$ e $f(a) = e$, logo $h \circ g(f(a)) = h(o)$, mas se $g \circ f(a) = o$, então $h \circ g(f(a)) = h(o)$. Por outro lado, essa última expressão corresponde a $h \circ g(f(a)) = h(g \circ f(a)) = (h \circ g) \circ f(a) = h \circ (g \circ f)(a)$. Portanto, de forma geral $(h \circ g) \circ f = h \circ (g \circ f)$. $\square$

EXERCÍCIO 2.5:

Seja $A = \emptyset$ e B um conjunto qualquer; se ocorre f: $\emptyset \longmapsto$ B, então $f(\emptyset) = \emptyset$ (função vazia). Por outro lado, vamos supor $A \neq \emptyset$ como objeto inicial. Seja B certo conjunto, isto é, $B = \{x, y, \ldots\}$, com $x \neq y$, que comporte funções tais como $f: A \longmapsto B$. Seja A um conjunto não vazio, de forma a admitir, pelo menos, um elemento, então podemos definir as funções constantes $f, g: A \longmapsto B$ como $f(z)$

$= x$ e $f(z) = y$, para todo $z\ A$. Obviamente, $f \neq g$, pois $x \neq y$. Logo, A não pode ser objeto inicial.

$\square$

EXERCÍCIO 2.6:

O ínfimo é uma noção de ordem. Dado dois elementos p e q, denotamos $p \sqcap q$ o *ínfimo* de p e q, ou seja, $p \sqcap q = inf\{p, q\}$. Em POSET, $p \times q$ é um produto de p e q se existem os morfismos $n: p \times q \longrightarrow p$ e $m: p \times q \longrightarrow q$, tais que para $i: e \longrightarrow p$ e $j: e \longrightarrow q$ existe um único $h: E \longrightarrow p \times q$, de maneira que comuta o diagrama

$$\begin{tikzcd}
 & e \arrow[dl, "i"'] \arrow[d, dashed, "h"'] \arrow[dr, "j"] & \\
p & p \times q \arrow[l, "n"] \arrow[r, "m"'] & q\,.
\end{tikzcd}$$

Do diagrama anterior, inferimos $n: p \times q \leq q$ e $m: p \times q \leq p$; além disso, temos $i: e \leq p$ e $j: e \leq q$ e $h: e \leq p \times q$. Pelas projeções i e j, $e \leq p \sqcap q$. Consequentemente, de h, obtemos $p \times q \leq p \sqcap q$ (1). Por outro lado, segundo o diagrama

$$\begin{tikzcd}
& e \arrow[dl, "i"'] \arrow[dr, "j"] \arrow[d, dashed, "h"] & \\
p & p \times q \arrow[l, "n"] \arrow[r, "m"'] \arrow[d, dashed, "l"] & q \\
& e \arrow[ul, "o"] \arrow[ur, "k"'] &
\end{tikzcd},$$

constatamos as seguintes projeções: *o:* $p \leq e$; *k:* $q \leq e$ e *l:* $p \times q \leq e$. Por *o* e *k*, segue $e \leq p \times q$. Pela *transitiva* de *h* e $e \leq p \times q$, temos $p \sqcap q \leq p \times q$ (2). Conforme as expressões (1) e (2), dizemos que $p \times q$ é o ínfimo de *p* e *q*, isto é $p \times q = p \sqcap q$. □

EXERCÍCIO 2.7:

Se *A* e *B* já são disjuntos ($A \cap B = \emptyset$), então a união disjunta de *A* e *B* é, simplesmente, $A \cup B$. Mas, se *A* e *B* não são disjuntos, basta obter duas “cópias” disjuntas de *A* e *B* e, neste caso, a união disjunta será a união destas cópias. Assim, por exemplo, $A' = \{\langle x, 0\rangle \mid x \in A\} = A \times \{0\}$ e $B' = \{\langle x, 1\rangle \mid x \in B\} = B \times \{1\}$, tal que $A' \cong A$ e $B' \cong B$, de forma que $A' \cap B' = \emptyset$. Definimos $A + B$, em geral, como $A' \cup B'$.

Definimos, a seguir, as projeções $iA: A \longmapsto A + B$ e a projeção $iB: B \longmapsto A + B$ de $A + B$ que comutam o seguinte diagrama

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[dr, "f"'] & A+B \arrow[d, dashed, "p"] & B \arrow[l, "i_B"'] \arrow[dl, "g"] \\
& A'+B', &
\end{tikzcd}$$

isto é, $p \circ iA = f$ e $p \circ iB = g$.

Provamos que as projeções iA e iB permitem fatorar o par de funções $f: A \longmapsto A' + B'$ e $g: B \longmapsto A' + B'$ se $p: A + B \longmapsto A + B'$ existe e é único.

$$p(x,a) = \begin{cases} f(x) & se \ \ a = 0 \\ g(x) & se \ \ a = 1 \end{cases},$$

tal que p depende de f e g. Logo:

1. $p \circ iA(x) = p\ (iA\ (x)) = p\ (x,\ 0) = f(x)$, isto é, $p \circ iA = f$;

2. $p \circ iB(x) = p\ (iB\ (x)) = p\ (x,\ 1) = g(x)$, isto é, $p \circ iB = g$.

Dizemos também p única ao supor que existe outra função $q: A + B \longmapsto A' + B'$ que comute o diagrama, isto é, $q \circ iA = f$ e $q \circ iB = g$. Seja $(x, a)\ A + B$, obtemos:

1. Para $a = 0$, obtemos:

$q\ (x, a) = q\ (x, 0) = q\ (iA\ (x)) = (q \circ iA)\ (x) = f(x) = (p \circ iA)\ (x) = p(iA\ (x)) = \qquad p\ (x, 0) = p\ (x, a)$;

2. Para $a = 1$, segue:

$q\ (x, a) = q\ (x, 1) = q\ (iB\ (x)) = (q \circ iB)\ (x) = g(x) = (p \circ iB)\ (x) = p(iB\ (x)) = \qquad p\ (x, 1) = p\ (x, a)$.

Por fim, $p = q$. Pelo exposto, a união disjunta em SET é o coproduto.

$\square$

EXERCÍCIO 2.8:

Ao supormos que '*i*' é um equalizador de *f* e *g* e é epimorfismo, temos o seguinte diagrama

$$\begin{tikzcd}
e \arrow[r, "i"] \arrow[d, "i"'] & a \arrow[d, "f"] \\
a \arrow[r, "g"'] & b
\end{tikzcd},$$

tal que $f \circ i = g \circ i$. Se 'i' é epimorfismo (cancelável à direita), então $f = g$.

Dado, ainda, que podemos redefinir o diagrama anterior na forma

$$\begin{tikzcd}
a \arrow[dr, dashed, "k"] \arrow[drr, bend left, "id_a"] \arrow[ddr, bend right, "id_a"'] & & \\
& e \arrow[r, "i"] \arrow[d, "i"'] & a \arrow[d, "f"] \\
& a \arrow[r, "g"'] & b
\end{tikzcd},$$

segue $f \circ ida = g \circ ida$ e, consequentemente, $f = g$. Deve existir $k: a \longrightarrow e$ tal que $i \circ k = ida$. Por outro lado, $i \circ (k \circ i) = (i \circ k) \circ i = ida \circ i = i$. Assim, dizemos $i = i \circ ide$, como $i \circ (k \circ i) = i \circ ide$. Como '$i$' é equalizador e monomorfismo (cancelável à esquerda), isto é, $k \circ i = ide$, então $k = i - 1$ resulta ser isomorfismo.

□

EXERCÍCIO 2.9:

1. Como R é *reflexiva*, isto é, (x, x) *R*, logo todo *x* $[x]$;

2. Ao supor (x, y) R, devemos mostrar que $[x] = [y]$. Seja *w* $[y]$, então (y, w) *R*. Mas, por hipótese, (x, y) *R*; logo, pela *transitividade*, (x, w) *R*. Portanto, *w* $[x]$, isto é, $[y] \subset [x]$. Para provar que $[x] \subset [y]$, notemos que o fato de (x, y) *R* acarreta, pela simetria}, (y, x) R. Então, por raciocínio análogo, obtemos $[x] \subset [y]$. Com isso, concluímos $[x] = [y]$;

3. Devemos provar que se $[x] \cap [y] \neq \emptyset$, então $[x] = [y]$. Se ocorre $[x] \cap [y] \neq \emptyset$, então existe um elemento *w A* com *w* $[x] \cap [y]$. Logo, (x, w) *R* e (y,w) *R*. Pela *simetria*, (w,y) *R* e, pela *transitividade*, (x,y) *R*. Por conseguinte, por (2), temos $[x] = [y]$.

□

EXERCÍCIO 3.1:

Vamos adotar a demonstração do teorema da dedução de Herbrand realizada em 1930. Devemos provar por indução em *i* que $\Gamma, A \vdash B$i, tal que $1 \leq i \leq n$. Desde já observemos que, em particular, para $i = n$, segue $\Gamma \vdash A \supset B$.

Como vimos, uma demonstração de *A* a partir de Γ é uma sequência finita de fbfs $B_1, \ldots, B_i, \ldots, B_n$, na qual cada B_i, $1 \leq i \leq n$, satisfaz uma das seguintes condições:

1. B_i é um axioma;

2. B_i pertence a Γ, A;

3. *Bi* é obtida de fbfs anteriores por meio da regra de inferência MP, ou ainda;

4. *Bi* = *Bn* = *A*.

É necessário provar que, dada a demonstração de *B* a partir de Γ, *A*, podemos exibir uma prova de $A \supset B$ a partir de Γ. Supondo que a prova de *B* a partir de Γ, *A*, tenha um único passo, é possível definir os seguintes casos:

1. *B1* é axioma;

2. *B*1 Γ, *A*;

3. *B*1 é o próprio *A*.

Portanto, para *i* = *1*, tal que $1 \leq i \leq n$, temos:

Caso 1) *B*1 é um axioma.

1. $\vdash B_1$	é axioma
2. $\vdash B_1 \supset (A \supset B_1)$	Ax **1**
3. $\vdash A \supset B_1$	1,2 por MP
4. $\Gamma \vdash A \supset B_1$	

Caso 2) *B*1 $\in$ Γ, A e *B*1 é diferente de A.

1. $\Gamma \vdash B_1$	Membro de Γ
2. $\Gamma \vdash B_1 \supset (A \supset B_1)$	Ax **1**
3. $\Gamma \vdash A \supset B_1$	1,2 por MP

Caso 3) B_1 é A.

1. $\vdash [A \supset (A \supset A) \supset A] \supset (A \supset A \supset A) \supset (A \supset A)$	Ax **2**
2. $\vdash A \supset (A \supset A) \supset A$	Ax **1**
3. $\vdash (A \supset A \supset A) \supset (A \supset A)$	1,2 por MP
4. $\vdash A \supset A \supset A$	Ax **1**
5. $\vdash A \supset A$	3,4 por MP
6. $\vdash A \supset B_1$	5 pela hipótese
7. $\Gamma \vdash A \supset B_1$	

Suponhamos, agora, que a prova de B a partir de Γ, A tenha mais que um passo, digamos n. Vamos supor, por hipótese de indução, que o teorema da dedução valha para todo $k < n$. Ora, nesse caso, para todo $k < n$, uma prova de B a partir de Γ, A implica que $B1,..., Bj,..., Bk$, $1 \leq j \leq k$, Bj satisfaz uma das seguintes condições:

1. *Bj* é um axioma, ou;

2. *Bj* pertence a Γ, A, ou;

3. *Bj* é obtida de fórmulas anteriores pela regra de inferência MP, ou ainda;

4. $Bj = A$.

Se for os casos de *Bj* ser axioma, *Bj* Γ *e* $Bj = A$, já provados conforme os casos anteriores. Assim, o único caso não provado é aquele em que *Bi* é uma consequência por MP de *Bj* e *Bk,* tal que *Bk* tem a forma $Bj \supset Bi$, de modo que assumimos $\Gamma \vdash$

$A \supset Bi$ para $j, k < i$.

Desta forma, pela hipótese indutiva $\Gamma \vdash A \supset Bj$ e $\Gamma \vdash A \supset Bi$, segue $\Gamma \vdash A \supset (Bj \supset Bi)$. Podemos definir $\Gamma \vdash A \supset Bi$ se mostrarmos que $\{\Gamma \vdash A \supset Bj, \Gamma \vdash A \supset (Bj \supset Bi)\} \vdash \Gamma \vdash A \supset Bi$. Por conseguinte, temos

Caso 4) Sejam *Bj* e *Bk*, para $i > j$ e $i > k$, tal que *Bk* tem a forma $Bj \supset Bi$

1. $\Gamma \vdash A \supset B_j$	Hipótese indutiva
2. $\Gamma \vdash A \supset (B_j \supset B_i)$	Hipótese indutiva
3. $\Gamma \vdash (A \supset (B_j \supset B_i)) \supset ((A \supset B_j) \supset (A \supset B_i))$	*Ax* 2 e *Colorário 1 : (1)*
4. $\Gamma \vdash (A \supset B_j) \supset (A \supset B_i)$	2,3 por MP
5. $\Gamma \vdash A \supset B_i$	1,4 por MP

Portanto, pelos casos analisados, se $\Gamma, A \vdash B$, então $\Gamma \vdash A \supset B$.

$\square$

REFERÊNCIAS

AWODEY, Steve. **Categoy Theory**. Oxford: Claredon Press, 2006.

BELL, John L. **The Development of Categorical Logic.** Disponível em: http://publish.uwo. ca/ jbell/. Acesso em: 04 de fevereiro de 2019.

BOYER, C.B. **História da Matemática**. São Paulo: Edgard Blücher, 1996.

BRANQUINHO, João; MURCHO, Desidério e GOMES, N. Gonçalves. **Enciclopédia de termos lógicos filosóficos**. São Paulo: Martins Fontes, 2006.

BURRIS, S.; SANKPPANAVAR, H. P. **A course in universal algebra**. New York: Springer-Verlag, 1981.

DAGHLIAN, Jacob. **Lógica e álgebra de Boole**. São Paulo: Atlas, 1994.

D'OTTAVIANO, L. M. Ítala; FEITOSA, A. Hércules. **Sobre a história da lógica, a lógica clássica e o surgimento das lógicas não-clássicas**. Disponível em: ftp://ftp.cle.unicamp.br/ pub/arquivos/educacional/ArtGT.pdf. Acesso em: 30 de junho de 2019.

DA COSTA, N. C. A. **Ensaios sobre os fundamentos da lógica**. São Paulo: Hucitec, 1994.

EILENBERG, S.; MAC LANE, S. General Theory of Natural Equivalences *in* **Transactions of the American Mathematical Society**, 58, 1945: 231-294.

EVES, Howard. **Introdução à história da matemática**. São Paulo: Editora da Unicamp, 2004.

FEITOSA, H. A; PAULOVICH, L. **Um Prelúdio à Lógica.** São Paulo: Editora da Unesp, 2005.

FILHO, E. A. **Operações Binárias**. São Paulo: Edgar Blücher, 1984.

GOLDBLATT, R. **Topoi.** The Categorial Analysis of Logic. New York: Dover, 2006.

KNEALE, W.; KNEALE, M. **O Desenvolvimento da Lógica**. Lisboa: Fundação Calouste Gulbenkian, 1980.

KLEENE, S. C. **Mathematical Logic**. New York: Dover, 2002

LANDRY, E.; MARQUIS, J. Categories in context: historical, foundational and philosophical. **Philosophia Mathematica**, 13, 2005: 1-43.

LAWVERE, F. Functorial Semantics of Algebraic Theories, **Proc. Nat. Acad. Sci. U.S.A.**, 50, 1963: 869-872.

LAWVERE, F.; SCHANUEL, S. **Conceptual Mathematics. A first introduction to categories**, Cambridge: Cambridge University Press, 1997.

LIPSCHUTZ, Seymour. **Topologia Geral**. São Paulo: McGraw-Hill, 1973.

MAC LANE, Saunders. **Categories of the Working Mathematican**. New York: Springer-Verlag, 1998.

MENDELSON, E. **Introduction to Mathematical Logic**. New Jersey: Van Nostrand Company, 1997.

MENEZES, P. F. Blauth; HAEUSLER, E. Hermann. **Teoria das Categorias para Ciência da Computação**. Porto Alegre: Instituto de Informática da UFRGS: Sagra Luzzatto, 2001.

OLIVEIRA, Franco. **Lógica e aritmética**. Brasília: Unb, 2004.

Sobre o livro

Projeto gráfico/capa	Erick Ferreira Cabral
Revisão Linguística e normalização	Antonio de Brito Freire

Mancha Gráfica	10,5 x 16,7 cm
Tipologias utilizadas	Adobe Garamond Pro 11/13,2 pt

A teoria das categorias é uma teoria matemática elegante e generalista que faz uso de uma linquagem abstrata cheia de gráficos e de uma axiomática intuitiva. Essa teoria permite expor de forma mais clara estruturas e relações matemáticas, bem como possibilita correlacionar os mais distintos ramos da matemática. Na presente obra oferecemos ao leitor um curso introdutório de "lógica proposicional categórica": uma lógica proposicional matemática (clássica) que se vale de técnicas formais poderosas da teoria das categorias.

eduepb