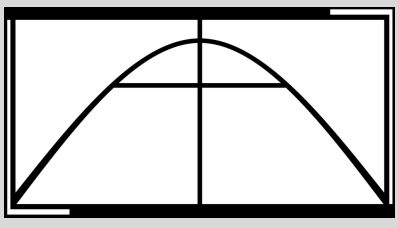
Elementos de Lógica

Volume 1

Enrique Hernández Manfredini

Lógica no Avião

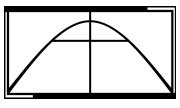


Elementos de Lógica

Volume 1

Enrique Hernández Manfredini

Departamento de Matemática
Universidade de Aveiro



Enrique Hernández Manfredini, Elementos de Lógica: Volume 1.
Brasília: Lógica no Avião, 2026.

Série L, Volume 3.

I.S.B.N. 978-65-02-02812-4.

Obra publicada com o apoio do PPGFIL/UnB.

UnB

À memória de Rolando Chuaqui

Agradecimentos

O autor é profundamente grato ao Prof. Manuel António Martins, que contribuiu com valiosas sugestões na elaboração e edição deste livro.

Prefácio

Este livro pretende oferecer uma versão autocontida do Cálculo Proposicional e a Lógica de Primeira Ordem.

Os conceitos vertidos no Capítulo I serão suficientes para uma compreensão intuitiva, ainda que incompleta, do Cálculo Proposicional e a Lógica de Primeira Ordem. O leitor com alguma experiência matemática pode omitir a leitura deste capítulo.

O Capítulo II é uma exposição do Cálculo Proposicional incluindo algumas das suas propriedades metalinguísticas, em particular o Teorema de Completude.

O Capítulo III examina noções de Teoria de Conjuntos, seus axiomas e um conceito geral de número. É incluída a construção dos números naturais, racionais e reais, mostrando como se pode desenvolver a matemática dentro da teoria; em particular, um conceito geral de número. Neste capítulo são examinados o Axioma de Escolhas, o teorema de Boa Ordem, o Lema de Zorn e a equivalência entre esses três resultados. Em particular, o Lema de Zorn é necessário para o capítulo seguinte, orientado a demonstrar que toda teoria consistente tem um modelo. Este é construído a partir de material sintático existente na própria teoria. Isto, pela sua vez, implica que toda fórmula válida na teoria é teorema dela. O último capítulo mostra alguns conceitos e exemplos na Teoria de Modelos.

E.H.M.

Prefácio Editorial

A publicação de *Elementos de Lógica*, do professor Enrique Hernánez Manfredini, atende a um objetivo primordial da linha editorial: suprir a demanda por materiais técnicos de qualidade em língua portuguesa que possuam um foco bem delimitado. Este primeiro volume se insere precisamente nesse propósito, sendo dedicado à Lógica Proposicional Clássica e a seus fundamentos.

Esta obra contribui para preencher uma lacuna na literatura de lógica em língua portuguesa, que frequentemente polariza-se entre textos introdutórios de caráter didático e obras especializadas voltadas para o público de pós-graduação. Um diferencial deste livro reside em sua capacidade de estabelecer uma ponte rigorosa e acessível entre esses dois extremos. Manfredini desenvolve um tratamento da lógica proposicional que, embora parta de noções básicas, eleva o nível de análise de forma progressiva, fornecendo ao leitor parte do ferramental técnico exigido em estudos mais avançados.

O público-alvo principal desta iniciativa são os estudantes de graduação em Filosofia, Matemática e áreas afins, bem como para todos que apresentem interesse particular nos aspectos técnicos da lógica. Ao dominar os conceitos apresentados neste volume, o leitor estará plenamente preparado para a continuidade do estudo formal. Ressalta-se que o Volume 2, já em planejamento, aprofundará a discussão ao abordar a Lógica de Primeira Ordem, Teoria dos Conjuntos e elementos de Teoria de Modelos.

A presente obra reflete o compromisso do selo editorial *Lógica no Avião* com a excelência acadêmica. Esperamos que este livro se consolide como referência didática e técnica, servindo como guia essencial para aqueles que buscam uma compreensão aprofundada da lógica como disciplina formal, estruturando o raciocínio e o pensamento crítico em suas respectivas áreas de estudo.

Edgar Almeida e Rodrigo Freire

Conteúdo

Volume 1

Volume 2

CAPíTULO 1

Noções Básicas

Os pré-requisitos necessários para abordar o estudo da lógica matemática são escassos; na sua maior parte se limitam a noções intuitivas básicas, familiares e em boa medida já presentes na linguagem conversacional e na capacidade dedutiva do entendimento comum. Estas incluem noções lógicas elementares e noções de conjuntos e números, acompanhados de um vocabulário técnico *standard* em matemática.

Algumas expressões da linguagem comum são substituídas por símbolos especiais que tornam a leitura mais compacta. Os símbolos introduzidos nestas preliminares devem ser entendidos como substitutos de expressões da linguagem comum; os conceitos associados a eles são intuitivos. Mais adiante estes símbolos serão formalmente definidos e adotarão um significado técnico formal.

Os conceitos vertidos nestas preliminares serão suficientes para uma razoável compreensão do Cálculo Proposicional e a Lógica de Primeira Ordem. Para um tratamento mais completo e auto-contido, incluímos um capítulo dedicado à Teoria de Conjuntos; os conceitos e fatos tratados aqui de maneira ingênua, são ali abordados e demonstrados formalmente. A diferença entre tratamento formal e informal de símbolos e conceitos irá ficando clara à medida que avançamos nesta exposição.

A este respeito, observe-se que há uma distinção essencial entre o *uso* e a *menção* de uma palavra, ou de uma expressão. *Utilizar* uma palavra (expressão) é *servir-se dela* para se referir ao seu *significado* ou *função*. *Mencionar* a palavra (expressão), é *referir-se a ela* como entidade gramatical, ela é o objeto do qual se fala. Certamente, é equívoco referir-se a uma palavra por meio dela própria, o que pode induzir a confusões. Para evitar esta situação, é habitual escrever entre aspas "$\cdots$" ou '$\cdots$' uma palavra (expressão) que esteja a ser mencionada. Assim, "x" ou 'x' passa a ser um *nome* do símbolo ou expressão que está entre aspas.

Contudo, a partir do contexto, torna-se normalmente óbvio se uma palavra está a ser usada ou está a ser mencionada e, por simplicidade, com frequência não se faz a distinção referida acima. Esta prática é conhecida como *autonímia*. No

que segue, permitir-nos-emos a liberdade de adotar ou não autonímia, segundo consideremos conveniente.

Noções Lógicas Básicas. Essas são extraídas da linguagem conversacional. Entre elas encontramos *proposições*, *funções*, *propriedades*, *sentenças existenciais*, *sentenças universais* e *conjuntos*.

As proposições ou sentenças são expressões que estabelecem fatos, isto é, algo que acontece ou que é de certa ou outra maneira. A partir de proposições simples, é possível formar proposições mais complexas por meio das partículas gramaticais funcionais de *negação*, *disjunção*, *conjunção*, *implicação* e *equivalência*. Desde um ponto de vista matemático, estas são *operações* entre proposições da mesma maneira que a soma e multiplicação são operações entre números; aqui são chamadas de *conectivos*. Seus símbolos são,

a) *negação*: $\neg$,
b) *disjunção*: $\vee$,
c) *conjunção*: $\wedge$,
d) *implicação*: $\longrightarrow$ ou $\Longrightarrow$,
e) *equivalência*: $\longleftrightarrow$ ou $\Longleftrightarrow$.

Informalmente, usaremos setas simples ou duplas indistintamente nas últimas duas operações. Num contexto formal será observada uma distinção rigorosa entre ambas modalidades.

Se p e q são proposições, as expressões construídas a partir delas por meio dos conectivos abreviam as sentenças da linguagem natural como segue.

a) '$\neg p$' abrevia a expressão 'não p'.
b) '$p \vee q$' abrevia a expressão 'p ou q'.
c) '$p \wedge q$' abrevia a expressão 'p e q'.
d) '$p \longrightarrow q$' abrevia a expressão 'p implica q'.
e) '$p \longleftrightarrow q$' abrevia a expressão 'p equivale a q'.

Chamaremos os elementos de uma disjunção, *disjuntos*, e os elementos de uma conjunção *conjuntos*; o primeiro elemento de uma implicação recebe o nome de *antecedente* o o segundo, *consequente*.

Expressões alternativas para $p \longrightarrow q$ são: 'se p então q', 'q, se p', 'p só se q', 'p é suficiente para q', 'q é necessário para p'.

Expressões alternativas para '$p \longleftrightarrow q$' são: 'p é necessária e suficiente para q', 'p se e só se q'; esta última é abreviada como 'p sse q'.

A partir de duas sentenças, por meio dos conectivos podemos formar sentenças mais complexas que, por sua vez, também podem ser usadas para formar outras sentenças. Sentenças também serão chamadas de expressões ou fórmulas.

Sentenças são sequências de símbolos básicos. Desse momento, essas expressões terão significados intuitivos.

Propriedades ou Predicados, Relações, Funções. As *propriedades* ou *predicados* correspondem às características ou atributos possuídas por um objeto. *Grosso modo*, correspondem a adjetivos e predicados das sentenças gramaticais. Podem ser atribuídas a objetos individuais ou a pares de objetos, a trios de objetos, etc. No caso de objetos individuais é habitualmente preferida a denominação de *predicados*; no caso de pares, trios, etc., habitua-se chamá-las de *relações*.

Os objetos individuais ou *indivíduos* são referidos por meio de *constantes* ou *variáveis individuais*. As constantes individuais são símbolos que se referem a objetos específicos ou indivíduos; correspondem aos nomes da linguagem conversacional. As variáveis individuais são símbolos que se referem a indivíduos de maneira genérica.

As funções são um caso especial de relações binárias, nas quais um elemento está relacionado com um elemento único. Este é por exemplo o caso de *o número inteiro imediatamente superior a x*, em que cada número tem exatamente um que é imediatamente superior a ele; na linguagem conversacional ocorrem com muita frequência, como em *a mãe de x*.

Se φ é uma propriedade referida a objetos individuais, escrevemos $\varphi(x)$ para indicar que x tem a propriedade φ. Por exemplo, para dizer que x é par, escrevemos $Par(x)$. Se φ se refere a pares de objetos, escrevemos $\varphi(x, y)$. Neste caso, φ é uma relação binária. Um exemplo frequente é a propriedade *ser menor que*; aqui, $\varphi(x, y)$ diz que *x é menor que y* e, em notação *prefixa* escreve-se $<(x, y)$ - diferente da habitual notação *infixa* $x < y$.

A situação é generalizada a qualquer número de variáveis. Note-se a relevância da ordem em que aparecem as variáveis. Quando não é necessário especificar as variáveis livres de uma fórmula φ se escreve esta tal como esta. Há casos em que é necessário ou conveniente se referir explicitamente a estas. Nestes casos, $\varphi(x_1, \ldots, x_n)$ significa que as variáveis livres de φ estão *entre* $x_1, \ldots, x_n$. Quer dizer que na lista podem aparecer mais variáveis para além das que tem φ. Uma fórmula cujas variáveis sejam $x_1, \ldots, x_n$ pode ser, por exemplo a disjunção de outras duas com menos variáveis. Neste caso convém dizer que estas têm variáveis *entre* $x_1, \ldots, x_n$. Indivíduos, propriedades e funções formam parte dos ingredientes que estão presentes em toda teoria e estrutura matemática.

Os conceitos de *relação e função* serão tecnicamente definidos na linguagem da Teoria de Conjuntos, apresentada no volume II deste trabalho.

Uma fórmula do tipo $\varphi(a)$ lê-se tal como está escrita, ou também como *a satisfaz* $\varphi(x)$, ou $\varphi(x)$ é satisfeita por a; ou simplesmente *a satisfaz* φ.

Sentenças existenciais e universais. Quantificadores. Variáveis livres e variáveis ligadas. Expressões do tipo $\varphi(x)$ dão lugar a sentenças *existenciais* e *universais*, isto é, sentenças da forma '*existe* x *tal que* $\varphi(x)$' e '*para todo* x *tem-se* $\varphi(x)$', ou '*para todo* x $\varphi(x)$', as quais simbolicamente são abreviadas como '$\exists x\varphi(x)$' e '$\forall x\varphi(x)$'. Os símbolos '$\exists$' e '$\forall$' são chamados de *quantificador existencial* e *quantificador universal*, respectivamente. Para o caso de duas variáveis, escreve-se '$\exists x\exists y\varphi(x,y)$' ou, simplesmente '$\exists x, y\varphi(x,y)$'. Similarmente, para '$\forall$' e para qualquer número de variáveis.

Uma variável que é susceptível de adotar valores diz-se *livre*; isto acontece quando a variável não está submetida à ação de um quantificador. Caso contrário diz-se *ligada*. Uma variável ser livre ou ligada depende do lugar em que ocorre numa fórmula. Por exemplo em x é par, x ocorre livre e pode adotar valores. Para $x = 3$ a fórmula diz que *3 é par*. Em $\exists x$(x é par), a variável x ocorre ligada. A primeira fórmula expressa algo acerca de x - *fala algo* - acerca de x. A segunda fórmula não expressa nada acerca de x, pois simplesmente diz que *existe um número par* e, dito desta maneira, é claro que a fórmula não se está a referir a x e portanto não faz sentido que a variável adote valores.

Há combinações de variáveis livres e ligadas. Por exemplo em $\exists y(x = 2y)$, y é ligada e x livre. (Esta é outra maneira de dizer que x é par). Em $\forall x(x$ é par $\vee$ x é ímpar$) \wedge (y = 3x)$, as três primeiras ocorrências de x são ligadas, a quarta é livre e a ocorrência de y é livre.

A sentença $\exists x[\varphi(x) \wedge \forall y(\varphi(y) \to y = x)]$ expressa que tal x é único. Esta sentença é abreviada por $\exists! x\varphi(x)$.

A sentença $\forall x\forall y[\varphi(x) \wedge \varphi(y) \longrightarrow x = y]$ diz que se x e y têm a propriedade φ, então devem ser iguais, isto é, que não há dois indivíduos diferentes com a dita propriedade. Podem não existir mas, no caso de existir algum, deve ser único. Por outras palavras, a sentença diz que existe *no máximo um* elemento que satisfaz φ. Esta sentença é abreviada por $\exists^* x\varphi(x)$.

Com sentenças, por meio de conectivos e quantificadores pode-se formar novas sentenças. De um ponto de vista matemático estas são sequências de símbolos; esse é um aspecto a ter em conta ao raciocinar acerca de fórmulas.

Uso de parenteses. Usamos parenteses da maneira usual em matemática: formalmente, numa expressão complexa, um par de parenteses encapsula uma parte da expressão para indicar que esta deve ser considerada como um objeto indivisível cujas partes não se devem confundir nem unir com outras partes da expressão. A situação será formalizada mais adiante.

Às vezes, não é preciso usar parenteses pois a estrutura da expressão não o requer. Mesmo assim, usaremos parentese desnecessários se isso facilitar a leitura.

Por exemplo, uma fórmula como $x = y \wedge y = z \longrightarrow y = z$ não requer parenteses, mas lê-se melhor como $(x = y) \wedge (y = z) \longrightarrow y = z$ ou, ainda, como $(x = y) \wedge (y = z) \longrightarrow (y = z)$. A fórmula $\exists x \leq z \forall y \leq u[\varphi(x) \wedge \xi(x)]$ (existe um $x \leq z$ tal que para todo $y \leq u$ tem-se $\varphi(x) \wedge \xi(x)$) lê-se mais facilmente como $(\exists x \leq z)(\forall y \leq u)[\varphi(x) \wedge \xi(x)]$.

Conjuntos. Um conjunto é qualquer agrupamento ou pluralidade de objetos; estes estão dentro do conjunto sem ordem, sem prioridades entre eles e sem prioridade entre os lugares que ocupam. Pode-se pensar num conjunto como uma coleção de objetos dentro de uma caixa. Um conjunto fica determinado de duas maneiras: por *extensão* ou por *compreensão*. A primeira consiste numa menção explícita dos seus elementos; se um elemento aparece mencionado duas ou mais vezes estas repetições não têm efeito algum; a segunda determina o conjunto por meio duma propriedade comum aos seus elementos, e só a eles. $\{1, 2, 3\}$ e $\{1, 2, 2, 3\}$ são exemplos da primeira, $\{x : 0 < x < 4\}$ é um exemplo da segunda. A relação que existe entre um conjunto e seus elementos é a de *pertinência*: $\in$. A expressão $x \in A$ significa que x *é um elemento de, ou que pertence ao, conjunto* A. No caso contrário escreve-se $x \notin A$.

Expressões como $(x \in A) \wedge (y \in A)$ são frequentemente abreviadas por $x, y \in A$. Aliás, abreviamos $(z \in y) \wedge (y \in x)$ por $z \in y \in x$. Mas repare-se que $\in$ não é transitiva, pelo que daqui não se segue $x \in z$. A linguagem da Teoria de Conjuntos consiste de variáveis individuais, dos conectivos, dos símbolos '$\forall$' e '$\exists$' do símbolo de igualdade '$=$' e da relação '$\in$'. As fórmulas desta linguagem são combinações gramaticalmente corretas destes símbolos. A definição de 'gramaticalmente correta' será dada mais adiante. Por agora, a formação de fórmulas fica confiada ao sentido comum.

Dois conjuntos que tenham os mesmos elementos são considerados iguais, e reciprocamente:

$$(\forall x)(\forall y)[(\forall z)(z \in x \longleftrightarrow z \in y) \longrightarrow x = y].$$

Esta propriedade é chamada de *extensionalidade* e será examinada em mais detalhe no capítulo de Teoria de Conjuntos no volume II deste trabalho .

Esquema Irrestrito de Compreensão. Está baseado no princípio de que uma propriedade φ dá origem (por compreensão) ao conjunto de elementos que têm a propriedade φ. A extensionalidade implica que este conjunto é único e é denotado por $\{x : \varphi(x)\}$, o qual lê-se como *o conjunto dos x tais que* $\varphi(x)$.

Expressões da forma $\varphi(x)$, aparte serem lidas tal como estão escritas, habitualmente são lidas como *x satisfaz* φ. Obviamente, com esta notação tem-se $a \in \{x : \varphi(x)\} \iff \varphi(a)$. Em lugar de ':' às vezes usa-se '|'. Uma propriedade

φ sobre conjuntos estará dada como uma fórmula da linguagem da Teoria de Conjuntos. Aplicando extensionalidade este conjunto resulta ser único.

Por outro lado, se duas fórmulas são logicamente equivalentes, então os conjunto determinados por elas são iguais. Por exemplo, para números inteiros, claramente as fórmulas $0 < x < 3$ e $x = 1 \vee x = 2$ são equivalentes, pelo qual os conjuntos determinados por elas $\{x : 0 < x < 3\}$ e $\{x : x = 1 \vee x = 2\}$ são iguais. Disso, $\{x : 0 < x < 3\}$=$\{x : x = 1 \vee x = 2\}$.

Em geral, $\{x : \varphi(x)\} = \{x : \psi(x)\} \iff (\varphi(x) \longleftrightarrow \psi(x))$. Isso estabelece uma correspondência entre fórmulas e conjuntos. Mas essa correspondência está sujeita a limitações, como se verá mais adiante.

A notação acima permite definir alguns conjuntos simples, como o conjunto *unitário* $\{a\}$, o conjunto de dois elementos $\{a, b\}$ e assim com qualquer número finito de elementos. Também permite definir o conceito de *par ordenado* de a e b, $\langle a, b, \rangle$, que ocorre por exemplo na representação cartesiana de um ponto. Usaremos a notação $\langle a, b\rangle$ ou (a, b) para pares ordenados.

Especial atenção merece o conjunto *sem* elementos, chamado *conjunto vazio*; intuitivamente, podemos pensar nele como uma *caixa* vazia; às vezes é referido como $\{\ \}$. O conjunto vazio é único e denotado também por $\emptyset$. As definições dos conjuntos mencionados acima são:

Definição 1.

1. *Unitário:* $\{a\} = \{x \mid x = a\}$.
2. *Dois elementos:* $\{a, b\} = \{x \mid x = a \vee x = b\}$.
3. *Conjunto vazio:* $\emptyset = \{x \mid x \neq x\}$.
4. *Par ordenado:* $(a, b) = \{\{a\}, \{a, b\}\}$.

A parte 4. da definição está baseada na condição de que dois pares são iguais se, e somente se, os seus primeiros elementos são iguais e os seus segundos elementos são iguais e reciprocamente. Pode-se verificar que

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \iff a = c \wedge b = d.$$

Raciocinando com o conjunto vazio. Devido ao fato que $\emptyset$ não tem elementos, resulta que todos os seus elementos têm *qualquer* propriedade φ, incluindo propriedades contraditórias.

Por exemplo, cada elemento do vazio é diferentes de si próprio. Mas, também: cada elemento do vazio é igual a, e é diferente de, si próprio. Em geral, para qualquer propriedade φ tem-se $(\forall x \in \emptyset)\varphi(x)$

Estes fatos podem parecer contra-intuitivos, mas se trata de examinar detidamente o significado das palavras. Têm a ver com as equivalências entre '$\forall x\varphi(x)$', e '$\neg\exists x\neg\varphi(x)$', já examinadas acima.

A sentença *todos os P são Q* equivale à *não existe P que não seja Q*. Por exemplo, *Todos os homens são mortais* equivale a *Não existe homem que não seja mortal*. Igualmente, a sentença *Existe um P que é Q* equivale a *Não todos os P não são Q*. Também *não todos os P são Q* equivale a *existe um P que não seja Q*.

Assim, negar que todos os elementos de $\emptyset$ têm alguma certa propriedade é afirmar que *há um elemento em* $\emptyset$ que não tem a tal propriedade, o que é certamente inaceitável.

A situação tem a ver também com quando uma sentença da forma '$p \longrightarrow q$' é falsa. Isto acontece se, e somente se, p é verdadeira e q é falsa. Em todos os outros casos aceita-se como verdadeira. Assim, em $x \in \emptyset \longrightarrow \varphi(x)$ o antecedente é sempre falso, o que faz que a sentença seja verdadeira. Nestas ocasiões diz-se que $\varphi(x)$ é *vacuamente verdadeira*.

A lógica tradicional não considerou a possibilidade de propriedades vazias. O silogismo aristotélico consistia de duas premissas e uma conclusão, separando essa daquelas por uma linha horizontal. Elas podem adotar uma das seguintes formas:

- Todos os M são P.
- Alguns M são P.
- Nenhum M é P.
- Algum M é P.

Há diversas maneiras de combinar estas quatro formas de sentenças em duas premissas e uma conclusão, que após alguns cálculos dá 256 combinações das quais 19 foram consideradas como válidas. Dessas, há quatro nas quais a conclusão não se segue das premissas se se aceita a possibilidade de que algum predicado seja vazio e receberam os apelidos *Darapti, Felapton, Fesapo* e *Bamalip*, respectivamente. Estas têm as formas

1. Todos os M são P
   Todos os M são R
   Alguns R são P

2. Nenhum M é P
   Todos os M são R
   Alguns R não são P

3. Nenhum P é M
   Todos os P são S
   Alguns S não são P

4. Todo P é M
   Todo M é S
   Alguns S são P

Observe que:

- a primeira é incorreta se $M = \emptyset = P$.
- A segunda é incorreta se $M = \emptyset = R$.

- A terceira é incorreta se $M = \emptyset$.
- A quarta é incorreta se $P = \emptyset$.

No capítulo de Estruturas de Primeira Ordem (volume II) se adotará a convenção de que o universo destas estruturas sejam não vazias, mas poderá haver predicados vazios ou fórmulas que cuja extensão seja vazia. Não se deve confundir ambas situações.

Relações entre, e operações com, conjuntos. Interessam, aqui, as relações de *igualdade* e de *inclusão* entre conjuntos. Como já estabelecido, conjuntos que têm os mesmos elementos são considerados iguais, e reciprocamente. Em símbolos:

$$A = B \iff \forall x(x \in A \leftrightarrow x \in B).$$

Um conjunto A está *incluído* ou é um *subconjunto* de um conjunto B se todos os elementos de A pertencem também a B. Em símbolos: $A \subseteq B$.

Há várias operações entre conjuntos: a *união de um par de conjuntos*, a *união de um conjunto*, a *intersecção de um par de conjuntos*, a *intersecção de um conjunto*, a *diferença* de dois conjuntos, *o produto cartesiano de um par de conjuntos* e a *potência de um conjunto*, denotadas respectivamente por: $A \cup B$, $\bigcup A$, $A \cap B$, $\bigcap A$, $A \setminus B$, $A \times B$ e $\mathcal{P}(A)$. Estão definidas por:

Definição 2.

1. *A é subconjunto de B:* $A \subseteq B \iff \forall x(x \in A \to x \in B)$.
2. *A união de A e B:* $A \cup B = \{x : x \in A \vee x \in B\}$.
3. *A união de A:* $\bigcup A = \{x : \exists y[x \in y) \wedge (y \in A)]\}$.
4. *A intersecção de A e B:* $A \cap B = \{x : x \in A \wedge x \in B\}$.
5. *A intersecção de A:* $\bigcap A = \{x : \forall y(y \in A \longrightarrow y \in x\})$.
6. *A menos B:* $A \setminus B = \{x : x \in A \wedge x \notin B\}$.
7. *O produto cartesiano de A e/por B:* $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.
8. *A potência de A:* $\mathcal{P}(A) = \{x : x \subseteq A\}$.

A primeira reúne os elementos de A e B num conjunto só. Na segunda, os elementos de A são conjuntos que, ao serem reunidos, produzem um novo conjunto: o *conjunto de elementos de elementos de A*. Por exemplo, se $A = \{B, C, D\}$, então $\bigcup A = B \cup C \cup D$. Se $A = \{A_i : i \in I\}$, então uma notação alternativa para $\bigcup A$ é $\bigcup A = \bigcup_{i \in I} A_i$. Similarmente para $\bigcap A$.

O leitor facilmente familiarizar-se-á com estas operações e com as suas propriedades elementares. A seguir, damos uma lista de algumas destas propriedades. Em qualquer caso, elas reaparecerão mais adiante. Demonstramos apenas as duas últimas.

TEOREMA 1 (Propriedades de $\cup, \cap,$ e $\subseteq$).

1. $A \subseteq A$.
2. $(A \subseteq B) \wedge (B \subseteq C) \longrightarrow (A \subseteq C)$.
3. $(A \subseteq B) \wedge (B \subseteq A) \longrightarrow (A = B)$.
4. $\cup$ *é comutativa, associativa e tem* $\emptyset$ *como elemento neutro.*
5. $\cap$ *é comutativa , associativa e* $A \cap \emptyset = \emptyset = \emptyset \cap A$.
6. $\cup$ *é distributiva relativamente a* $\cap$.
7. $\cap$ *é distributiva relativamente a* $\cup$.
8. $(A \subseteq B) \wedge (A \subseteq C) \longrightarrow A \subseteq B \cap C$.
9. $(A \setminus B) \subseteq A$.
10. $(C \setminus A) \cup (C \setminus B) = C \setminus (A \cap B)$.
11. $(C \setminus A) \cap (C \setminus B) = C \setminus (A \cup B)$.
12. $A \times \emptyset = \emptyset = \emptyset \times A$.
13. $\bigcup(A \cup B) = \Big(\bigcup A\Big) \cup \Big(\bigcup B\Big)$.
14. $\bigcup\{x\} = x$.

Prova.

Item 13. $x \in \bigcup(A \cup B) \iff x \in y$, para algum $y \in A \cup B \iff x \in y$, para algum y tal que $y \in A$ ou $y \in B \iff [x \in y$, para algum y tal que $y \in A]$ ou $[x \in y$, para algum y tal que $y \in B] \iff [x \in \bigcup A]$ ou $[x \in \bigcup B]$.

Item 14. O único elemento de $\{x\}$ é x. Portanto o conjunto de elementos de elementos de $\{x\}$ é x. □

É prática corrente abreviar expressões da seguinte maneira:

- $\forall x(x \in y \longrightarrow \varphi(x))$, por $(\forall x \in y)(\varphi(x))$.
- $\exists x[x \in y \wedge \varphi(x)]$ por $(\exists x \in)y(\varphi(x))$ e
- $\{x : x \in A \wedge \varphi(x)\}$ por $\{x \in A : \varphi(x)\}$

Relações e funções. Na prática uma relação é percebida como uma conexão que de alguma maneira vincula alguma coisa ou coisas com outra ou outras. A gama de relações é múltipla e variada; há relações entre objetos, entre pessoas, relações espaciais, temporais, familiares, etc. Relações são concebidas como *algo* que de alguma maneira está estabelecido entre os objetos relacionados; a percepção comum é que pode haver duas relações diferentes que vinculam os mesmos objetos; mais precisamente, pode haver duas relações diferentes R_1 e R_2 com as quais acontece que para quaisquer x e y que estão relacionadas por R_1, estão também relacionadas por R_2, e reciprocamente; contudo, as relações são de *natureza* diferente. Ora bem, se ambas relações relacionam exatamente os mesmos objetos, a matemática não pode distinguir entre elas, pois a *natureza* das relações não é uma entidade matemática. Quer dizer que uma relação, de um ponto de

vista matemático, é uma entidade *extensional*: o que interessa é que objetos estão na relação. Em um caso simples, uma relação consiste de *pares* de objetos. Mais precisamente, uma relação *é um conjunto de pares*. Se x e y estão relacionados por meio de R, se escreve xRy. Isto fica formalizado na

Definição 3.

1. *R é uma relação entre A e B* $\iff R \subseteq A \times B$
2. *R é uma relação (definida) sobre, ou em A* $\iff R \subseteq A \times A$.

Esses tipos de relações são chamadas *binárias* ou de *aridade* 2, por serem subconjuntos de um produto cartesiano. Considerando que pode haver produtos cartesianos com qualquer número de fatores, também haverá relações de qualquer aridade.

As propriedades individuais dos objetos são consideradas como relações de aridade 1. Como, por exemplo, em *x é primo* ou $x \neq 0$. Em tais casos, assim como uma relação binária é um subconjunto de um produto cartesiano, uma relação *unária* é simplesmente um subconjunto de um conjunto. De momento só nos ocuparemos de relações de aridade 2 e de aridade 1, (isto é, propriedades unárias). No caso de aridade 1, (relação unária), se trata de uma propriedade.

O *domínio* de uma relação é o conjunto de objetos que estão em relação com outro, e o *rango*, ou *contradomínio,* é o conjunto de objetos com os quais algum objeto está relacionado. Dizer que dois elementos estão relacionados, significa dizer que o o par formado por eles pertence à relação.

Definição 4.

1. $aRb \iff (a, b) \in R$.
2. $Dom(R) = \{x : \exists y(xRy)\}$. *$Dom(R)$: O domínio de R.*
3. $Ran(R) = \{y : \exists x(xRy)\} =$. *$Ran(R)$: O rango de R.*

As seguintes expressões formam parte do vocabulário habitual no contexto das relações.

Definição 5.

1. *y é um sucessor de x segundo R* $\iff$ *y é um R-sucessor de x* $\iff (x, y) \in R$.
2. *x é um predecessor de y segundo R* $\iff$ *y é um sucessor de x segundo R* $\iff$ *x é um R-predecessor de y* $\iff (x, y) \in R$.
3. *y é um sucessor estrito de x segundo R* $\iff$ *y é um R-sucessor estrito de x* $\iff (x, y) \in R \wedge y \neq x$.
4. *x é um R-predecessor estrito de y* $\iff (x, y) \in R \wedge x \neq y$.

5. $R[x] = \{y : xRy\}$. *O conjunto de sucessores de x segundo R* $R^{-1} = \{(y, x) : (x, y) \in R\}$. *a função inversa de R.*
6. $R[A] = \{y : \exists x \in A(xRy)\}$. *O conjunto de sucessores segundo R de elementos de A .*
7. $R^{-1}[y] = \{x : xRy\}$. *O conjunto de predecessores de y segundo R.*
8. $R^{-1}[B] = \{x : \exists y \in B(xRy)\}$. *O conjunto de predecessores segundo R de elementos de B .*

Funções. Outra classe de relações de essencial importância são as *funções*. Nelas, o domínio é igual a A e cada elemento do domínio está relacionado com exatamente *um* elemento de B. Dizemos então que R é uma *função de A em B*, o que se denota por $R : A \longrightarrow B$. É habitual usar as letras $f, g, h, \ldots$ para funções.

Definição 6 (Função de A em B).

$$f : A \longrightarrow B \iff (f \subseteq A \times B) \wedge (\forall x \in A)(\exists! y \in B)[(x, y) \in f]$$

Em palavras, a expressão $f : A \longrightarrow B$ é lida como *f é uma função de A em B.* Tratando-se de uma relação, $(x, y) \in f$ pode-se escrever como xfy mas não é o usual.

Notação: $f(x) = y \iff (x, y) \in f$.

Acima, y é chamada de *imagem de x por f* e x é uma *pré-imagem de y por f.* As notações usuais para relações são aplicadas naturalmente no caso das funções.

Em $f(x) = y$ chama-se $f(x)$ de *imagem de x* e chamas-se x de *pré-imagem de y*. A definição prescreve que cada x tem uma *única* imagem e elementos diferentes do rango de f, denotado $Ran(f)$, devem ter diferentes pré-imagens.

Para todo x e todo y em A tem-se: $x = y \longrightarrow f(x) = f(y)$ e, equivalentemente, $f(x) \neq f(y) \longrightarrow x \neq y$. Mas um $y \in Ran(f)$ pode ter múltiplas pré-imagens em A.

A propriedade de cada elemento estar relacionado com exatamente *um* elemento é referida como *unicidade* e uma relação que a tenha diz-se que é *unívoca.*

Na expressão $f(x)$, x representa elementos do domínio da função f. Se o domínio é um produto cartesiano $A \times B$ e $x \in A \times B$, então x é da forma (u, v) e a sua imagem por f é $f(x) = f((u, v))$, mas para não sobrecarregar a notação escreve-se simplesmente $f(u, v)$.

No primeiro caso f é *função unária* ou *função em uma variável*; no segundo caso f é *função binária* ou *função em duas variáveis.* Semelhantemente com funções em qualquer número de variáveis.

Usando funções pode-se simplificar algumas expressões de conjuntos. Por exemplo, quando $f(x) = y = 2x$, tem-se

$$\{x : \exists y(x = 2y \wedge y \leq 4)\} = \{2y : y \leq 4\} = \{0, 2, 4, 6, 8\}.$$

Definição 7.

$$\{f(y) : \varphi(y)\} = \{x : \exists y(x = f(y) \wedge \varphi(y))\}.$$

Relações diversas. Relações de equivalência. Classes de Equivalência. Partições. A função vazia. Conjuntos e tipos de funções. Ao longo deste estudo também encontraremos com frequência diversos conceitos relativos à relações e funções, para os quais adotaremos as seguintes definições.

Definição 8. *Seja R uma relação binária definida sobre um conjunto X.*

1. *R é reflexiva $\iff (\forall x \in X(xRx))$.*
2. *R é simétrica $\iff (\forall x, y \in X)[(xRy) \longrightarrow (yRx)]$.*
3. *R é antissimétrica $\iff (\forall x, y \in X)[(xRy) \wedge (yRx) \longrightarrow x = y)]$.*
4. *R é transitiva $\iff (\forall x, y, z \in X)((xRy) \wedge (yRz) \longrightarrow (xRz))$.*
5. *Se $(xRy) \wedge (x \neq y)$, diz-se que x precede estritamente a, ou que é um predecessor estrito de y (por R). Também, que y precede estritamente a, ou que é um sucessor estrito de x, (por R).*
6. *R é estrita sse $(\forall x, y \in X)[xRy \longrightarrow x \neq y]$.*
7. *R é irreflexiva sse $\forall x \neg(xRx)$. (Vê-se facilmente que R é irreflexiva sse R é estrita).*
8. *Uma ordem parcial R em X é lineal (ou total) se e só se $(\forall x, y \in X)[(xRy) \vee (yRx)]$. Um conjunto provido com uma ordem linear (ou total) é um conjunto linearmente (ou totalmente) ordenado.*
9. *Seja R reflexiva, $A \subseteq X$ e $a \in A$. Um elemento a é elemento minimal de A sse $(\neg \exists x \in A)[(xRa) \wedge (x \neq a)]$.*
10. *Seja R irreflexiva, $A \subseteq X$ e $a \in A$. Um elemento a é elemento minimal de A sse $(\neg \exists x \in A)(xRa)$. (Se observará que um elemento minimal de um conjunto é um elemento que está "no fundo" do conjunto).*
11. *Uma cadeia em um conjunto parcialmente ordenado $\langle X, R\rangle$ é um subconjunto de X, linearmente ordenado por R.*
12. *Sejam C uma cadeia em um conjunto parcialmente ordenado $\langle X, R\rangle$ e $s \in X$:*
    (a) *c é um limite superior de $C \iff (\forall s \in C)(cRs)$.*
    (b) *C é limitada superiormente $\iff$ existe um limite superior de C.*
13. *Em conjunto parcialmente ordenado $\langle X, R\rangle$, o elemento $M \in X$ é elemento maximal $\iff \neg(\exists x \in X)[MRx \wedge M \neq x]$.*

De particular importância são as relações que são simultaneamente reflexivas, simétricas e transitivas, chamadas de *relações de equivalência*. Elas estão intimamente relacionadas com as *partições* do seu universo. Uma partição de um

conjunto A é um conjunto de subconjuntos não vazios de A que não se intersectam dois a dois e cuja união é o conjunto A.

DEFINIÇÃO 9 (Relações de Equivalência. Partições).

1. *Seja $R \subseteq A \times A$. A relação R é de* equivalência *se para todo $x, y, z \in A$:*
   a) xRx *(Reflexiva).*
   b) $xRy \implies yRx$ *(Simétrica).*
   c) $(xRy) \wedge (yRz) \implies (xRz)$ *(Transitiva).*
2. *Seja $X \subseteq \mathcal{P}(A)$. X é uma* partição de A *se para todo o $Y, Z \in X$:*
   a) $Y \neq \emptyset$.
   b) $Y \neq Z \implies Y \cap Z = \emptyset$.
   c) $\bigcup X = \bigcup_{Y \in X} Y = A$.

Dizemos que x é equivalente a $y \iff xRy$. Os elementos de X são chamados de classes de equivalência e denotados $R[x]$, para $x \in X$.

Uma propriedade importante destes dois conceitos é que são intercambiáveis, no sentido que uma relação de equivalência determina uma partição do universo e, reciprocamente, uma partição do universo determina nele uma relação de equivalência. A mesma situação tem lugar entre partições e funções: toda função determina uma partição no seu domínio e, sob certa condição que veremos mais adiante, toda partição de um conjunto determina uma função cujo domínio é esse conjunto.

$R[x]$ determina uma partição.

TEOREMA 2 (Notações como antes).

1. *Se R é de equivalência, então $\{R[x] : x \in A\}$ é uma partição de A.*
2. *Se X é uma partição de A, então a relação definida por*

$$xRy \iff (\exists Z \in X)[(x \in Z) \wedge (y \in Z)]$$

é uma relação de equivalência.

Prova. Parte 1.

1. Pela reflexividade, para todo $x \in A$, $x \in R[x]$. Assim $R[x] \neq \emptyset$.
2. Se $R[x] \cap R[y] \neq \emptyset$, então $\exists z[(z \in R[x] \wedge z \in R[y])]$. Por definição de $R[\cdot]$, $\exists z[(zRx) \wedge zRy)]$. Por simetria de R, $\exists z[(xRz) \wedge zRy)]$. Por transitividade de R, xRy. Donde $R[x] = R[y]$. Assim,

   $$R[x] \cap R[y] \neq \emptyset \implies R[x] = R[y]$$

   e, equivalentemente, $R[x] \neq R[y] \implies R[x] \cap R[y] = \emptyset$.
3. Claramente $\bigcup\{R[x] : x \in A\} = A$, pois cada elemento a de A está em um elemento de $\{R[x] : x \in A\}$ e, nomeadamente, $a \in R[a]$.

Parte 2. Seja X uma partição de A. Definamos a relação

$$xRy \iff \exists Z \in X[(x \in Z) \wedge (y \in Z)].$$

Por definição de partição, este Z é único. Demonstramos que R é uma relação de equivalência.

1. Reflexividade. Seja $x \in A$. Por definição de partição, $(\exists Z \in X)\ (x \in Z)$. Por definição de R, xRx.
2. Simetria. Suponhamos xRy, $(\exists Z \in X)[(x \in Z) \wedge (y \in Z)]$. É obvio que nesta fórmula a ordem não interessa $(\exists Z \in X)[(y \in Z) \wedge (x \in Z)]$. Logo, yRx.
3. Transitividade. Suponhamos $(xRy) \wedge (yRz)$, isto é,

   $(\exists Z_1 \in X)[(x \in Z_1) \wedge (y \in Z_1)]$ e $(\exists Z_2 \in X)[(y \in Z_2) \wedge (z \in Z_2)]$.

   Uma vez que y pode pertencer apenas a uma classe da partição, $Z_1 = Z_2$. Assim $(\exists Z \in X)[(x \in Z) \wedge (z \in Z)]$, isto é, xRz.

□

Se R é relação de equivalência, então os conjuntos $R[x]$ recebem o nome de *classes de equivalência.*

Definição 10. *Seja $X \in \mathcal{P}(A)$ um conjunto de subconjuntos de A. X é uma partição de A se*

1. $\forall x, y \in X[(x \neq y \longrightarrow x \cap y = \emptyset)]$ *e*
2. $\bigcup X = A$.

O conceito de função está relacionado com os conceitos de partição e relação de equivalência, como descreve o seguinte

Teorema 3. *Seja $f : A \longrightarrow B$.*

1. $\{f^{-1}(y) : y \in f[A]\}$ *constitui uma partição de A.*
2. *Se $xRy \iff f(x) = f(y)$, então R é uma relação de equivalência.*

O conjunto de funções de A em B. A função vazia.

Definição 11 (Conjunto de funções de A em B).

$$A^B = \{f : (f : A \longrightarrow B)\}.$$

Teorema 4. *Dados quaisquer conjuntos A e B:*

1. $\emptyset^A = \emptyset$.
2. $B^\emptyset = \{\emptyset\}$.

Prova.

1. $f \in \emptyset^A \iff f : A \longrightarrow \emptyset$ e $f : A \longrightarrow \emptyset \iff (f \subseteq A \times \emptyset) \wedge (\forall\, x \in A)(\exists! y \in \emptyset)[(x, y) \in A \times \emptyset]$. Como $A \neq \emptyset$, existe um $x \in A$. Para esse x temos que existe um $y \in \emptyset$, o que é impossível. Portanto não há $f \in \emptyset^A$.
2. $(f \in B^\emptyset) \iff (f \subseteq \emptyset) \wedge \forall x[x \in \emptyset \longrightarrow (\exists y \in B)((x, y) \in f)]$. Ora, a última implicação é sempre (vacuamente) verdadeira, pois não há algo em $\emptyset$. Isto pode-se ver melhor se se pensar que a implicação é falsa. Se este é o caso, quer dizer que o antecedente é verdadeiro e o consequente é falso. Mas o antecedente não pode ser verdadeiro.

□

Definição 12 (Função sobrejetiva ou epijetiva). *Seja* $f : A \longrightarrow B$.

$$f \text{ é sobrejetiva, ou epijetiva, } \iff (\forall y \in B)(\exists x \in A)(f(x) = y),$$

Ou seja, f é sobrejetiva, ou epijetiva, se e somente se $Ran(f) = B$.
Se cada $y \in Ran(f)$ tem exatamente *uma pré-imagem*, a função diz-se *injetiva*.

Definição 13 (Função injetiva). *Seja* $f : A \longrightarrow B$.

$$f \text{ é injetiva } \iff (\forall x, y \in A)[x \neq y \longrightarrow f(x) \neq f(y)].$$

Se f é injetiva e $y \in Ran(f)$, escreve-se $f^{-1}(y) = x$ em lugar de $f^{-1}[y] = \{x\}$. Uma função injetiva de especial interesse é a *identidade, Id* que atribui a cada elemento x o mesmo x.

Definição 14 (A função identidade em A). *A função* $Id_A : A \longrightarrow A$ *é dada por* $Id_A(x) = x$, *para* $x \in A$. *Equivalentemente,* $Id_A = \{(x, x) : x \in A\}$.

Entre as funções injetivas, têm especial interesse as funções *biunívocas*. Como o nome o diz, estas são unívocas em ambas direções. Uma função biunívoca de A em B é uma função injetiva de A em B cuja imagem é B.

Definição 15 (Função biunívoca ou bijectiva). *Seja* $f : A \longrightarrow B$.

$$f \text{ é biunívoca } \iff (Ran(f) = B) \wedge (\forall x, y \in A)[x \neq y \longrightarrow f(x) \neq f(y)].$$

Definição 16. *Sejam A, B e C conjuntos quaisquer. Sejam* $f : A \longrightarrow B$ *e* $g : B \longrightarrow C$. *A função* $g \circ f : A \longrightarrow C$ *é a função definida por*

$$(g \circ f)(x) = g(f(x)).$$

Ou seja, se f transforma x em $f(x)$, a seguir este é transformado por g em $g(f(x))$. Observe-se a ordem em que f e g aparecem escritas. Esta é uma operação transitiva entre de funções.

TEOREMA 5. *Se* $f : A \longrightarrow B$, $g : B \longrightarrow C$ *e* $h : C \longrightarrow D$, *então*

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

Prova.

$((h \circ g) \circ f)(x) = (h \circ g)f(x) = h(g(f(x)))$.
$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$.

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

A identidade não altera o resultado da operação '$\circ$'.

TEOREMA 6. *Se* $f : A \longrightarrow A$, *então* $f \circ Id = f = Id \circ f$.

Prova. $(Id_A \circ f)(x) = id_A(f(x)) = f(x)$ e $(f \circ Id)(x) = f(id(x)) = f(x)$. □

Se uma função é biunívoca, então a sua inversa é também uma função que também é biunívoca.

A biunicidade é uma propriedade importante e sua existência entre um par de conjuntos A, B recebe uma notação especial.

DEFINIÇÃO 17 (Equipolência).

1. A *é equipolente a* $B \iff (\exists f)[(f : A \longrightarrow B) \wedge (f$ *é biunívoca*$)]$.
2. $A \approx B \iff A$ *é equipolente a* B.

A relação $\approx$ tem as seguintes propriedades.

TEOREMA 7. *Para quaisquer conjuntos* A, B, C *tem-se*

1. $A \approx A$.
2. $A \approx B \longrightarrow B \approx A$.
3. $A \approx B \wedge B \approx C \longrightarrow A \approx C$.

Prova.

1. $Id : A \longrightarrow A$ é biunívoca.
2. Se $A \approx B$, há uma função biunívoca $f : A \longrightarrow B$. Agora, $f^{-1} : B \longrightarrow A$ é biunívoca.
3. Se $A \approx B \wedge B \approx C$, então há funções biunívocas $f : A \longrightarrow B$ e $g : B \longrightarrow C$. Ora, $g \circ f$ é biunívoca de A em C.

□

Algumas funções permitem comparar o *tamanho relativo* dos conjuntos; por exemplo se há uma função de A em B e $Ran(f) = B$, podemos apreciar que há em A *pelo menos tantos elementos como em* B. De igual modo, se há uma injeção de A em B e não há bijeção de A em B, o tamanho de A é menor do que o de B. E se há uma função biunívoca de A em B, podemos apreciar que A tem

tantos elementos como B. Um aspecto interessante disto é que permite comparar *os tamanhos* de dois conjuntos *sem contá-los.*

De especial interesse é a comparação de um conjunto com sua potência.

TEOREMA 8 (G. Cantor). *Para qualquer conjunto A tem-se:*

1. *Existe uma injeção de A em* $\mathcal{P}(A)$.
2. *Não existe uma bijeção de A em* $\mathcal{P}(A)$.

Prova.

1. $f : A \longrightarrow \mathcal{P}(A)$ dada por $f(a) = \{a\}$ é uma injeção.
2. Suponhamos que existe uma tal bijeção, digamos, f. Considere-se o conjunto $B = \{x \in A : x \notin f(x))\}$. Obviamente $B \in \mathcal{P}(A)$ e, como f é bijectiva, B é imagem de algum elemento de A, digamos $B = f(b)$. Ora, deve ser $b \in B$ ou $b \notin B$.
   - Se $b \in B$, pela definição de B, $b \notin f(b)$.
   - Se $b \notin B$, pela definição de B, $b \in B$.

   A suposição da existência de uma bijeção f conduz a uma contradição. Concluímos que não existe bijeção de a em $\mathcal{P}(A)$.

□

O teorema implica que há conjuntos com tamanhos arbitrariamente grandes.

Subíndices. Um estilo de notação amplamente utilizado é aquele que usa subíndices e, possivelmente, superíndices.

Dado um conjunto A, adota-se um conjunto I e uma função de f de I em A. Cada elemento de A está indicado através de f por um elemento de $i \in I$ por $f(i)$. Em lugar de escrever $f(i)$ escreve-se A_i, com ênfase no elemento mais do que na função. Esta modalidade oferece bastante flexibilidade notacional. Por exemplo, se A é um conjunto com n elementos, podemos usar $I = \{1, \ldots, n\}$ para expressar A por $A = \{A_1, \ldots, A_n\}$ ou por $A = \{A_i : i \in I\}$.

A reunião de A pode ser expressada por $\bigcup_{i=1}^{n} A_i$ ou $\bigcup_{i \in I} A_i$.

Em geral, pode-se adotar qualquer conjunto de índices I e conceber uma função com domínio I e contradomínio A. Mas deve-se ter em conta que pode haver elementos que aparecem mencionados mais de uma vez se essa função não for biunívoca.

Observe-se que escrever $A = \{A_1, \ldots, A_n\}$ constitui um abuso da linguagem pois, aqui, A aparece simultaneamente como função e como contradomínio. Em geral, esta prática não resulta em confusões, mas vale a pena ter presente o significado dos símbolos.

As expressões *R-sucessor* e *R-predecessor* são também usadas para *sucessor segundo R* e *predecessor segundo R.*

Um tipo de relação de especial importância são as *relações bem-fundadas*. Estas constituem uma poderosa ferramenta para demonstrar que todos os elementos de certos conjuntos têm uma certa propriedade e para definir funções e conjuntos.

Como já observado, as fórmulas são sequências de símbolos. Tema a se examinar a seguir.

Sequências e ênuplas. As fórmulas são sequências ou ênuplas de símbolos. Assim como foi definido um par (ordenado), podemos definir triplas, quádruplas, etc. Quaisquer destes podem ser definidos como uma função com domínio em $\mathbb{N}$. Uma função com domínio em $\mathbb{N}$ é chamada de *sequência*. Uma função com domínio em $n \in \mathbb{N}$, é uma sequência finita de comprimento n.

Definição 18. *Seja A um conjunto.*

1. *Uma sequência de elementos de A de comprimento n é uma função de n em A. É denotada por $\langle a_0, ..., a_{n-1}\rangle$ ou por $(a_0, ..., a_{n-1})$.*
2. *Uma $0-$upla de elementos de A é $\emptyset$.*
3. *Uma $1-$upla de elementos de A é um elemento de A, (a)*
4. *Uma $2-$upla de elementos de A é um elemento da forma $\{a, \{a, b\}\}$.*
5. *Uma $(n+1)-$upla de elementos de A é da forma $\langle\langle a_0, ..., a_{n-1}\rangle, a_n\rangle$.*

Tal como estão definidos, ênuplas e sequências são objetos diferentes, mas como existe uma bijeção natural entre eles não faremos distinção entre ambos os conceitos.

Relações bem-fundadas. Seja R uma relação binária, irreflexiva, sobre um conjunto $U \neq \emptyset$ e X um subconjunto de U. *R é bem-fundada* se todo subconjunto não vazio de U tem um elemento minimal.

Definição 19. *Seja $R \subseteq U \times U$, $X \subseteq U$ e $a \in X$ e R bem-fundada.*

1. *a é um átomo de U (segundo R) $\iff$ a é minimal em U.*
2. *$At(U) = \{a \in U : \text{é um átomo}\}$.*

Se R é bem-fundada, não existem sequências infinitas estritamente descendentes de elementos de U; isto é, sequências da forma $\ldots, x_3, x_2, x_1$ tais que $\ldots Rx_3Rx_2Rx_1$ com $x_{n+1} \neq x_n$.

Se uma destas sequências existisse, então o conjunto de todos os seus elementos $\{..., x_3Rx_2Rx_1\}$ não teria um elemento minimal.

Observação A condição de irreflexividade de R não é essencial. É adotada aqui para simplificar a notação.

Princípio de indução sobre relações bem-fundadas. Neste contexto, o Princípio de Indução sobre relações bem-fundadas diz que se um subconjunto X de U:

a) contém os átomos de U e
b) qualquer elemento x de U cujos predecessores estão em X está em X,

então $X = U$. A segunda condição significa que o fato dos predecessores de x pertencerem a X *obriga* x a estar em X.

Tecnicamente: se $x \in U$, então $R^{-1}[x] \subseteq X \longrightarrow x \in X$. Ou, equivalentemente: se $x \in U$, então $(\forall y)(yRx \longrightarrow x \in X)$.

A condição $R^{-1}[x] \subseteq X$ é chamada de *hipótese inductiva*. Esta será referida como HI. Observe-se que esta é uma *condição sobre os predecessores de* x e *não sobre* x.

Teorema 9 (Princípio de Indução sobre relações bem-fundadas 1). *Sejam U um conjunto, R irreflexiva e bem-fundada em U. Se*

1. $X \subseteq U$,
2. $At \subseteq X$ *e*
3. $(\forall x \in U)(R^{-1}[x] \subseteq X \longrightarrow x \in X)$,

então $X = U$.

Prova. Suponha-se 1, 2 e 3. Suponhamos que $X \neq U$; então $U \setminus X \neq \emptyset$. Seja u um elemento minimal de $U \setminus X$, isto é, $u \in U \wedge u \notin X$. Por 2, $u \notin At$ e $R^{-1}(u) \not\subseteq At$. (Senão, por 3 $u \in X$).

Da definição de $\subseteq$, vem $(\exists y \in U \setminus X)(yRu)$, contradizendo a minimalidade de u em $U \setminus X$. □

Nota. A demostração anterior é um caso de demostração por *reductio ad absurdum* ou simplesmente *ad absurdum*. Consiste em demostrar uma certa afirmação φ supondo que ela é falsa. Se a suposição de falsidade conduz a um absurdo ou contradição, φ fica estabelecida como verdadeira.

Neste caso φ é $X = U$. A suposição $\neg\varphi$ conduz à existência de um $u \in U \setminus X$ que simultaneamente é minimal e não é minimal de $U \setminus X$.

Com frequência X é um conjunto caracterizado por uma propriedade φ; em tal caso o principio de indução fica formulado em termos de φ em lugar de X. Assim:

Teorema 10 (Princípio de Indução sobre relações bem-fundadas 2). *Sejam U um conjunto, R bem-fundada em U. Se*

1. *φ é uma propriedade de elementos de U,*

2. $(\forall x \in At)\varphi(x)$ *e*
3. $(\forall x \in U)(\forall y \in R^{-1}[x])[\varphi(y) \longrightarrow \varphi(x)]$,
então $(\forall x \in U)(\varphi(x))$.

Princípio de recursão ou recorrência sobre relações bem-fundadas. Também é chamado de Recorrência.

No mesmo contexto de U com uma relação bem-fundada R em U, considere:

- um conjunto S,
- uma função g de At em S, $g : At \longrightarrow S$ e
- uma função h de $\mathcal{P}(S)$ em S.

O *principio de recursão* (também referida como *recorrência*) *sobre relações bem-fundadas* afirma que pode-se estender g a uma *única* função f cujo domínio é U e tal que para $x \notin At$, $f(x)$ é a imagem por h do conjunto de imagens por f do conjunto de predecessores de x.

Passo a passo, o processo é como segue:

1. Tome-se um elemento x de U.
2. Se $x \in At$, então $f(x) = g(x)$. Se não:
3. procura-se o conjunto de R-predecessores de x: $R^{-1}[x]$. Este é um subconjunto de U.
4. Forme-se o conjunto de f-imagens dos R-predecessores de x: $f[R^{-1}[x]]$. Este é um subconjunto de S, isto é, um elemento de $\mathcal{P}(S)$.
5. Finalmente, define-se $f(x) = h(f[R^{-1}[x]])$.
6. Resultado: f é uma função de U em S.

Isso fica formalizado no seguinte teorema, juntamente com a sua demonstração.

Teorema 11. *Princípio de Recursão sobre relações bem-fundadas] Sejam* U, S *conjuntos,* R *uma relação bem-fundada em* U. *Se* $g : At \longrightarrow S$ *e* $h : \mathcal{P}(S) \longrightarrow S$, *então* $(\exists! f)(f : U \longrightarrow S)$ *tal que*

$$f(x) = \begin{cases} f(x) = g(x), & \text{se } x \in At \\ f(x) = h(f[R^{-1}[x]]), & \text{se } x \notin At \end{cases}.$$

Prova. (*Indução sobre* R).

I. Existência de f. f está definida sobre At e há que demonstrar que está definida sobre todo U e, para isto, seja $X = \{x \in U : \exists y(y = f(x)\}$. Demonstramos que $X = U$.

Está claro que $At \subseteq X$. Seja $x \in U$ com $x \notin At$ e suponha-se que $R^{-1}[x] \subseteq X$, (HI). Então $f[R^{-1}[x]] \subseteq S$, isto é, $f[R^{-1[x]}] \in \mathcal{P}(S)$ e $h(f[R^{-1}[x]]) \in S$.

Consequentemente $f(x) = h(f[R^{-1}[x]])$, isto é, $x \in X$ e, pelo Teorema de Indução, $X = U$.

II. Unicidade de f. Seja f' tal que $f'(x) = g(x)$ para $x \in At$ e, para $x \notin At$, $f'(x) = h(f'[R^{-1}[x]])$. Obviamente $f'(x) = f(x)$ para $x \in At$. Se $x \notin At$ e por hipótese $f'(x) = f(x)$ para $x \in R^{-1}[x]$, (HI), então $f'[R^{-1}[x]] = f[R^{-1}[x]]$, isto é, $f' = f$. □

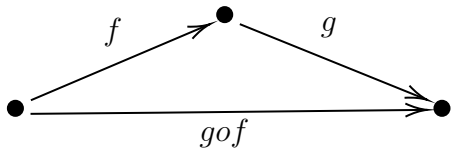


FIGURA 1.1. Composição de funções

Devido a uma aparente semelhança entre eles é fácil confundir os princípios de *indução* e *recursão*. Com efeito, em ambos casos se parte de um ou mais casos base, e os casos seguintes são obtidos a partir dos casos anteriores.

Há uma transmissão, a partir da base, para casos posteriores.

No princípio de indução o que se transmite é uma propriedade. No princípio de recursão se estende uma definição. O primeiro fornece um método de *demonstração*: uma maneira de demonstrar que *todos* os elementos de U têm certa propriedade. Isto se faz demonstrando que os átomos tem a propriedade e que ela se transmite a elementos em níveis superiores até impregnar todo o U.

O segundo fornece um método de *definição*. Pode-se também pensar que é um método de *construção* de f, começando com os valores iniciais de g e estendendo o domínio de g para níveis superiores utilizando os valores obtidos nos níveis anteriores, até obter $dom(f) = U$.

Devido ao fato que o procedimento descrito produz uma função única a partir de At, g, h e R, é de fato um método de definição, chamado *definição por recursão ou recorrência*; e diz-se que f está *definida por recursão ou recorrência sobre* R.

Enquanto indução é um *método de demostração*, recursão é *um método de definição*.

Embora sejam obviamente diferentes, estão intimamente ligados e podem ser confundidos. Por exemplo, pode-se definir por recursão com base em certa relação bem-fundada R um certo conjunto C no qual R induz uma relação bem-fundada R' a qual, por sua vez, pode ser utilizada para desenvolver argumentos por indução e por recursão em C.

Com alguma frequência se encontra na literatura expressões como: *demostração por indução sobre* U em lugar de *indução sobre* R. Similarmente com

recorrência. Também se encontra a expressão de *definição por indução* em lugar de *definimos por recursão.* Estas maneiras de falar são comuns e estão sancionadas pela tradição. Tratando-se de um curso para principiantes, convém conservar aqui os significados originais dos conceitos, evitando confusões.

A forma em que têm sido apresentados aqui os princípios de indução e recorrência é apenas uma entre uma variedade de versões. Na prática podem ser adotadas formas mais complexas e que habitualmente são utilizadas sem maior explicação.

Pode acontecer que f ou h seja uma função com mais de uma varável, ou que h seja uma função de S em S e não em $\mathcal{P}(S)$, ou de $S \times S$ em S.

Não necessariamente todos os subconjuntos de S devem tomam parte na construção de f, mas apenas aqueles da forma $f[R^{-1}(x)]$ para algum $x \in U$.

Na prática os dois princípios são aplicados contextualmente, sem maior explicação acerca de quais são os elementos envolvidos. Um exemplo será dado a seguir pelo *fatorial de* n, em que g é uma função não em $\mathcal{P}(S)$ mas em S e h é uma função de S em S e não em $\mathcal{P}(S)$; aliás, f pode ser uma função com mais de uma variável.

Em cada caso h deverá adotar formas adequadas ao domínio que corresponda à circunstância. Em geral tais variações não apresentam dificuldades uma vez que os passos 1, 2 e 3, comuns a todos os casos, são facilmente identificáveis. As provas dadas acima para ambos princípios se adaptam de maneira natural às diferentes formas adotadas por eles. O essencial é:

1. que R seja bem-fundada no conjunto, em que se vai definir ou demonstrar,
2. que haja uma função cujo domínio e At e
3. que haja uma função h definida sobre sobre algum conjunto.

Na prática os dois princípios são aplicados contextualmente, sem maior explicação acerca de quais são os elementos envolvidos. Apresentamos, como exemplo, a definição recursiva da conhecida função *factorial* no conjunto $\mathbb{N}$ de números naturais.

$$\begin{cases} 0! = 1 \\ n! = n \cdot (n-1)! \end{cases}.$$

Escrevendo $f(n)$ em lugar de $n!$:

$$\begin{cases} f(0) = 1 \\ f(n) = n \cdot f(n-1) \end{cases}.$$

De modo explícito, tem-se

- $U = \mathbb{N}$.

- $At = \{0\}$.
- $g : At \longrightarrow \mathbb{N}$ e $g(0) = 1$.
- $xRy \iff x = y + 1$. (Uma função).
- $S = \mathbb{N}$.
- $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.
- $h(x, y) = x \cdot y$.
- $f(x) = h(x, f(R^{-1}(x)) = h(x, f(x - 1))$.

E consequentemente

$$\begin{cases} 0! = 1 \\ n! = n \cdot (n-1)! \end{cases}$$

Escrevamos $f(n)$ em lugar de $n!$:

$$\begin{cases} f(0) = 1 \\ f(n) = n \cdot f(n-1) \end{cases}$$

Neste exemplo, tem-se:

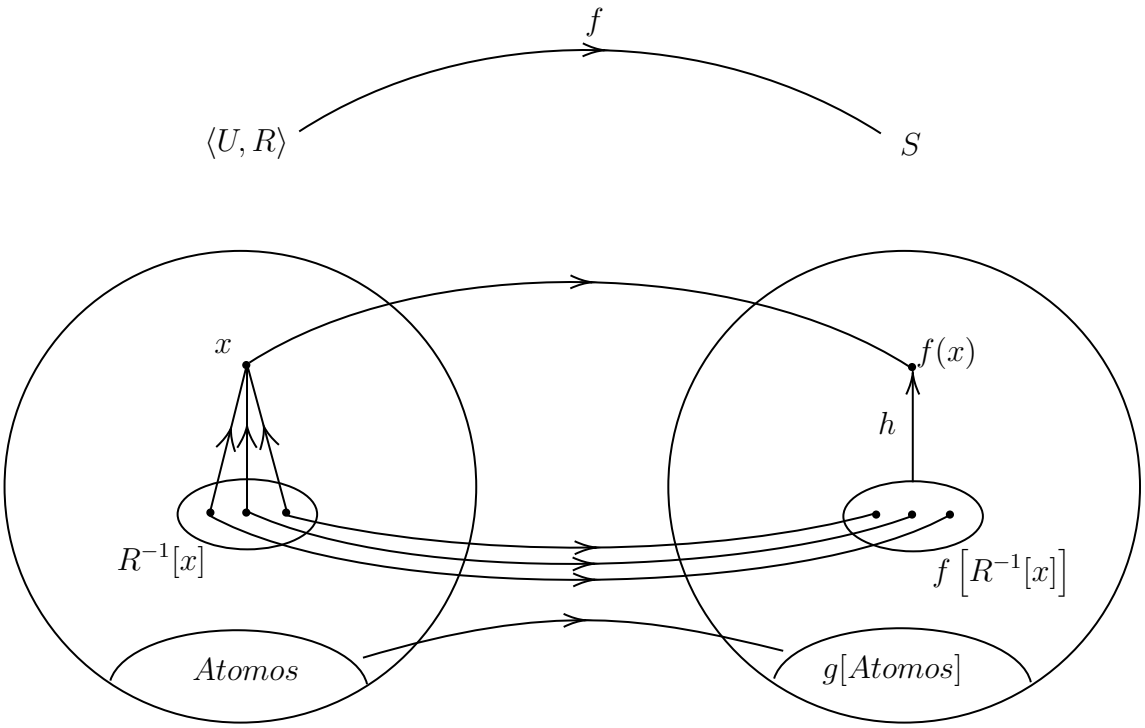
- $U = \mathbb{N}$.
- $S = \mathbb{N}$.
- $mRn \iff m = n + 1$, (R é uma função).
- $At = 0$ e $g(0) = 1$.
- $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.
- $h(m, n) = m \cdot n$.
- $R^{-1}(n) = n - 1$.
- $f(n) = h(n, f(R^{-1}(n))) = h(x, f(n - 1))$ e,
- finalmente, $f(n) = n \cdot f(n - 1)$.

As relações bem-fundadas estão a acompanhar outros tipos de relação de grande importância: as relações de ordem parcial, ordem total e as boa ordem.

Relações de ordem parcial, ordem total e boa ordem.

Definição 20. *Seja R uma relação binária sobre um conjunto U.*

1. *R é uma relação de ordem parcial se, e somente se,*
   a) *R é reflexiva,*
   b) *R é antissimétrica, isto é, $\forall x, y \in U[xRy \wedge yRx \longrightarrow x = y]$ e*
   c) *R é transitiva.*
2. *R é uma relação de ordem total se, e somente se*
   a) *R é uma relação de ordem parcial e*
   b) *R é linear ou total, isto é, $\forall x, y \in U(x \in y \cup y \in x)$.*
3. *R é uma relação de boa ordem se, e somente se,*



$$g : Atoms \to g[Atoms]$$

$$f(x) = h(f[R^{-1}[x]])$$

FIGURA 1.2. Definição por Recursão

a) R é uma relação de ordem total e
b) R é bem-fundada.

Números Naturais. Esses são os familiares 0, 1, 2, 3, ... e são concebidos, como conjuntos, do seguinte modo:

$0 = \emptyset$.
$1 = 0 \cup \{0\}$.
$2 = 1 \cup \{1\} = \{0, 1\}$.
...
$n + 1 = n \cup \{n\}\{0, 1, \ldots n\}$.
...
...

Com essa definição, um número natural é igual ao conjunto dos seus predecessores e um elemento de um natural é também subconjunto dele:

$$n = \{0, 1, \ldots, n-1\}.$$

Assim, se $m \in n$, então $n = \{0, 1, 2, \ldots m, \ldots, n-1\}$ e, portanto,

$$m \in n \longrightarrow m \subseteq n.$$

Esta propriedade merece um nome.

Definição 21 (Transitividade).

n é transitivo, denotado $Transit(n)$, sse $\forall m(m \in n \longrightarrow m \subseteq n)$.

O conjunto formado por todos os naturais é denotado por $\mathbb{N}$ ou ω.

$$\mathbb{N} = \omega = \{0, 1, 2, 3, ...n, , n+1, ...\}.$$

As familiares relações de ordem '$<$' e '$\leq$' em ω são definidas por

1. $n < m \iff n \in m$.
2. $n \leq m \iff (n \in m) \vee (n = m)$.

Com frequência trocamos, indistintamente, $\in$ por $<$ e vice-versa. Vamos supor conhecimento prévio e familiaridade com as seguintes propriedades e fatos.

3. A relação $<$ entre naturais tem as propriedades:
   a) $n < m \longrightarrow n \neq m$. (Estrita)
   b) Para todo n, m, k:
   c) $n \not< n$ *(Antirreflexiva)*
   d) $(n < m) \wedge (m < k) \longrightarrow n < k$. *(Transitiva)*
   e) $(n < m) \vee (m = n) \vee (m < n)$. (Tricotomia)
   f) $<$ é bem-fundada.
4. $\leq$ é uma ordem parcial:
   a) $n \leq n$. (*Reflexiva*)
   b) $(n \leq m) \wedge (m \leq n) \longrightarrow (n = m)$. (*Antissimétrica*)
   c) $(n \leq m) \wedge (m \leq k) \longrightarrow (n \leq k)$. (*Transitiva*)
   d) $(n < m) \vee (m = n) \vee (m < n)$. (Tricotomia)
   e) $\leq$ linearmente ordenada.
   f) $\leq$ é bem-fundada. Todo subconjunto não vazio de $\mathbb{N}$ tem um primeiro elemento ou elemento minimal.
   g) $\leq$ é uma boa ordem.

Algumas propriedades de $\mathbb{N}$ que aqui interessam são apresentadas no:

Teorema 12.

1. $\bigcup n \subseteq n$.

2. $\bigcup(n+1) = n$.
3. Se $n \neq 0$, $n = \bigcup n \cup \{\bigcup n\}$.
4. $\bigcup 0 = 0$.
5. $\bigcup \mathbb{N} = \mathbb{N}$.

Prova.

1. $m \in \bigcup n \longrightarrow m \in k \in n$ para algum n. Logo $m \subseteq n \in n$, e $m \in n$.
2. Por Teorema 1. 14, 15, com 1 (acima) temos
$$\bigcup(n+1) = \bigcup n \cup \bigcup\{n\} = \bigcup n \cup n = n.$$
3. Se $n \neq 0$, então $n = k + 1$ para algum k. Temos
$$\bigcup n = \bigcup(k+1) = k, \text{ por 2,}$$
donde $\{\bigcup\{k+1\} = \{k\}$. Com isto,
$$n = k \cup \{k\} = \bigcup n \cup \{\bigcup n\}.$$
4. Por 1 e $x \in \emptyset \longrightarrow x \in \bigcup \emptyset$.
5. $m \in \bigcup \mathbb{N} \longrightarrow m \in n \in \mathbb{N}$ para algum n. Logo $m \subseteq n \subseteq \mathbb{N}$ e $m \in \mathbb{N}$.

□

Definição 22 (Finito, Infinito).

1. A *é finito* $\iff \exists n \in \mathbb{N}(A \approx n)$.
2. A *é infinito* $\iff$ A *não é finito.*

A definição oficializa tanto a noção quanto a prática de contar com os naturais.

Definição 23 (Contável ou enumerável).

1. A *é* contável *ou* enumerável*:* $\iff A \approx \mathbb{N}$.
2. $Cont(A) \iff A$ *é contável.*

A definição formaliza a noção intuitiva de finitude e de infinitude. Um conjunto que não é equipolente a algum número natural é infinito.

Examinamos, na continuação, uma variedade de propriedades de $\mathbb{N}$ com relação aos conceitos de 'finito' e 'infinito'. Quase todas são intuitivas, fáceis de visualizar e satisfeitas por qualquer conjunto contável. Mas, antes, observe que $\emptyset$ é finito, pois é equipolente com $0(= \emptyset)$. A bijeção entre ambos é a função vazia.

Nosso primeiro teorema diz que um natural diferente de 0 não é equipolente a um subconjunto próprio dele.

A condição 'diferente de 0' se deve ao fato que o vazio é vacuamente equipolente a todos os seus subconjuntos próprios, uma vez que não tem subconjuntos próprios. (cf. Raciocinando no vazio).

TEOREMA 13.

1. $(\forall n \in \mathbb{N}(n \neq 0 \longrightarrow \forall X \subsetneq n)\neg(n \approx X)$.
2. $\forall X[(X \text{ é finito}) \wedge (Y \subsetneq X) \longrightarrow \neg(Y \approx X)]$.

Prova. Demonstramos 2. A prova de 1 é similar.

Demonstramos que um conjunto equipolente com um subconjunto próprio deve ser infinito. A afirmação é equivalente a dizer que se há uma injeção de um conjunto dentro de si próprio, então ele deve ser infinito.

> Seja A um conjunto e $f : A \longrightarrow A$ uma injeção.
> Há um $a \in A$ tal que $a \notin f[A]$. (*)
> Afirmamos: Os elementos $a, f(a), f^2(a), \ldots$ são diferentes dois a dois.

Com efeito, pode-se observar que $f^n(a) \neq a$ para todo o $n \in \mathbb{N}$, (por (*)). Se $f^k(a) = f^l(a)$ para certos $k > l$, então $f^{k-l}(a) = a$. Quer dizer que os $f^n(a)$'s com $n \in \mathbb{N}$, são todos diferentes 2 a 2. Portanto A deve ser infinito. □

TEOREMA 14.

1. $\forall a \in \mathbb{N}(\mathbb{N} \approx \setminus\{a\})$.
2. $(\forall X)[(X \subsetneq \mathbb{N}) \wedge (X \text{ é finito}) \longrightarrow \mathbb{N} \approx (\mathbb{N} \setminus X)]$.
3. $Cont(A) \longrightarrow (\forall X)[(X \subsetneq A) \wedge (X \text{ é finito}) \longrightarrow Cont(A \setminus X)]$.

Prova. Demonstramos 1. O restante fica para o leitor. Note que a equipolência está dada por

$$f(n) = \begin{cases} n & \text{se } n < a \\ n+1 & \text{se } n \geq a \end{cases}.$$

Logo $f : \mathbb{N} \longrightarrow \mathbb{N} \setminus \{a\}$ é bijetiva. □

TEOREMA 15.

1. $(\forall a)[\mathbb{N} \approx (\mathbb{N} \cup \{a\})]$.
2. $Cont(A) \longrightarrow \forall a[A \approx (A \cup \{a\})]$.
3. $\forall X[(X \text{ é finito }) \wedge (X \cap \mathbb{N} = \emptyset) \longrightarrow \mathbb{N} \approx (\mathbb{N} \cup X)]$.
4. $Cont(A) \longrightarrow \forall X[(X \text{ é finito})\wedge \longrightarrow Cont(A \cup X)]$.

Prova. Apresentamos as funções que estabelecem as equipolências. Note que os itens 3. e 4. são consequências dos anteriores.

1. $f : \mathbb{N} \longrightarrow \mathbb{N} \cup \{a\}$, $f(0) = a$ e $f(n) = n + 1$.
2. $f(n) = \begin{cases} n & \text{se } n < a \\ n+1 & \text{se } n \geq a \end{cases}$

3. Digamos que X tem n elementos, $X = \{x_0, \ldots, x_{n-1}\}$. Definamos
$$f(k) = \begin{cases} x_k & \text{se } k \in \{0, 1, 2 \ldots\} \\ k - n & \text{se } k \geq n \end{cases}.$$
4. Definamos $f : \mathbb{N} \longrightarrow \mathbb{N} \cup X$ como segue:
$$f(x_i) = i \text{ para } i < n.$$
$$f(k) = n + k \text{ para } k \in \mathbb{N}$$

□

Teorema 16. $(\forall n \in \mathbb{N})[\neg(\mathbb{N} \approx n)]$, *ou seja ,* $\mathbb{N}$ *é infinito.*

Prova. Suponhamos que $\mathbb{N} \approx n$ para algum $n \in \mathbb{N}$. Adotemos este n como o menor natural com esta propriedade. Esse n deve ser tal que > 0 e > 1; digamos $n = \{0, 1, \ldots, n-1\}$. Então $\mathbb{N} \setminus \{0\} \approx \{1, 2, \ldots n-1\} \approx$\{0, 1, 2, ... n-2\}. Mas $\mathbb{N} \setminus \{0\} \approx \mathbb{N}$, contradizendo a minimalidade de n. □

Teorema 17.

1. $(\forall m, n \in \mathbb{N})[(m < n \longrightarrow \neg(n \approx m)$.
2. *Se* $n \in \mathbb{N}$, $(\forall X \subseteq n)(\exists k < n)(X \approx k)$.
3. $(\forall n \in \mathbb{N})(\forall X \subsetneqq n)\neg(n \approx X)$.
4. $\forall X[X(\text{é finito}) \wedge (Y \subsetneqq X) \longrightarrow \neg(Y \approx X)]$.
5. $Cont(A) \Longrightarrow [(\forall X \subseteq A)(X \text{ é finito}) \wedge (Y \subsetneqq X) \longrightarrow \neg(Y \approx X)]$.

Prova.

1. Suponhamos que existe um n tal que para algum $m < n$, $m \approx n$. Seja este o menor natural com esta propriedade. Logo, existe uma bijeção f entre m e n. Retiremos desta bijeção o último par $(m-1, n-1)$. A função que resulta $f(\setminus\{(n-1, m-1)\}$ é uma bijeção de $n-1$ em $m-1$, contradizendo a minimalidade de n.
2. $X \subseteq n$ está bem ordenado pela ordem em n. Assim, $X = \{x_0, \ldots, x_k\}$ para algum k. Logo, $X \approx k + 1$.

Os itens 3, 4 e 5 são consequências de 1 e 2. □

Teorema 18.

1. *Seja* $a \in \mathbb{N}$ *(fixo). Então* $\mathbb{N} \approx \{n + a : n \in \mathbb{N}\}$.
   a) *Em particular, para* $a = 1, \mathbb{N} \approx \{n + 1 : n \in \mathbb{N}\} = \{1, 2, 3, \ldots\ldots\}$.
2. *O conjunto de números pares é equipolente a* $\mathbb{N}$.
3. *O conjunto de números impares é equipolente a* $\mathbb{N}$.

Prova. Para cada caso exibimos uma função biunívoca f que estabelece a equipolência.

1. $f : \mathbb{N} \longrightarrow \{n + a : n \in \mathbb{N}\}$, com $f(n) = n + a$.
2. $f : \mathbb{N} \longrightarrow \{2n : n \in \mathbb{N}\}$, com $f(n) = 2n$.
3. $f : \mathbb{N} \longrightarrow \{2n + 1 : n \in \mathbb{N}\}$, com $f(n) = 2n + 1$.

□

Estaremos interessados em determinar o número de fórmulas de uma linguagem formal contável.

Os teoremas seguintes estão orientados para esse fim.

Teorema 19.

1. $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.
2. O produto cartesiano de contáveis é contável. $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

Prova.

1. Cada natural n tem uma expressão única da forma $n = 2^j(2^k + 1)$, com $j, k \in \mathbb{N}$. Esta expressão provê a requerida bijeção.
2. Consequência de 1.

□

Teorema 20. *A união de um número finito de conjuntos finitos é finita.*

Prova.

Caso 1.

A intersecção de dois conjuntos diferentes é vazia.
Indução sobre o número n de conjuntos.
Para $n = 0, 1, 2$, é trivial: Se $A_1 \approx i$ e $A_2 \approx j$, $A_1 \cup A_2 \approx i + j$.
Suposto válido para n,

$$\bigcup_{i=1}^{i=n+1} A_i = (\bigcup_{i=1}^{i=n}) A_i \cup A_{n+1}$$

A finitude da união segue do caso $n = 2$.

Caso 2.

Se há intersecções não vazias, podemos separar a união em partes que não intersectam do modo que se mostra, neste exemplo, para $n = 4$.
Temos os conjuntos A_1, A_2, A_3, A_4.
Formamos $A_1 \cup (A_2 \setminus A_1) \cup (A_3 \setminus (A_1 \cup A_2)) \cup (A_4 \setminus (A_1 \cup A_2 \cup A_3))$.
É claro que os elementos desta união não intersectam e que é igual a $A_1 \cup A_2 \cup A_3 \cup A_4$.

O caso geral para qualquer número de conjuntos está definido recursivamente por

$$\bigcup_{n=1}^{n+1} = A_1 \cup (A_2 \setminus A_1) \cup (A_3 \setminus (A_1 \cup A_2)) \cup \cdots$$
$$\cdots \cup (A_{n+1} \setminus (A_1 \cup A_2 \cdots \cup A_n)$$

Tendo aqui uma união de conjuntos que não intersectam, aplicamos o Caso 1 aos componentes da união.

□

O próximo teorema estabelece que um conjunto é finito se, e somente se, é limitado superiormente.

Teorema 21. *Se $B \subseteq \mathbb{N}$, então*

$$(\exists N \in \mathbb{N})(\forall x \in B)(N > x) \iff (\exists n \in \mathbb{N})(X \approx n).$$

Prova.

Da direita para a esquerda, não há nada para demonstrar.

Para o outro sentido, seja $N \in \mathbb{N}$ o primeiro elemento de $\mathbb{N}$ tal que para todo o $x \in B$ tem-se $N > x$. Para demonstrar que há um $n \in \mathbb{N}$ tal que $B \approx n$, simplesmente contamos os elementos de B em ordem crescente, e o número a seguir será o pretendido n.

Isto é trivial, mas em rigor é preciso definir por recursão uma função definida em $\mathbb{N}$. Esta função atribuirá em ordem crescente um natural a cada elemento de B. A contagem terminará ao chegar ao primeiro elemento N de $\mathbb{N}$ que não está em B. Após terminar a contagem, manter-se-á constante para o resto de $\mathbb{N}$. Com esta ideia, definamos $f : \mathbb{N} \longrightarrow B$ por:

$$f(0) = \text{ o } 1^{\text{o}} \text{ elemento } x \text{ de } \mathbb{N} \text{ tal que } x \in X \text{ e}$$

$$f(n+1) = \begin{cases} \text{o } 1^{\text{o}}\ x \in B \text{ tal que } x > f(n), & \text{se } f(k) < N \\ N, & \text{se } f(n) \geq N \end{cases}.$$

Claramente:

$$f \text{é bijectiva,}$$
$$\{k : f(k) \leq N\} \in \mathbb{N} \text{ e}$$
$$n = \{k : f(k) \leq N\}$$

é o número n procurado. □

Intuitivamente, é claro que um subconjunto de $\mathbb{N}$ deve ser finito ou contável, assunto tratado no

Teorema 22.

1. $\forall B \subseteq \mathbb{N}[(B \text{ é finito}) \vee (B \approx \mathbb{N})]$.
2. $Cont(A) \Longrightarrow \forall B \subseteq A[(B \text{ é finito}) \vee (B \approx A)]$.

Prova.

1. Seja $B \subseteq \mathbb{N}$ e suponhamos que B não é finito. Então B não é limitado superiormente e para cada elemento $x \in B$ existe um $y \in B$ com $y > x$. Isso quer dizer que a contagem não para nesse N. Sendo assim, definamos por recorrência a função $g : \mathbb{N} \longrightarrow X$:

$$g(0) = \text{ o } 1^{\text{o}} \text{ elemento } x \text{ de } B.$$

$$g(n+1) = \text{o } 1^{\text{o}}\ x \in X \text{ tal que } x > g(n).$$

Em resumo $\neg(B \text{ é finito}) \Longrightarrow (B \approx \mathbb{N})$.

2. Se A é contável, é equipolente a $\mathbb{N}$. Um subconjunto de A é a imagem de um subconjunto B de $\mathbb{N}$. Por 1, B é finito ou contável. Portanto a sua imagem por uma função biunívoca é finita ou contável. □

Um conjunto infinito A pode ser do tamanho de $\mathbb{N}$ ou pode ser maior. O seguinte teorema diz que para não exceder o tamanho de $\mathbb{N}$ é necessário e suficiente que haja uma epijeção de $\mathbb{N}$ sobre A. Este teorema é uma ferramenta útil para estabelecer resultados posteriores, como se verá.

Teorema 23.

$$Cont(A) \Longleftrightarrow (A \text{ é infinito}) \wedge \exists f[(f : \mathbb{N} \longrightarrow A) \wedge (f \text{ é epijetiva})].$$

Prova.

Para a parte $\Longrightarrow$ não há nada para demonstrar.

Para a parte $\Longleftarrow$ seja $f : \mathbb{N} \longrightarrow A$, epijetiva.

Pela escolha de f, todo elemento de A é imagem de um elemento de $\mathbb{N}$.

Definamos $g : A \longrightarrow \mathbb{N}$ do seguinte modo: para cada $y \in A$, seja $g(y) =$ o 1^{o} elemento de $\mathbb{N}$ tal que $f(x) = y$.

Claramente g é injetiva e $g[A] \subseteq \mathbb{N}$.

Pelo teorema anterior, $g[A]$ é contável.

Pela bijectividade de g em $g[A]$, A é contável.

□

Teorema 24. *A união de dois conjuntos contáveis é contável.*

Prova. Sejam A e B contáveis, $A \approx \mathbb{N}$ e $B \approx \mathbb{N}$.

Caso 1. $A \cap B = \emptyset$

$A \approx \{2n : n \in \mathbb{N}\}$ e $B \approx \{2n+1 : n \in \mathbb{N}\}$. Ou seja, há bijecções:

$f : \{2n : n \in \mathbb{N}\} \longrightarrow A$ e
$g : \{2n+1 : n \in \mathbb{N}\} \longrightarrow B$.
Definimos $h : \mathbb{N} \longrightarrow A \cup B$ assim:

$$h(n) = \begin{cases} f(n), & \text{se } n \text{ é par.} \\ g(n), & \text{se } n \text{ é impar.} \end{cases}$$

Claramente, h é biunívoca, o que mostra a afirmação.

Caso 2. $A \cap B \neq \emptyset$.

Sabemos $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$.

Caso 2.a) $Cont(A \setminus B) \wedge Cont(A \cap B) \wedge Cont(B \setminus A)$.

Nesse caso, $A \setminus B \approx \{3k : k \in \mathbb{N}\}$.
Logo, há bijeção $f : A \setminus B \longrightarrow \{3k : k \in \mathbb{N}\}$.
$A \cap B \approx \{3k+1 : k \in \mathbb{N}\}$.
Logo, há bijeção $g : A \cap B \to \{3k+1 : k \in \mathbb{N}\}$.
$B \setminus A \approx \{3k+2 : k \in \mathbb{N}\}$.
Logo, há bijeção $h : B \setminus A \to \{3k+2 : k \in \mathbb{N}\}$.
Definamos

$$f(x) = \begin{cases} g(x) & \text{se } x \in A \setminus B \\ h(x) & \text{se } x \in A \cap B \\ i(x) & \text{se } x \in inB \setminus A \end{cases}$$

Claramente f é uma bijeção, demonstrando a afirmação do teorema.

Há outros casos como, por exemplo,

Caso 2.b) $A \setminus B$ é finito, $A \cap B$ é contável e $B \setminus A$ é contável, etc. Esses casos são tratados aplicando teoremas anteriores.

□

TEOREMA 25. *A união contável de contáveis é contável. (isto é, a reunião dum número contável de conjuntos contáveis é contável).*

Prova.

Seja $\mathcal{A}$ um conjunto contável de conjuntos contáveis, $\mathcal{A} = \{A_n : n \in \mathbb{N}\}$. Observar que para cada n, $A_n \approx \mathbb{N} \approx \{(n, x) : x \in \mathbb{N}\}$ e isso pode ser visualizado por meio deste quadro:

$$\mathcal{A} \approx \begin{cases} \{(0,0),(0,1),(0,2),\ldots\ldots\}(\approx A_0) \\ \{(1,0),(1,1),(1,2),\ldots\ldots\}(\approx A_1) \\ \{(2,0),(2,1),(2,2),\ldots\ldots\}(\approx A_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}.$$

O quadro mostra que $\mathcal{A} \approx \mathbb{N} \times \mathbb{N}$ e que $\bigcup \mathcal{A} \approx \mathbb{N}$.

Formemos o conjunto $\widetilde{\mathcal{A}} = \{A_i \times \{A_i\} : i \in \mathbb{N}\}$ e para visualizar a situação vejamos em como está formada a parte de $\overline{\mathcal{A}}$ para $n = 2$:

$$A_2 = \{a_{20}, a_{21}, a_{22}, a_{23} \ldots\ldots\}.$$

$$A_2 \times \{A_2\} = \{\langle a_{20}, A_2, \rangle, \langle a_{21}, A_2, \rangle, \langle a_{22}, A_2, \rangle, \langle a_{23}, A_2, \rangle \ldots\ldots\}.$$

Os conjuntos em $\widetilde{\mathcal{A}}$ não intersectam, pois os A_i's são diferentes entre si.

Mostramos que existe uma função sobrejetiva $f : \widetilde{\mathcal{A}} \longrightarrow \bigcup \mathcal{A}$. Definamos

$$f : \widetilde{\mathcal{A}} \longrightarrow \bigcup_{i \in \mathbb{N}} A_i \text{ por } f(\langle a_{nk}, A_n, \rangle) = a_{nk}.$$

Claramente f é uma função; com efeito,

$$f(\langle a_{ni}, A_n \rangle) \neq f(\langle a_{mj}, A_m \rangle) \longrightarrow \langle a_{ni}, A_n \rangle) \neq \langle a_{mj}, A_m \rangle$$

pois, se $f(\langle a_{ni}, A_n \rangle) = a_{ni}$ e $f(\langle a_{mj}, A_n \rangle) = a_{mj}$ são diferentes, então $a_{ni} \neq a_{mj}$.

Note-se que se os A_i's não intersectam, f é biunívoca. E, se houver A_i's que intersectam como, por exemplo, $A_2 \cap A_5 \neq \emptyset$ com $a_{29} = a_{57}$, então $f(\langle a_{29}, A_2, \rangle) = f(\langle a_{57}, A_5, \rangle)$.

Logo, $\mathcal{A}$ é contável. □

Números ordinais

Viramos agora a atenção para um conceito que generaliza aquele de número natural.

Um número ordinal é um conjunto provido da relação de pertencimento que

(i) É bem fundado com $\in$, isto é, todo subconjunto não vazio tem um elemento minimal.
(ii) É transitivo, ou seja, todo elemento dele é um subconjunto dele.
(iii) Satisfaz a lei de tricotomia para $\in$.

Formalmente:

Definição 24. *Um conjunto x é um número ordinal, $Ord(x)$, sse*

1. $(\forall y \subseteq x)[y \neq \emptyset \longrightarrow \exists a(\forall z \in y)(z \notin a)]$.
2. $(\forall y \in x[(y \in x) \longrightarrow (y \subseteq x)]$, $(Trans(x))$.
3. $(\forall u, v \in x)[(u \in v) \vee (u = v) \vee (v \in u)]$. *(Tricotomia)*

É costume usar letras gregas minúsculas $\alpha, \beta, \gamma, ...$ como variáveis para ordinais. Com esta convenção, $\forall \alpha \varphi(\alpha)$ significa $\forall x(Ord(x) \longrightarrow \varphi(x))$ e $\exists \alpha \varphi(\alpha)$ significa $\exists x[Ord(x) \wedge \varphi(x)]$.

Estudaremos dos números ordinais as propriedades que nos interessam. Após as propriedades de números naturais e ω, é imediato que todo número natural é um ordinal, e que ω é um número ordinal.

TEOREMA 26. $(\forall x \in \omega)[Ord(x)]$ *e* $Ord(\omega)$.

TEOREMA 27. $\alpha \notin \alpha$.

Prova. Suponha-se que $\alpha \in \alpha$. Então $\{\alpha\} \subseteq \alpha$. Essa suposição implica que $\{\alpha\}$ é um subconjunto de α que não tem elemento minimal, contrário á condição 2 da definição de ordinal. □

TEOREMA 28.

1. μ *é minimal em* $x \subseteq \alpha$ *se e só se* $\forall y \in x(y = \mu) \vee (\mu \in y)$.
2. *Um elemento minimal em* $x \subseteq \alpha$ *é único.*
3. *(*x *é bem fundado)* $\wedge$ *(*$\emptyset \neq y \subseteq x$*)* $\longrightarrow$ *(*y *é bem fundado).*
4. $\emptyset \neq y \subseteq \alpha \longrightarrow (y$ *é bem fundado).*

Prova.

1. Trivial.
2. Se μ e μ' são ambos minimais, então $\mu \in \mu'$ contradiz a minimalidade de μ'.
3. Seja $0 \neq z \subseteq y$. Logo $z \subseteq x$ e portanto existe $u \in z$ tal que para todo $v \in x, v \notin u$. *A fortiori*, para todo $v \in y$, $v \notin u$, isto é, v é minimal em y e todo subconjunto $\neq \emptyset$ de y tem um elemento minimal.
4. Imediato, por *3.*

□

Na lei de tricotomia cada uma das três possibilidades exclui as outras duas.

TEOREMA 29.

1. $x \in u \longrightarrow x \neq u \wedge u \notin x$.
2. $x = u \longrightarrow x \notin u \wedge u \notin x$.
3. $u \in x \longrightarrow x \neq u \wedge x \notin u$.

Prova. Se $(x \in u) \wedge (x = u)$, então o conjunto $\{x, u\}$ não tem elemento minimal, em contradição com a condição 2. na definição de ordinal. A prova para as demais cláusulas é semelhante à essa. □

TEOREMA 30. *μ é minimal em $x \iff (\mu \in x) \wedge \forall z \in x(z \neq \mu \longrightarrow \mu \in z)$.*

Prova. Por tricotomia, tem-se que:

$$\begin{aligned} \mu \text{ é minimal em } x &\iff (\mu \in x) \wedge \forall z \in x[z \notin \mu] \\ &\iff (\mu \in x) \wedge \forall z \in x[(z = \mu) \vee (\mu \in z)] \\ &\iff (\mu \in x) \wedge \forall z \in x[(z \neq \mu) \longrightarrow (\mu \in z)] \end{aligned}$$

□

TEOREMA 31. *$\alpha \in \beta \in \gamma \longrightarrow \alpha \in \gamma$.*

Prova. $\alpha \in \beta \in \gamma \longrightarrow \alpha \in \beta \subseteq \gamma$. Portanto $\alpha \in \gamma$. □

TEOREMA 32. *$\bigcup \alpha \subseteq \alpha$.*

Prova. Seja $x \in \bigcup \alpha$. Existe y tal que $x \in y \in \alpha$. A transitividade de α implica que $y \subseteq \alpha$. Daqui, $x \in \alpha$. □

TEOREMA 33. *$\neg\exists\beta[\alpha \in \beta \in (\alpha \cup \{\alpha\})]$.*

Prova. Suponhamos que $\exists\beta[\alpha \in \beta \in (\alpha \cup \{\alpha\})]$. Assim, como $\beta \in \alpha \cup \{\alpha\}$, tem-se $(\beta \in \alpha) \vee (\beta = \alpha)$.

- Se $\beta \in \alpha$, então $\alpha \in \alpha$.
- Se $\beta = \alpha$, então $\alpha \in \alpha$.

Ambos casos conduzem a contradição. □

O próximo teorema afirma que todos os elementos de um ordinal são também ordinais.

TEOREMA 34. *$\forall x \in \alpha[Ord(x)]$.*

Prova. Seja $x \in \alpha$ (a)

Devemos demonstrar que x cumpre com as três condições que definem um ordinal.

1. Claramente, x é bem fundado.
2. Como $\forall x, u \in \alpha[(x \in u) \vee (x = u) \vee (u \in x)] \longrightarrow \forall x, u \in x[(x \in u) \vee (x = u) \vee (u \in x)]$, claramente x satisfaz a lei de tricotomia.
3. Resta mostrar que x é transitivo. Isto é, que $z \in x \longrightarrow z \subseteq x$.
   - Sejam pois $u \in z \in x$. (b)
   - De (a) e $Trans(\alpha)$, vem $x \subseteq \alpha$.
   - Isso, com (b), dá $z \in \alpha$, o qual, com $Trans(\alpha)$ dá $z \subseteq \alpha$.

- Isto, com a parte $u \in z$ de (b) dá $u \in \alpha$.
- Ora, por tricotomia, $(x \in u) \vee (x = u) \vee (u \in x)$.
- $x \in u$ reunido com (b) dá $x \in u \in z \in x$, o que mostra que o conjunto $\{x, u, z\}$ não tem elemento minimal. Isto elimina a possibilidade $x \in u$.
- $x = u$ reunido com (b) dá $u = x \in z \in x$, mostrando que o conjunto $\{u, x, z\}$ não tem elemento minimal. Isto elimina a possibilidade $u = x$. Portanto, a única alternativa factível é $u \in x$.

Resumindo, $u \in z \in x \longrightarrow u \in x$, mostrando que $Trans(x)$.

□

O sucessor de um ordinal é também um ordinal.

Teorema 35.

1. $Ord(\alpha \cup \{\alpha\})$.
2. $\bigcup(\alpha \cup \{\alpha\}) = \alpha$.

Prova.

1. Demonstramos que $\alpha \cup \{\alpha\}$ é bem fundado. Seja $\emptyset \neq x \subseteq \alpha \cup \{\alpha\}$.
   - Se $x \subseteq \alpha$, então x tem elemento minimal.
   - Se $x = \{\alpha\}x$ tem α como elemento minimal.
   - Se $x \cap \alpha \neq \emptyset$ e $\alpha \in x$, seja μ o elemento minimal de x em $x \cap \alpha$.

   Afirmamos que μ é minimal em $\alpha \cup \{\alpha\}$.
   - Se não, seja μ' minimal em $\alpha \cup \{\alpha\}$.
   - Então $\mu' \in \mu$. Como $\mu \in \alpha$, $\mu' \in \alpha$. Também $\mu' \in x$, assim $\mu' \in x \cap \alpha$, logo μ' é minimal em $x \cap \alpha$, com o qual $\mu' = \mu$ e μ é minimal em $\alpha \cup \{\alpha\}$.
   - Claramente $\alpha \cup \{\alpha\}$ satisfaz a lei da tricotomia.

   Falta ver que $\alpha \cup \{\alpha\}$, é transitivo. Seja $x \in \alpha \cup \{\alpha\}$.
   - Se $x = \alpha$, $x \subseteq \alpha$.
   - Se $x \in \alpha$, $x \subseteq \alpha$. (Pois α é transitivo).
2. $\bigcup(\alpha \cup \{\alpha\}) = \bigcup\alpha \cup \bigcup\{\alpha\} = \bigcup\alpha \cup \alpha = \alpha$, pois $\bigcup\alpha \subseteq \alpha$.

□

Teorema 36. $Ord(\bigcup\alpha)$.

Prova.

- Mostramos que $\bigcup\alpha$ é bem fundado.

  Seja $\emptyset \neq x \subseteq \bigcup\alpha$.

  Como $\bigcup \subseteq \alpha$, $x \subseteq \alpha$.

  x tem um elemento minimal em α.

Logo x tem um elemento minimal em $\bigcup \alpha$.

- A lei de tricotomia é transmitida diretamente de $\bigcup \alpha$ para α.
- Demonstramos que $\bigcup \alpha$ é transitivo; isto é, que $x \in \bigcup \alpha \longrightarrow x \subseteq \bigcup \alpha$.

  Seja $u \in x$. Queremos $u \in \bigcup \alpha$.

  Com efeito, seja $u \in x$. (*)

  Existe y tal que $x \in y \in \alpha$.

  Daqui, $x \in y \subseteq \alpha$.

  Donde $x \in \alpha$.

  Com (*) isto dá $u \in x \in \alpha$, o que significa que $u \in \bigcup \alpha$.

Resumindo, $\bigcup \alpha$ satisfaz as três condições que definem um ordinal.

□

Um conjunto de ordinais não é necessariamente um ordinal, mas o é se o conjunto é transitivo.

TEOREMA 37. $(y \subseteq \alpha) \wedge Transit(y) \longrightarrow Ord(y)$.

Prova. Suponhamos o antecedente.

- Seja $\emptyset \neq x \subseteq y$

  Então $\emptyset \neq x \subseteq \alpha$.

  Por ser um subconjunto de um conjunto bem fundado, x tem elemento minimal.
- Sejam $u, v \in y$.

  Então $u, v \in \alpha$.

  α satisfaz a lei de tricotomia, portanto y também a satisfaz.
- $Transit(y)$ por hipótese.

Assim $Ord(y)$. □

Um subconjunto próprio e transitivo de um ordinal é elemento deste ordinal.

TEOREMA 38. $y \subsetneq \alpha \wedge Transit(y) \longrightarrow y \in \alpha$.

Prova.

Suposto o antecedente, temos $(\alpha \setminus y \neq \emptyset) \wedge (\alpha \setminus y \subseteq \alpha)$.

Seja v o minimal de $\alpha \setminus y$.

Então $(v \in \alpha) \wedge (v \notin y)$ (*)

Afirmamos: $v = y$. Disso, obter-se-á $y \in \alpha$ como requerido.

Seja $x \in v$. Isto, com (*) dá $x \in \alpha$.

Pela minimalidade de v em $\alpha \setminus y$ $x \notin \alpha \setminus y$.

Isto equivale a $(x \notin \alpha) \vee (x \in y)$.

Logo $v \subseteq y$. Também $v \subseteq y$. (**)

Seja agora $x \in y$ Queremos $x \in v$.

Como $y \subseteq \alpha$, $x \in \alpha$.

Tem-se, também, que $v \in \alpha$.

Logo $(v \in x) \vee (v = x) \vee (x \in v)$.

Se $v \in x$, por (**), $v \in y$, o que contradiz $v \in \alpha \setminus y$.

Se $v = x$, $(x \in \alpha) \wedge (x \notin y)$, o que contradiz (**).

Concluímos $x \in v$, com o qual $y \subseteq v$ e $y = v$.

Como $v \in \alpha$, $y \in \alpha$, completando a demonstração.

□

A intersecção de ordinais é um ordinal.

Teorema 39. *$Ord(\alpha \cap \beta)$.*

Prova. Demonstramos que a intersecção satisfaz as três condições que definem um número ordinal.

- α é bem-fundado.
  Como $\alpha \cap \beta \subseteq \alpha$, $\alpha \cap \beta$ é bem-fundado.
- Sejam $u, v \in \alpha \cap \beta$,
  $u, v \in \alpha$.
  α satisfaz a lei de tricotomia.
  Portanto $\alpha \cap \beta$ satisfaz a lei de tricotomia.
- Seja $x \in \alpha \cap \beta$ e $x \in \alpha$. Logo $x \subseteq \alpha$.
  $x \in \beta$, portanto $x \subseteq \beta$.
  Logo $x \subseteq \alpha$ e $x \subseteq \beta$. Assim $x \subseteq \alpha \cap \beta$.

□

Teorema 40.

1. $(\alpha \cap \beta = \alpha) \vee (\alpha \cap \beta \in \alpha)$.
2. $(\alpha \cap \beta = \beta) \vee (\alpha \cap \beta \in \beta)$.

Prova.

1. Tem-se que $(\alpha \cap \beta \subsetneq \alpha) \wedge Transit(\alpha \cap \beta) \longrightarrow \alpha \cap \beta \in \alpha$. Portanto, $(\alpha \cap \beta = \alpha) \vee (\alpha \cap \beta \in \alpha)$.
2. Semelhante ao caso anterior.

□

Teorema 41. *$\forall y \in xOrd(y) \longrightarrow x$ é bem fundado.*

Prova. Seja $\emptyset \neq u \subseteq x$. Mostramos que u tem elemento minimal.

Seja $\alpha \in u$. Considere-se $\alpha \cap u$.

Como $\alpha \cap u \subseteq \alpha$, $\alpha \cap u$ é bem fundado.

Se $\alpha \cap u = \emptyset$, α, então é minimal em u.

Se $\alpha \cap u \neq \emptyset$, então $\alpha \cap u$ tem um elemento minimal μ.

μ é um elemento minimal de u em $\alpha \cap u$.

Também μ é um elemento minimal de u. Se não, seja $\mu' \in u$ tal que $\mu' \in \mu \in u$.

Então $\mu' \in \alpha$, contradizendo a escolha de μ.

□

TEOREMA 42. *Todo conjunto não vazio de ordinais tem um elemento minimal.*

Prova. Seja A um conjunto não vazio de ordinais.

Seja $\gamma \in A$ e $B = \{\alpha \in A : \alpha \in \gamma\}$. Obviamente $B \subseteq \gamma$.

Se $B = \emptyset$, γ é minimal em A.

Se $B \neq \emptyset$, como γ é bem fundado, assim o é B.

Portanto B tem um elemento minimal $\mu \in B$.

Afirmamos que μ é minimal em A.

Se não, seja $\delta \in A$ tal que $\delta \in \mu$.

Então $\delta \in \mu \in \gamma$. Daqui $\delta \in \gamma$.

Logo $\delta \in B$, o que contradiz a minimalidade de μ em B.

Logo, μ é minimal em A.

□

Os ordinais respondem a lei de tricotomia. Observa-se que isso não é o mesmo que afirmar que a lei de tricotomia seja válida *dentro* de um ordinal.

TEOREMA 43. $(\alpha \in \beta) \vee (\alpha = \beta) \vee (\beta \in \alpha)$.

Prova. Considere-se o conjunto $\{\alpha, \beta\}$.

Se $\alpha \neq \beta$, então $\{\alpha, \beta\}$ tem um elemento minimal.

Este deve ser α, ou deve ser β. No primeiro caso $\alpha \in \beta$. No segundo caso, $\beta \in \alpha$.

Logo $(\alpha \in \beta) \vee (\alpha = \beta) \vee (\beta \in \alpha)$.

□

O teorema a seguir mostra que a reunião de um conjunto de ordinais é um ordinal.

TEOREMA 44. $(\forall y \in x)Ord(y) \longrightarrow Ord(\bigcup x)$.

Prova. Suponhamos $(\forall y \in x)Ord(y)$.

- Veremos que $\bigcup x$, é bem fundado.

  Primeiro, observe-se que $\bigcup x$ é um conjunto de ordinais. Com efeito, seja $v \in \bigcup x$.

  Então para certo α $v \in \alpha \in x$. (x é um conjunto de ordinais). Claramente $Ord(v)$. Assim $\bigcup x$ é um conjunto de ordinais.

  Daqui, $\bigcup x$ é bem fundado.
- Sejam $u, v \in \bigcup x$. Pelo dito acima, $Ord(u) \wedge Ord(v)$, portanto a lei de tricotomia vale em $\bigcup z$.
- $\bigcup x$ é transitivo. Seja $v \in \bigcup x$; demonstramos que $v \subseteq \bigcup x$.

  Seja $u \in v$.

  Então $u \in v \in \alpha \in x$, para certo α.

  Daqui, $u \in v \subseteq \alpha \in x$, para certo α.

  Donde $u \in \alpha \in x$, para certo α.

  O que significa que $u \in \bigcup x$ e que $v \subseteq \bigcup x$.

□

O próximo teorema tem especial importância como se verá na parte da Completude da Lógica de Primeira Ordem.

TEOREMA 45. $\left[\alpha = \bigcup \alpha\right] \vee \left[\alpha = \bigcup \alpha \cup \{\bigcup \alpha\}\right]$

Prova. Suponhamos $\alpha \neq \bigcup \alpha$. Demonstramos $\alpha = \bigcup \alpha \cup \{\bigcup \alpha\}$.

Sabemos que $\bigcup \alpha \subseteq \alpha$ e que $Ord(\bigcup \alpha)$.

Logo $\bigcup \alpha \in \alpha$.

Donde $\bigcup \alpha \cup \{\bigcup \alpha\} \subseteq \alpha$.

Para demonstrar a inclusão no sentido contrário, seja $\delta \in \alpha$.

Suponhamos $\delta \notin \bigcup \alpha \cup \{\bigcup \alpha\}$.

Isto é $(\delta \notin \bigcup \alpha) \wedge (\delta \neq \bigcup \alpha)$. (*)

Por tricotomia, $\bigcup \alpha \in \delta$.

Como $\delta \in \alpha$, $\delta \subseteq \bigcup \alpha$.

Por outro lado, de $\bigcup \alpha \in \delta$ infere-se $\bigcup \alpha \subseteq \delta$.

Daqui $\delta = \bigcup \alpha$.

Isto contradiz $\delta \neq \bigcup \alpha$ em (*).

□

O teorema mostra as duas formas que pode adotar um ordinal: a primeira chama-se de *limite*; a segunda, a de *sucessor* com a qual já estamos familiarizados. Observe-se que a forma de um ordinal sucessor não é outra coisa do que o sucessor do seu antecessor, como se pode apreciar por exemplo em $7 = 6 \cup \{6\}$. É fácil ver que um ordinal α é limite sse para todo $\beta \in \alpha$ tem-se $\beta \cup \{\beta\} \in \alpha$. É habitual escrever "$<$" em lugar de "$\in$" e $Lim(\alpha)$ para "α é *limite*".

DEFINIÇÃO 25. $Lim(\alpha) \Longleftrightarrow \forall\beta \in \alpha(\beta \cup \{\beta\}) \in \alpha$.

Há diferentes maneiras equivalentes de conceber ordinais limite. Estas, fáceis de demonstrar, estão dadas no

TEOREMA 46. *As quatro seguintes expressões são equivalentes.*

1. $Lim(\alpha)$.
2. $(\forall\beta \in \alpha)(\exists\gamma \in \alpha)(\beta \in \gamma)$.
3. $\forall\beta \in \alpha(\beta \cup \{\beta\}) \in \alpha$.
4. $\alpha \subseteq \bigcup \alpha$.

Prova. Exercício. □

Há versões específicas dos princípios de indução e recursão para ordinais.

Princípio de Indução para ordinais. .

Sejam κ um ordinal e φ uma fórmula de primeira ordem.

Se

a) φ é satisfeita por $\emptyset$,
b) toda vez que é satisfeita por um ordinal (sucessor), é satisfeita pelo seu sucessor e
c) dado um ordinal limite, se é satisfeita por todos os seus antecessores é também satisfeita pelo mencionado ordinal limite,

então

d) φ é satisfeita por todos os ordinais menores do que κ.

Em símbolos:

$$\varphi(\emptyset) \wedge \forall\alpha[\varphi(\alpha = \beta \cup \{\beta\}) \longrightarrow (\varphi(\beta) \longrightarrow \varphi(\alpha))] \wedge$$
$$\wedge \forall\beta[Lim(\beta) \wedge (\forall\gamma < \beta)\varphi(\gamma) \longrightarrow \varphi(\beta))] \longrightarrow (\forall\alpha \in \kappa)\varphi(\alpha)$$

Princípio de recorrência para ordinais.

Se

a) κ um ordinal e S um conjunto,
b) $g(\emptyset) = s$, para certo $s \in S$ e
c) $h : \mathcal{P}(S) \longrightarrow S$,

então existe uma única função $f : \kappa \longrightarrow S$ tal que
- se $\alpha = \emptyset$, então $f(\emptyset) = g(\emptyset)$,
- se $\alpha = \beta \cup \{\beta\}$, então $f(\alpha) = h(f(\beta))$ e
- se α é limite, então $f(\alpha) = f(\bigcup \alpha) = h(\{f(\beta) : \beta < \alpha\})$.

Não usaremos aqui o Princípio de Indução. O Princípio de Recorrência será utilizado na parte da Completude da Lógica de Primeira Ordem, especificamente na "henkinsação" de uma teoria.

A restrição a um ordinal κ tem a ver com a aplicação especifica que faremos do Princípio de Recorrência. Ambos princípios podem ser estendidos a todos os ordinais, mas em tal caso estamos a tratar com a classe própria dos ordinais, assunto que está para além do que nos interessa aqui.

Na discussão que está a seguir vamos tonar preciso o resultado conhecido como Teorema de Cantor.

O teorema de Cantor afirma que o tamanho da potência de um conjunto A é estritamente maior do que o de A. Escrevendo $\prec$ para indicar "estritamente maior do que",

Teorema 47 (Cantor). $A \prec \mathcal{P}(A)$.

Prova.

1. A função $\mathcal{P}(A)$ definida por $f(x) = \{x\}$ é injetiva e mostra que $A \precsim \mathcal{P}(A)$.
2. Falta mostrar que $A \not\approx \mathcal{P}(A)$:

   Suponha-se o contrário e seja $g : A \longrightarrow \mathbb{P}(A)$ uma bijeção.

   Ponha-se $B = \{a \in A : a \notin g(a)\}$.

   Se $a \in A$, então claramente $a \in B \iff a \notin g(a)$ (*)

   Uma vez que g é bijectiva e $B \in \mathcal{P}(A)$, B é imagem de algum $a \in A$: $B = g(a)$.

   Por (*) , $a \in B \iff a \notin g(a)$, isto é, $a \in B \iff a \notin B$.

   Esta contradição completa a demonstração.

□

Para além de ω. Já vimos que o sucessor de um ordinal é também um ordinal. Do facto de o sucessor de um ordinal ser também um ordinal, resulta que os ordinais vão para além de ω. Abreviando $\omega \cup \{\omega\}$ por $\omega + 1$, etc:

$$0, 1, 2, \ldots\ldots\ldots \omega, \omega + 1, \omega + 2, \ldots\ldots$$

É fácil demonstrar que

Teorema 48. $\omega \approx \omega + 1$.

Prova. A demonstração segue as mesmas linhas da de $\mathbb{N} \approx \mathbb{N} \cup a$. □

Definindo, para $n \geq 2$, $\omega + n = \omega(n-1) + 1$, do teorema infere-se que

$$\omega + 1 \approx \omega + 2 \approx \omega + 3 \approx ...$$

Após estes novos ordinais temos, ainda, $\omega + \omega$ definido por

$$\omega + \omega = \bigcup\{\omega + n : n \in \omega\}.$$

Teorema 49.

1. $\omega + n \approx \omega$.
2. $\omega + \omega \approx \omega$.

Definindo $\omega+\omega+\omega = \bigcup\{\omega+\omega+n : n \in \omega\}$ tem-se que $\omega \approx \omega+\omega \approx \omega+\omega+\omega$ e assim sucessivamente.

Estas operações com ω continuam a produzir novos ordinais, maiores que, *mas equipolentes com,* ω.

Se pensarmos que uma função dos números é medir o tamanho dos conjuntos, nos perguntamos se há números apenas para conjuntos finitos ou contáveis.

Por uma parte, o Teorema de Cantor (ver no próximo Capítulo) diz que dado um conjunto há sempre conjuntos de tamanho estritamente maior do que ele. Por outra parte, um resultado afirma que todo conjunto é equipolente a um ordinal. Isto conduz a definir certos números ordinais que não são equipolentes a nenhum ordinal menor do que eles e que, portanto, são estritamente maiores do que eles. Definimos, assim, um **número cardinal** como um ordinal não equipolente com nenhum dos ordinais anteriores. Um número cardinal é também chamado de **ordinal inicial**, devido ao fato que a partir dele começam a surgir ordinais equipolentes a ele.

Com esta definição, resulta que os números naturais e ω são números cardinais, mas não $\omega + n$ para $n \in \omega$, não $\omega + \omega$, e, como se poderá ver, há muitos outros. O primeiro cardinal após ω é denotado por $\aleph_1$, o segundo por $\aleph_2$ e assim sucessivamente. Dado um ordinal α, o α-ésimo cardinal é $\aleph_\alpha$. ω entra nessa lista de cardinais como $\aleph_0$.

Deste modo, surge a hierarquia dos números transfinitos:

$$\aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\alpha, \ldots$$

Com esta notação, a parte 2. do teorema anterior pode escrita como

$$\aleph_0 + \aleph_0 = \aleph_0$$

Contar os elementos de um conjunto é estabelecer uma bijeção entre um número e o conjunto, e tal como com os naturais contamos o número de elementos

de conjuntos finitos, com ω podemos contar conjuntos equipolentes a ele, que temos definido como 'contáveis'. Devido à equipolência entre ω e alguns dos ordinais maiores do que ele, o número de elementos de um conjunto contável é definido como o *primeiro* ordinal equipolente a ele. Este ordinal é ω

Seguindo a mesma ideia podemos definir o número de elementos de um conjunto qualquer como o *primeiro* ordinal equipolente a ele. Isto conduz à definição de *número cardinal*.

Definição 26.

$$Card(x) \Longleftrightarrow [Ord(x) \wedge \forall(y)(Ord(y) \wedge y \in x \longrightarrow (y \not\approx x)]$$

Usando variáveis ordinais: $Card(\alpha) \Longleftrightarrow [\forall\beta(\beta \in \alpha \rightarrow \beta \not\approx \alpha]$.

$Card(\alpha)$ lê-se "α é cardinal". Todos os naturais e ω são números cardinais. $\omega + 1, \omega + 2, \ldots$ não o são. Quando o interesse é em se referir a ω como um número cardinal, emprega-se o nome de $\aleph_0$.

O teorema de Cantor diz que há conjuntos infinitos de tamanho arbitrariamente grandes. Consequentemente, é de esperar que haja cardinais arbitrariamente grandes, dando lugar a uma hierarquia de cardinais transfinitos:

$$\aleph_0, \aleph_1, \aleph_2, \aleph_3, \ldots\ldots, \aleph_\alpha, \ldots$$

$\aleph_0$ é o primeiro cardinal infinito; $\aleph_0 = \omega$. $\aleph_1$ é o primeiro ordinal estritamente maior que $\aleph_0$. $\aleph_2$ é o primeiro ordinal estritamente maior que $\aleph_1$, e assim por diante.

Dado um ordinal α, $\aleph_\alpha$ é o α-ésimo cardinal transfinito.

Vamos precisar, no volume 2, de um resultado que é fácil de captar intuitivamente e que apresentamos aqui sem demonstração por involver elementos da teoria de cardinais, o que vai para além do pretendido neste livro.

Teorema 50. *Se κ é qualquer cardinal infinito e A é um conjunto de cardinalidade κ, então*

1. *para qualquer $n \in \mathbb{N}$, tem-se que $\kappa^n \approx \kappa$.*
2. *$A \approx A^n$.*

O teorema diz que o conjunto de sequências finitas de um conjunto A de cardinalidade κ tem cardinalidade κ, isto é, $Card(A^n) = Card(A)$. No caso de $Card(A) = \aleph_0$, tem-se que o conjunto de sequências finitas de elementos de A é de cardinalidade $\aleph_0$.

Observe-se que simplesmente "definir" os $\aleph$'s não faz com que eles existam. Sua existência requer algumas preparações.

Boa ordenação, Axioma da Escolha e Lema de Zorn. Com a hierarquia dos $\aleph$'s esperamos estabelecer o número de elementos de qualquer conjunto A, mas isto equivale a estabelecer que há uma bijeção entre A e algum ordinal que por sua vez será equipolente a algum $\aleph$. Para estabelecer que há essa bijeção é preciso que A esteja bem ordenado, ou que se possa bem ordená-lo - tão bem ordenado quanto o ordinal ao qual deve ser equipolente. Sem a bijeção não há contagem. Mais, essa bijeção deve ser um isomorfismo. Que tal boa ordem sempre pode ser obtida foi demonstrado por Zermelo no

Teorema 51 (Boa ordenação. Zermelo, 1904). *Todo conjunto pode ser bem ordenado. Em símbolos:* $(\forall X)(\exists R)[(R \subseteq X \times X) \wedge (R \text{ é uma boa ordem})]$.

Para demonstrar isso Zermelo formulou e adotou como axioma outro princípio, conhecido como *Axioma de Escolha*. Este afirma que *dado qualquer conjunto A de conjuntos não vazios existe um novo conjunto que escolhe um elemento de cada conjunto em A.*

Em linguagem matemática, a frase *'escolhe um elemento de cada conjunto de A'* significa que *'há uma função que a cada elemento y de A associa um elemento do mesmo y'*. Em símbolos:

Axioma da Escolha (Zermelo, 1904). $(\forall X)[(\forall y)(y \in X \longrightarrow y \neq \emptyset) \longrightarrow (\exists f)[(f \text{ é uma função}) \wedge (Dom(f) = X) \wedge (\forall y \in X)(f(y) \in y]$.

É trivial que o Teorema de Zermelo implica o Axioma de Escolha, pois se os conjuntos podem ser bem ordenados, basta definir f como a função que associa a cada um deles o seu primeiro elemento. Por outra parte, demonstra-se que o Axioma da Escolha implica o Teorema de Zermelo. Com isso, resulta que o Teorema de Zermelo e o Axioma de Escolha são equivalentes.

O teorema de Cantor garante que sempre é possível encontrar conjuntos de maior tamanho do que um conjunto dado. O Axioma da Escolha garante que todo conjunto é bem ordenado; isto implica que todo conjunto é equipotente a um ordinal. Desses dois fatos se segue que há ordinais de qualquer tamanho: Dado um ordinal, sempre há ordinais de tamanhos maiores. Graças ao Axioma da Escolha, a existência dos $\aleph$'s fica estabelecida.

Intimamente relacionado com ambos há um terceiro teorema conhecido como *Lema de Zorn*, que se refere a conjuntos parcialmente ordenados. Ele será usado no estudo das propriedades dos sistemas lógicos.

Lema de Zorn. *Todo conjunto não vazio, parcialmente ordenado, e no qual toda a cadeia está limitada superiormente, tem um elemento maximal.*

O Lema de Zorn resulta ser equivalente ao Axioma de Escolha e também ao Teorema de Boa Ordenação.

$$\boxed{\text{Axioma da Escolha} \iff \text{T. de Boa Ordenação} \iff \text{Lema de Zorn}}$$

Estas equivalências são apenas mencionadas aqui; para os efeitos deste curso, basta uma compreensão do seu significado e importância.

Há versões mais débeis do Axioma da Escolha, que são implicadas por este (mas não o contrário). Dessas, nos interessa uma que será utilizada mais à frente, na parte de Cálculo Proposicional. Trata-se do Axioma da Escolha Dependente. O axioma consiste em obter escolhas numa sequência, de maneira que a escolha em algum ponto da sequência depende de escolhas feitas previamente.

O Axioma da Escolha Dependente. Digamos que uma relação binária R sobre um conjunto X é *total*, se $(\forall x \in X)(\exists y \in U)(xRy)$.

Teorema 52 (Axioma da Escolha Dependente). *Sejam X um conjunto não vazio, $R \subseteq X \times X$ tal que R é total. Então existe uma sequência $\langle x_n \rangle_{n\in\mathbb{N}}$ tal que $x_n R x_{n+1}$.*

Prova. Considere o conjunto $\{R[x] : x \in X\}$. Este consiste dos conjuntos $R[x]'s$ (com $x \in X$) não vazios. Pelo Axioma da Escolha, existe uma função

$$f : \{R[x] : x \in X\} \longrightarrow \bigcup[\{R[x] : x \in X\}], \text{ tal que } f(R[x]) \in R[x].$$

A ideia da prova é como segue.

1. Escolha-se um elemento de X. Este será nosso x_o.
2. Forme-se $R[x_0]$.
3. Dentro de $R[x_0]$ encontre-se o elemento determinado pela função escolha, f. Este será nosso x_1.
4. Com este x_1, volta-se para 1. e aplica-se-se o passo 2.

Continue-se de este modo repetindo o ciclo 1, 2, 3, 1, 2, 3, 1, 2, ...

Indo para as formalidades,

- inicie com $x_0 = x$.
- Forme $f(R[x]) = (f \circ R)[x])$.
- Forme, sucessivamente, $(f \circ R)^2[x], (f \circ R)^3[x], \ldots, (f \circ R)^n[x], \ldots$.
- Ponha-se $x_n = (f \circ R)^n[x]$.

A sequência $\langle x_n \rangle_{n\in\mathbb{N}}$ é a sequência requerida. □

Esquema Irrestrito de Compreensão (revisitado). O Paradoxo de Russell. O princípio de que uma propriedade permite formar o conjunto dos elementos com essa propriedade tem sido até agora adotado e usado aqui devido a que se apresenta ao entendimento de maneira razoável e natural. Graças a ele, temos livremente construído ou feito referência a uma diversidade de conjuntos. Porém, não deve ser aplicado sem limitações, como mostram os exemplos a seguir.

Observe-se que o universo dos ordinais satisfaz as condições de um ordinal. Naturalmente esta situação leva a pensar que o universo dos ordinais é ele próprio um ordinal.

Seja ORD o universo dos ordinais, i.e, $ORD = \{x : Ord(x)\}$. A conjectura de que ORD é um ordinal equivale a $ORD \in ORD$, colidindo com o Teorema $\alpha \notin \alpha$. Isto demonstra que o universo de todos os ordinais não é um ordinal: a fórmula $Ord(x)$ não define um conjunto. Quer dizer que o esquema irrestrito de compreensão é ilegítimo e que é preciso estabelecer algum critério que limite o campo de fórmulas que definem conjuntos.

TEOREMA 53. $\neg\exists x[\forall y(y \in x) \longleftrightarrow Ord(y)]$.

Prova. Apresentada acima. □

O paradoxo de Russell.

Observe-se que se $A = \{x : \varphi(x)\}$, então $x \in A \iff \varphi(x)$.

Em particular, temos $A \in A \iff \varphi(A)$.

Considere-se a fórmula $x \notin x$.

$A = \{x : x \notin x)\}$.

A equivalência anterior deve-se a $A \in A \iff A \notin A$.

Em palavras: *seja A o conjunto dos conjuntos que não se contém a si próprios. Então A contem a si próprio se, e só se, A não contém a si próprio.*

Com isto, aqui temos mais uma fórmula que não gera um conjunto. Na realidade, ela foi o primeiro exemplo de uma fórmula que não corresponde a um conjunto.

Esta contradição é conhecida como o *Paradoxo de Russell*, que a descobriu examinando um sistema proposto por Fregue, o qual se propunha demonstrar que toda a matemática se reduz à lógica. O paradoxo mostrou que o sistema de Fregue não cumpria o seu objectivo. O paradoxo deu lugar à uma intensa atividade e polêmica na colectividade matemática, na qual diversas respostas ou teorias foram propostas para resolver a contradição, e marcou um ponto importante na história da Matemática. O leitor interessado encontrará uma vasta literatura onde o tema é discutido. Para dar um exemplo, veja-se Fraenkel & Bar Hillel.

Versões populares do Paradoxo de Russell.

1. Uma primeira versão é a dos *índices dos índices*, da qual damos aqui uma versão modificada que se refere a livros em lugar de índices:

   Em uma biblioteca há livros de duas classes:

   - Classe A: os livros que se mencionam a si próprios.

- Classe B: os livros que não se mencionam a si próprios.

O bibliotecário ficou encarregado de confeccionar um livro com um registo de todos os livros da classe B e incluí-lo na biblioteca.

Terminado o livro, ao bibliotecário restava-lhe apenas decidir se este se mencionaria a si próprio ou não, confrontando-se com o seguinte dilema:

- Se o livro não mencionava a si próprio, então pertencia à classe B; portando devia registar este fato e mencionar a si próprio.
- Se o livro mencionava a si próprio, então aparecia no seu registro; portanto não pertencia à classe B.

Por outras palavras, o livro pertence à classe B se, e só se, não pertence à classe B.

2. O próprio Russell deu uma versão popularizada do seu paradoxo definindo um barbeiro como alguém que barbeia a todos aqueles que não barbeiam a si próprios e só a eles. Coloca-se a questão: *um barbeiro barbeia a si próprio ou não*? Aqui, a condição $x \notin x$ é substituída por *B não barbeia a B*.
3. Uma situação semelhante se manifesta no *paradoxo do mentiroso*: alguém diz: "*o que estou a dizer é falso*". Aqui, claramente, o que o mentiroso diz é falso se e só se o que ele diz é verdadeiro.

Uma conclusão que se obtém destes exemplos é que *nem todas as fórmulas* dão origem a um conjunto. Há fórmulas que devem ser evitadas. O Axioma Irrestrito de Compreensão, *cada propriedade φ determina um conjunto; viz., o conjunto* $\{x : \varphi(x)\}$ deve ser limitado à classe das fórmulas que determinam conjuntos. Este tema será abordado com mais detalhe no Capítulo 3.

Até aqui temos os resultados preliminares. O próximo capítulo tratará do Cálculo Proposicional.

CAPíTULO 2

Cálculo Proposicional

Neste capítulo é apresentado um tratamento formal da lógica das proposições ou sentenças: o que normalmente entendemos por afirmações ou declarações que dizem que algo é de certa maneira ou que tem certa propriedade. Num tratamento formal, em primeiro lugar, há que se descrever a linguagem do sistema lógico. Logo, há que se descrever como raciocinar dentro do sistema. Em nosso caso, a maneira de raciocinar será dada por regras de inferência. Estas prescrevem como, a partir de certas proposições, chamadas premissas, se deriva uma outra proposição, chamada conclusão. Para que se tenha um ponto de partida neste processo de derivação são adotadas certas proposições iniciais que chamamos axiomas.

Até aqui, o sistema se apresenta como uma estrutura puramente simbólica; um simples jogo de caracteres, semelhante a um jogo de xadrez descrito, por exemplo, em notação algébrica, mas sem peças e sem tabuleiro. Este é o aspecto sintáctico do sistema: um sistema de caracteres organizados, mas no momento desprovidos de significado. Ora, o objectivo de uma linguagem é falar acerca de algo. Para tornar isto possível é preciso atribuir significado às expressões. Quando se chega a este ponto as expressões dizem algo acerca de alguma realidade. Agora as peças estão sobre o tabuleiro. Este é o aspecto semântico da linguagem. O que foi dito até aqui não se limita ao campo da lógica das proposições: descreve, em geral, os aspectos essenciais de qualquer sistema formal.

Quando uma linguagem é submetida a estudo ou desenvolvimento, é referida como linguagem objecto. A linguagem utilizada para tal efeito é chamada metalinguagem. Temos assim dois níveis de linguagem, e é importante distinguir entre ambos e saber dentro de qual nível se está a pensar. Com referência aos aspectos sintáctico e semântico dos sistemas, estes e as suas expressões têm diversas propriedades. Em particular, estaremos interessados na demonstrabilidade e verdade de uma expressão. Uma expressão é demonstrável se é possível chegar a ela a partir dos axiomas por meio das regras de inferência. Esta é uma propriedade sintáctica. A segunda, a verdade, é uma propriedade que pertence ao terreno da semântica. Obviamente, elas são expressadas na metalinguagem.

O tema deste capítulo é o desenvolvimento detalhado dos conceitos vertidos acima. A primeira parte é dedicada a provar que uma condição suficiente para uma expressão ser verdadeira é ser demonstrável. Isto é, que toda expressão demonstrável é verdadeira. A segunda parte é dedicada à verificação que esta condição é também necessária. Informal, mas sugestivamente, podemos exprimir ambos resultados dizendo que tudo que é demonstrável é verdadeiro e que tudo o verdadeiro é demonstrável. O primeiro constitui o chamado teorema de correção; o segundo, o teorema de completude do Cálculo Proposicional. Deste modo, resulta que no domínio das proposições, verdade e demonstrabilidade são conceitos equivalentes.

Sintaxe

Esta parte trata do sistema lógico como um sistema formal de símbolos puros, formado por entidades concebidas *in se* e *per se*, totalmente desprovidas de significado.

A Linguagem de $\mathfrak{P}$. Os símbolos que compõe a linguagem de $\mathfrak{P}$ são

(i) Variáveis proposicionais: $p, q, r, s, p_1, p_2, ...$
(ii) Conectivos: $\neg$ e $\vee$.
(iii) Parênteses: (e).

Notação 1. $Var(\mathfrak{P}) = \{p,\ q,\ r,\ s,\ t,\ p_1,\ q_1,\ \dots\}$

A seguir definimos recursivamente, sobre os naturais, as expressões gramaticalmente corretas da linguagem de $\mathfrak{P}$. Estas expressões são chamadas de *fórmulas proposicionais* ou, neste capítulo, simplesmente de *fórmulas*.

Definição 27 (Fórmulas de $\mathfrak{P}$).

1. $F_0 = Var(\mathfrak{P})$.
2. $F_{n+1} = F_n \cup \{\neg A : A \in F_n\} \cup \{(A \vee B) : A, B \in F_n\}$
3. $Flas(\mathfrak{P}) = \bigcup_{k\in\omega} F_k$.

Notação 2. *Utilizaremos a, b, c, $a_1, a_2, \dots$ como variáveis sintáticas de variáveis proposicionais, isto é, variáveis cujo domínio é $Var(\mathfrak{P})$. E utilizaremos A, B, C, $A_1, A_2, \dots$ como variáveis sintáticas para nos referirmos às fórmulas, isto é, variáveis cujo domínio é $Flas(\mathfrak{P})$.*

Segundo a definição, se A e B são fórmulas, então $(A \vee B)$ é uma fórmula. Com frequência omitiremos os parênteses em $(A \vee B)$ e escrevemos simplesmente $A \vee B$ quando não houver risco de ambiguidade. Como é habitual, as variáveis estão destinadas a representar, ou ser substituídas por, indivíduos do universo no

qual o sistema vai ser interpretado. As variáveis são as fórmulas mais simples da linguagem.

A Lógica de $\mathfrak{P}$. Os *axiomas* são todas as fórmulas da forma $\neg A \vee A$.

NOTAÇÃO 3. $Ax(\mathfrak{P}) = \{\neg A \vee A : A \in Flas(\mathfrak{P})\}$.

As *regras de inferência (primitivas)* são

$$\frac{A}{B \vee A}\ \text{Expansão} \qquad \frac{A \vee A}{A}\ \text{Contração} \qquad \frac{A \vee (B \vee C)}{(A \vee B) \vee C}\ \text{Associativa} \qquad \frac{A \vee B \quad \neg A \vee C}{B \vee C}\ \text{Corte}$$

DEFINIÇÃO 28 (Teoremas de $\mathfrak{P}$).

1. $T_0 = Ax(\mathfrak{P})$.
2. $T_{n+1} = T_n \cup \{B \vee A : A \in T_n\} \cup \{A : A \vee A \in T_n\} \cup \{(A \vee B) \vee C : A \vee (B \vee C) \in T_n\} \cup \{B \vee C : A \vee B \in T_n \text{ e } \neg A \vee C \in T_n\}$.
3. $Teor(\mathfrak{P}) = \bigcup_{k \in \omega} T_k$.

NOTAÇÃO 4. *$\vdash A$ denota que $A \in Teor(\mathfrak{P})$. Em palavras, $\vdash A$ denota que A é um teorema de $\mathfrak{P}$.*

Devido ao fato que este conceito, assim como outros, não são exclusivos de $\mathfrak{P}$ mas de qualquer sistema lógico, por vezes é útil ou necessário mencionar o sistema do qual se está a tratar, especialmente se este não resulta claro no contexto.

No caso de $\mathfrak{P}$, a notação acima torna-se mais explícita como segue:

$$\mathfrak{P} \vdash A : \ A \in Teor(\mathfrak{P}).$$

Neste ponto cabe observar que, enquanto "$\neg p \vee p$" é um teorema de $\mathfrak{P}$, "$\vdash \ \neg \ p \vee \ p$" não o é. De fato, "$\vdash \neg p \vee p$" nem sequer é uma fórmula de $\mathfrak{P}$, mas é uma afirmação *acerca* de "$\neg p \vee p''$ e de $\mathfrak{P}$, que diz que em $\mathfrak{P}$ a fórmula $\neg p \vee p$ é demonstrável.

Expressões que afirmam que algo acontece em $\mathfrak{P}$ são, a rigor, chamadas *metaexpressões*. Se estas *metaexpressões* afirmam algo verdadeiro então, a rigor, são chamadas *metateoremas*. Porém, normalmente é fácil pelo contexto nos apercebermos se uma expressão pertence à linguagem objeto ou à metalinguagem e, em tais casos, não é necessário explicitar a distinção anterior.

Contudo, deve-se ter sempre presente a distinção entre os diferentes níveis de linguagem.

Com frequência serão utilizadas, na metalinguagem, a negação, a conjunção e as quantificações existencial e universal da linguagem conversacional.

É conveniente introduzir as seguintes abreviaturas para a metalinguagem, o que proporcionará uma escrita mais compacta: (as duas últimas não são novas).

$$\begin{aligned} \text{não} &: \widehat{\neg} \\ \text{e} &: \& \\ \text{Existe} &: \widehat{\exists} \\ \text{Para todo} &: \widehat{\forall} \\ \text{Implica} &: \Longrightarrow \\ \text{Equivale} &: \Longleftrightarrow \end{aligned}$$

DEFINIÇÃO 29 (Demonstração, ou prova, em $\mathfrak{P}$). *Seja $A_1, \ldots, A_n$ uma sequência de fórmulas de $\mathfrak{P}$. A sequência $A_1, \ldots, A_n$ é uma* demonstração*, ou* prova*, (em $\mathfrak{P}$), sse para cada $i \in \{1, \ldots, n\}$:*

(i) $A_i \in Ax(\mathfrak{P})$ *ou*

(ii) A_i *é inferido de uma ou mais fórmulas anteriores da sequência por meio de uma das regras de inferência.*

Diz-se de uma demonstração que esta é uma demonstração da sua última fórmula.

É fácil ver que qualquer segmento inicial de uma demonstração é, também, uma demonstração. Mais ainda, não é difícil demonstrar por indução, da maneira esquematizada na sequência, que os teoremas são precisamente as fórmulas que têm uma demonstração.

TEOREMA 54. $\vdash A \Longleftrightarrow$ *Existe uma prova de A.*

Prova. Para ($\Longrightarrow$) vê-se que todo axioma tem uma prova. Supondo que toda fórmula em T_k tem uma prova, é fácil estender esta prova para uma prova de fórmulas de T_{k+1}.

Para ($\Longleftarrow$), observa-se que toda prova de comprimento 1 é a prova de um axioma. Supondo que o último elemento de uma prova de comprimento n é um elemento de T, é fácil ver que o último elemento de uma prova de comprimento $n+1$ é também um elemento de T. □

Semântica

Esta parte atribui significado aos símbolos do sistema formal. Os objetos do universo no qual o sistema $\mathfrak{P}$ será interpretado é constituído por proposições. Estas proposições são consideradas como entidades atômicas, não suscetíveis de serem separadas das suas partes constituintes, por exemplo sujeito e predicado.

Desta maneira, o que se pode distinguir entre duas sentenças é que uma seja verdadeira e a outra falsa. Se ambas são verdadeiras, ou ambas falsas, são consideradas equivalentes e indistinguíveis no sistema. Estas considerações levam, de maneira natural, a conceber o universo de interpretação de $\mathfrak{P}$ como consistindo de dois objetos, V e F, *verdade* e *falsidade*. Estes são chamados *valores de verdade*, comodamente representados pelos números 1 e 0, respectivamente. Assim, nosso universo é, simplesmente, $\{0, 1\}$.

Começamos por atribuir valores de verdade às variáveis proposicionais:

Definição 30 (Valoração). *Uma* valoração (das variáveis de $\mathfrak{P}$) *é uma função* $f : Var(\mathfrak{P}) \longrightarrow \{0, 1\}$.

Assim, uma valoração atribui a cada variável um valor de verdade.

Uma vez dada uma interpretação das variáveis proposicionais (isto é, uma valoração), desejamos estender esta interpretação a todas as fórmulas. Isto conduz a considerações sobre duas novas operações em $\{0, 1\}$ para estender a interpretação a fórmulas mais complexas, nomeadamente a fórmulas da forma $\neg A$ e $A \vee B$.

Definição 31. *As valorações* $* : \{0, 1\} \longrightarrow \{0, 1\}$ *e* $\triangledown : \{0, 1\} \times \{0, 1\} \longrightarrow \{0, 1\}$ *são definidas pelas seguintes tabelas:*

	$*$
0	1
1	0

$\triangledown$	0	1
0	0	1
1	1	1

Uma valoração induz, de maneira natural, uma função que atribui valores a todas as fórmulas de $\mathfrak{P}$, o que pode ser descrito da seguinte maneira:

Definição 32 (Valor de uma fórmula para uma valoração dada). *Sejam* f *uma valoração e* A *uma fórmula. O* valor de A por f *é a função*

$$\overline{f} : Flas(\mathfrak{P}) \longrightarrow \{0, 1\}$$

definida como segue.

1. $\overline{f}(A) = f(A)$, *para* $A \in Var(\mathfrak{P})$.
2. $\overline{f}(\neg A) = \overline{f}(A)^*$
3. $\overline{f}(A \vee B) = \overline{f}(A) \triangledown \overline{f}(B)$.

Quando não houver lugar para ambiguidade, não é preciso fazer a distinção notacional entre estas duas noções e podemos escrever simplesmente f em lugar de $\overline{f}$.

É útil representar os valores de uma fórmula por meio de *tabelas de verdade*, do modo a seguir (os valores de $p \vee q$ e de $\neg p$ aparecem embaixo do símbolo do conectivo):

$\neg$	p
0	1
1	0

p	$\vee$	q
1	1	1
1	1	0
0	1	1
0	0	0

p	$\vee$	$\neg q$
1	1	0 1
1	1	1 0
0	0	0 1
0	1	1 0

Para três variáveis: $p \vee (q \vee r)$

p	$\vee$	$q \vee r$
1	1	1 1 1
1	1	1 1 0
1	1	0 1 1
1	1	0 0 0
0	1	1 1 1
0	1	1 1 0
0	1	0 1 1
0	0	0 0 0

DEFINIÇÃO 33 (Tautologia, contingência, contradição). *Seja A uma fórmula de $\mathfrak{P}$.*

1. *A é uma* tautologia *sse $\overline{f}(A) = 1$ para toda valoração f.*
2. *A é uma* contradição *sse $\overline{f}(A) = 0$ para toda valoração f.*
3. *A é uma* contingência *sse existem valorações f e g tais que $\overline{f}(A) = 0$ e $\overline{g}(A) = 1$.*

NOTAÇÃO 5. *$Taut(A)$ denota que A é tautologia.*

O teorema a seguir estabelece que toda fórmula demonstrável é verdadeira. Mais adiante, ver-se-á que os conceitos de tautologia e teorema são, de fato, equivalentes.

TEOREMA 55 (Da validade, ou Teorema A). $\vdash A \Longrightarrow Taut(A)$.

Prova. Por indução sobre teoremas. Se $A \in T_0$, então $A = \neg B \vee B$ para certo B e, para toda valoração f, tem-se

$$\begin{aligned} \overline{f}(A) &= \overline{f}(\neg B \vee B) \\ &= \overline{f}(\neg B) \nabla \overline{f}(B) \\ &= \overline{f}(B)^* \nabla \overline{f}(B) \\ &= 1. \end{aligned}$$

Suponha que o teorema A é verdadeiro para todo $C \in T_k$ e seja $A \in T_{k+1}$. Se $A \in T_k$, então não há nada para demonstrar. Suponha que $A \notin T_k$, isto é, $A \in T_{k+1} \backslash T_k$. Então temos quatro casos:

a) $A \in \{B \vee C : C \in T_k\}$ ou
b) $A \in \{B : B \vee B \in T_k\}$ ou
c) $A \in \{(B \vee C) \vee D : B \vee (C \vee D) \in T_k\}$ ou
d) $A \in \{C \vee D : B \vee C \in T_k \& \neg B \vee D \in T_k\}$.

Seja f uma valoração qualquer.

No caso a), $A = B \vee C$ para certos B e C com $C \in T_k$ e tem-se:

$$\begin{array}{rcll} \overline{f}(A) & = & \overline{f}(B \vee C) & \\ & = & \overline{f}(B) \nabla \overline{f}(C) & \text{(Def. de } \overline{f}\text{).} \\ & = & \overline{f}(B) \nabla 1 & \text{(H.I.).} \\ & = & 1. & \text{(Def. de } \bigtriangledown\text{).} \end{array}$$

No caso b), $A = B$ para certo B tal que $B \vee B \in T_k$ e tem-se:

$$\begin{array}{rcll} \overline{f}(A) & = & \overline{f}(B) & \\ & = & \overline{f}(B) \nabla \overline{f}(B) & \text{(Def. de} \bigtriangledown\text{).} \\ & = & \overline{f}(B \vee B) & \text{(Def. de } \overline{f}\text{).} \\ & = & 1 & \text{(H.I.).} \end{array}$$

No caso c), $A = (B \vee C) \vee D$ para certos B, C e D tais que $B \vee (C \vee D) \in T_k$ e tem-se:

$$\begin{array}{rcl} \overline{f}(A) & = & \overline{f}\left[(B \vee C) \vee D\right] \\ & = & \left[\overline{f}(B \vee (C)\right] \nabla \overline{f}(D) \\ & = & \left[\overline{f}(B) \nabla \overline{f}(C)\right] \nabla \overline{f}(D) \\ & = & \overline{f}(B) \nabla \left[\overline{f}(C) \nabla \overline{f}(D)\right] \\ & = & \overline{f}(B) \nabla \overline{f}(C \vee D) \\ & = & \overline{f}\left[B \vee (C \vee D)\right] \\ & = & 1. \end{array}$$

No caso d) queremos demonstrar que, se $B \vee C \in T_k$ e $\neg B \vee D \in T_k$, então $Taut(B \vee C) \& Taut(\neg B \vee D) \Longrightarrow Taut(C \vee D)$. Demonstraremos, equivalentemente, que

$$\hat{\neg} Taut(C \vee D) \Longrightarrow \left[\hat{\neg} Taut(B \vee C) \text{ ou } \hat{\neg} Taut(\neg B \vee D)\right].$$

Suponha-se que $\hat{\neg} Taut(C \vee D)$, isto é, existe valoração f tal que $f(C \vee D) = 0$. Mas $f(C \vee D) = f(C) \nabla f(D)$. Assim, $f(C) = f(D) = 0$.

Ora, $f(B) = 0$, ou $f(B) = 1$,

- Se $f(B) = 0$, então $f(B \vee C) = f(B) \nabla f(C) = 0 \nabla 0 = 0$ e, portanto, $\hat{\neg} Taut(B \vee C)$.
- Se $f(B) = 1$, então $f(\neg B) = 0$ e $f(\neg B \vee D) = f(\neg B) \nabla f(D) = f(B)^* \nabla f(D) = 1^* \nabla 0 = 0 \nabla 0 = 0$.

Portanto, $\widehat{\neg} Taut(\neg B \vee D)$, isto é, $\widehat{\neg} Taut(B \vee C)$ ou $\widehat{\neg} Taut(\neg B \vee D)$, o que completa a demonstração do Teorema.

□

O teorema recíproco do teorema da validade é o teorema principal do presente tratamento do cálculo proposicional; na sua prova utilizaremos dez teoremas que estão a seguir.

O Teorema de Completude do Cálculo Proposicional

Devido ao fato que expressões da forma $A_1 \vee (A_2 \vee (\cdots \vee A_n))$ aparecerão repetidamente, é útil estabelecer a seguinte convenção sobre parênteses:

$$A_1 \vee A_2 \vee \cdots \vee A_n = A_1 \vee (A_2 \vee (\cdots \vee A_n)).$$

Se Ψ é uma propriedade satisfeita por um número finito de naturais, denotaremos por $\bigvee_{\Psi(i)} A_i$ a disjunção dos A_i's, tais que $\Psi(i)$, na ordem *crescente* dos subíndices, com a convenção sobre parênteses adotada acima (cf. Teorema 63).

Será inevitável fazer alusão à sequências finitas de fórmulas, pelo que será útil estabelecer algumas convenções em relação a elas. Em geral, uma sequência finita σ de elementos de um conjunto X é uma função de um número natural n em X.

$$\sigma : n \to X, \quad n \text{ é o } \textit{comprimento} \text{ de } \sigma.$$

Lembramos que

$$\begin{aligned} 0 &= \phi, \\ 1 &= \{0\}, \\ n+1 &= n \cup \{n\}. \end{aligned}$$

Assim, por exemplo, $4 = \{0,\ 1,\ 2,\ 3\}$

e, em geral: $n = \{0, \ldots, n-1\}$.

Utilizaremos i, j, k, m e n, como variáveis com domínio nos números naturais.

No contexto das sequências, é habitual fazer referência à imagem por σ de $i \in n$ por σ_i em lugar de $\sigma(i)$ e referir-se à σ pela sua imagem em X:

$$\sigma = \langle \sigma_0, \ldots,\ \sigma_{n-1} \rangle .$$

Quando facilitar a leitura, faremos a contagem dos σ_i's a partir de 1 em lugar de 0. Assim, escrevemos:

$$\sigma = \langle \sigma_1, \ldots, \sigma_n \rangle \text{ em lugar de } \sigma = \langle \sigma_0, \ldots, \sigma_{n-1} \rangle .$$

Escreveremos $B\ \varepsilon\ \langle A_1, \ldots, A_n \rangle$ como abreviatura de $B \in Ran(\langle A_1, \ldots, A_n \rangle)$.

Note-se a diferença entre ε e $\in$. A necessidade de considerar sequências de fórmulas surge porque em expressões da forma $A_1 \vee \cdots \vee A_n$ devemos permitir que haja fórmulas repetidas.

Se $A = \langle A_1, \ldots, A_n \rangle$, então definimos

$$\bigvee A = \begin{cases} A_1 & \text{quando } n = 1 \\ A_1 \vee \bigvee \langle A_2, \ldots, A_n \rangle & \text{quando } n \neq 1 \end{cases}$$

O que se segue são afirmações acerca de fórmulas $A, B, C, \ldots$ que devem ser entendidas como afirmações para quaisquer fórmulas $A, B, C, \ldots$, isto é, são afirmações universalmente quantificadas em todas as suas variáveis. Os Teoremas a seguir são regras que permitem derivar de certa(s) fórmula(s) outra fórmula, pelo que têm a forma de regras de inferência; o que as diferencia das regras de inferência primitivas é que estas são *regras de inferência derivadas*.

Teorema 56 (Regra Comutativa).

$$\vdash A \vee B \Longrightarrow \vdash B \vee A.$$

Prova.

(1)	$\vdash$	$A \vee B$	(Hipótese).
(2)	$\vdash$	$\neg A \vee A$	(Axioma).
(3)	$\vdash$	$B \vee A$	(Corte 1, 2).

□

Teorema 57 (Dupla negação).

$$\vdash A \vee B \Longrightarrow \vdash \neg\neg A \vee B.$$

Prova.

(1)	$\vdash$	$A \vee B$	(Hipótese).
(2)	$\vdash$	$\neg\neg A \vee \neg A$	(Axioma).
(3)	$\vdash$	$\neg A \vee \neg\neg A$	(Comutativa 2).
(4)	$\vdash$	$B \vee \neg\neg A$	(Corte 1, 3).
(5)	$\vdash$	$\neg\neg A \vee B$	(Comutativa 4).

□

Os teoremas 58, 60 e 69 proporcionam liberdade de associação e reordenação das fórmulas numa expressão.

Teorema 58 (Associatividade Esquerda-Direita).

$$\vdash (A \vee B) \vee C \Longrightarrow \vdash A \vee (B \vee C).$$

Prova.

(1) $\vdash (A \vee B) \vee C$ (Hipótese).
(2) $\vdash C \vee (A \vee B)$ (Comutativa).
(3) $\vdash (C \vee A) \vee B$ (Associativa).
(4) $\vdash B \vee (C \vee A)$ (Comutativa).
(5) $\vdash (B \vee C) \vee A$ (Associativa).
(6) $\vdash A \vee (B \vee C)$ (Comutativa).

□

Teorema 59.

$$\vdash \neg A \vee C \& \vdash \neg B \vee C \Longrightarrow \vdash \neg(A \vee B) \vee C.$$

Prova.

(1) $\vdash \neg A \vee C$ (Hipótese).
(2) $\vdash \neg B \vee C$ (Hipótese).
(3) $\vdash \neg(A \vee B) \vee (A \vee B)$ (Axioma).
(4) $\vdash (A \vee B) \vee \neg(A \vee B)$ (Comutativa 3).
(5) $\vdash A \vee (B \vee \neg(A \vee B))$ (Associativa E-D, 4).
(6) $\vdash (B \vee \neg(A \vee B)) \vee C$ (Corte 5,1).
(7) $\vdash B \vee (\neg(A \vee B) \vee C)$ (Associativa E-D, 6).
(8) $\vdash \neg(A \vee B) \vee (B \vee (\neg(A \vee B) \vee C))$ (Expansão 7).
(9) $\vdash (B \vee (\neg(A \vee B) \vee C)) \vee \neg(A \vee B)$ (Comutativa 8).
(10) $\vdash B \vee ((\neg(A \vee B) \vee C) \vee \neg(A \vee B))$ (Associativa E-D, 10).
(11) $\vdash ((\neg(A \vee B) \vee C) \vee \neg(A \vee B)) \vee C$ (Corte 10, 2).
(12) $\vdash (\neg(A \vee B) \vee C) \vee (\neg(A \vee B)) \vee C)$ (Associativa E-D 11).
(13) $\vdash \neg(A \vee B) \vee C$ (Contração 12).

□

Teorema 60.

$$\vdash (B \vee C) \vee A \Longrightarrow \vdash (C \vee B) \vee A.$$

Prova.

(1)	$\vdash$	$(B \vee C) \vee A$	(Hipótese).
(2)	$\vdash$	$C \vee ((B \vee C) \vee A)$	(Expansão).
(3)	$\vdash$	$(C \vee (B \vee C)) \vee A$	(Associativa).
(4)	$\vdash$	$A \vee (C \vee (B \vee C))$	(Comutativa).
(5)	$\vdash$	$(A \vee C) \vee (B \vee C)$	(Associativa).
(6)	$\vdash$	$((A \vee C) \vee B) \vee C$	(Associativa).
(7)	$\vdash$	$C \vee ((A \vee C) \vee B)$	(Comutativa).
(8)	$\vdash$	$A \vee (C \vee ((A \vee C) \vee B))$	(Expansão).
(9)	$\vdash$	$(A \vee C) \vee ((A \vee C) \vee B))$	(Associativa).
(10)	$\vdash$	$((A \vee C) \vee B) \vee (A \vee C)$	(Comutativa). (Expansão).
(11)	$\vdash$	$B \vee (((A \vee C) \vee B) \vee (A \vee C))$	(Comutativa).
(12)	$\vdash$	$(((A \vee C) \vee B) \vee (A \vee C)) \vee B$	(Associativa E-D).
(13)	$\vdash$	$((A \vee C) \vee B) \vee ((A \vee C) \vee B)$	(Contração).
(14)	$\vdash$	$(A \vee C) \vee B$	(Associativa E-D).
(15)	$\vdash$	$A \vee (C \vee B)$	(Comutativa).
(16)	$\vdash$	$(C \vee B) \vee A$	

□

Teorema 61.

$$\vdash A \vee (B \vee (C \vee D)) \Longrightarrow \vdash C \vee (A \vee (B \vee D)).$$

Prova.

(1)	$\vdash$	$A \vee (B \vee (C \vee D))$	(Hipótese).
(2)	$\vdash$	$C \vee (A \vee (B \vee (C \vee D)))$	(Expansão).
(3)	$\vdash$	$(C \vee A) \vee (B \vee (C \vee D))$	(Associativa).
(4)	$\vdash$	$((C \vee A) \vee B) \vee (C \vee D)$	(Associativa).
(5)	$\vdash$	$(C \vee D) \vee ((C \vee A) \vee B)$	(Comutativa).
(6)	$\vdash$	$(D \vee C) \vee ((C \vee A) \vee B)$	(Teorema 60).
(7)	$\vdash$	$((C \vee A) \vee B) \vee (D \vee C)$	(Comutativa).
(8)	$\vdash$	$(((C \vee A) \vee B) \vee D) \vee C$	(Associativa).
(9)	$\vdash$	$((((C \vee A) \vee B) \vee D) \vee C) \vee A$	(Exp. + Comut).
(10)	$\vdash$	$(((C \vee A) \vee B) \vee D) \vee (C \vee A)$	(Associativa E-D).
(11)	$\vdash$	$((((C \vee A) \vee B) \vee D) \vee (C \vee A)) \vee B$	(Exp. + Comut).
(12)	$\vdash$	$(((C \vee A) \vee B) \vee D) \vee ((C \vee A) \vee B)$	(Associativa E-D).
(13)	$\vdash$	$((((C \vee A) \vee B) \vee D) \vee ((C \vee A) \vee B)) \vee D$	(Exp. + Comut).
(14)	$\vdash$	$(((C \vee A) \vee B) \vee D) \vee (((C \vee A) \vee B) \vee D)$	(Associativa E-D).
(15)	$\vdash$	$((C \vee A) \vee B) \vee D)$	(Contracção).
(16)	$\vdash$	$(C \vee A) \vee (B \vee D)$	(Associativa E-D).
(17)	$\vdash$	$C \vee (A \vee (B \vee D))$	(Associativa E-D).

□

Teorema 62.

$$\vdash A \vee ((B \vee C) \vee D) \Longleftrightarrow \vdash A \vee (B \vee (C \vee D)).$$

Prova.

$\boxed{\Longrightarrow}$

(1)	$\vdash$	$A \vee ((B \vee C) \vee D)$	(Hipótese).
(2)	$\vdash$	$((B \vee C) \vee D) \vee A$	(Comutativa).
(3)	$\vdash$	$(D \vee (B \vee C)) \vee A$	(Teorema 60).
(4)	$\vdash$	$A \vee (D \vee (B \vee C))$	(Comutativa).
(5)	$\vdash$	$B \vee (A \vee (D \vee C))$	(Teorema 69).
(6)	$\vdash$	$(A \vee (D \vee C)) \vee B$	(Comutativa).
(7)	$\vdash$	$((D \vee C) \vee A) \vee B$	(Teorema 60).
(8)	$\vdash$	$(D \vee C) \vee (A \vee B)$	(Associatividade E-D).
(9)	$\vdash$	$(C \vee D) \vee (A \vee B)$	(Teorema 60).
(10)	$\vdash$	$(A \vee B) \vee (C \vee D)$	(Comutativa).
(11)	$\vdash$	$A \vee (B \vee (C \vee D))$	(Associativa).

$\boxed{\Longleftarrow}$

(1)	$\vdash$	$A \vee (B \vee (C \vee D))$	(Hipótese).
(2)	$\vdash$	$(B \vee (C \vee D)) \vee A$	(Comutativa).
(3)	$\vdash$	$B \vee ((C \vee D) \vee A)$	(Associativa).
(4)	$\vdash$	$B \vee (C \vee (D \vee A))$	(Parte $\Longrightarrow$).
(5)	$\vdash$	$(B \vee C) \vee (D \vee A)$	(Associativa).
(6)	$\vdash$	$((B \vee C) \vee D) \vee A$	(Associativa).
(7)	$\vdash$	$A \vee ((B \vee C) \vee D)$	(Comutativa).

□

O teorema a seguir afirma que, se uma cadeia de disjunções é demonstrável, então também o é a cadeia que resulta de deslocar qualquer das fórmulas envolvidas para o início.

Teorema 63.

$$(\widehat{\forall} n \geq 2)(\widehat{\forall} i \in \{1, ..., n\})\Big(\vdash A_1 \vee A_2 \vee ... \vee A_n \Longleftrightarrow \ \vdash A_i \vee \bigvee_{k \neq i} A_k\Big).$$

Prova.

$\boxed{\Longrightarrow}$ A prova é por indução sobre n:

Para $n = 2$, o resultado é trivial.

Para $n > 2$, separamos a situação em três casos.

Caso 1. $i = 1$. Nada por demonstrar.

Caso 2. $i = 2$.

$\vdash A_1 \vee A_2 \vee A_3 \vee \ldots \vee A_n$ (Hipótese).
$\vdash (A_1 \vee A_2) \vee (A_3 \vee \ldots \vee A_n)$ (Associativa).
$\vdash (A_2 \vee A_1) \vee (A_3 \vee \ldots \vee A_n)$ (Teorema 60).
$\vdash A_2 \vee (A_1 \vee A_3 \vee \ldots \vee A_n)$ (Associativa E-D).

Caso 3. $i > 2$.

$\vdash A_1 \vee A_2 \vee A_3 \vee \ldots \vee A_n$ (Hipótese).
$\vdash (A_1 \vee A_2) \vee (A_3 \vee \ldots \vee A_n)$ (Associativa).
$\vdash A_i \vee \left[(A_1 \vee A_2) \vee \bigvee_{k \neq 1,2,i} A_k)\right]$ (H.I).
$\vdash A_i \vee \bigvee_{k \neq i} A_k$ (Teorema 62).

$\boxed{\Longleftarrow}$ A demonstração é similar e é deixada como exercício. □

TEOREMA 64. *Para todo $n \geq 1$ e para toda valoração f, tem-se:*

$$\overline{f}(A_1 \vee A_2 \vee \cdots \vee A_n) = 1 \iff \overline{f}(A_i) = 1 \text{ para algum } i.$$

Prova.
Indução sobre n.
(i) Para $n = 1$ a afirmação é trivial.
(ii) Para $n > 1$, suponha-se que a afirmação é verdadeira para $n = k$.
Queremos demonstrar para $n = k + 1$. Para isso, temos:

$\overline{f}(A_1 \vee A_2 \vee ... \vee A_k \vee A_{k+1}) = 1 \iff$ (Def.de $\overline{f}$)
$\overline{f}(A_1) \bigtriangledown \overline{f}(A_2 \vee ... \vee A_k \vee A_{k+1}) = 1 \iff$ (Def. de $\bigtriangledown$).
$\overline{f}(A_1) = 1$ ou $\overline{f}(A_2 \vee ... \vee A_k \vee A_{k+1}) = 1 \iff$ (H.I.).
$\overline{f}(A_1) = 1$ *ou* $\overline{f}(A_i) = 1$,
para algum $i \in \{2, ..., k+1\} \iff$
$\overline{f}(A_i) = 1$ para algum $i \in \{1, 2, ..., k+1\}$

□

TEOREMA 65. *Para todo $n \geq 2$, se para cada $i \in \{1, \ldots, n\}$, ou A_i é uma variável ou A_i é a negação de uma variável, então*

$$Taut(A_1 \vee A_2 \vee \cdots \vee A_n) \iff A_i = \neg A_j \text{ para certos } i, j \in \{1, 2, ..., n\}.$$

(Isto é, uma disjunção de variáveis e negações de variáveis é tautologia se, e somente se, uma dessas variáveis ocorre simultaneamente com a sua negação).

Prova.
$\boxed{\Longleftarrow}$ Seja $f \in \{0,1\}^{Var(\mathfrak{P})}$ uma valoração qualquer.

Se o lado direito se verifica, então existem $i, j \in \{1, \ldots, n\}$ tais que $f(A_i) = 1$ ou $f(A_j) = 1$. Pelo teorema anterior (9), $Taut(A_1 \vee A_2 \vee \cdots \vee A_n)$.

$\boxed{\Longrightarrow}$ Suponha-se que o lado direito é falso e defina-se $f \in \{0,\ 1\}^{Var(\mathfrak{P})}$ de modo que $f(a) = 1$ see $\neg a \varepsilon \langle A_1, A_2, \ldots, A_n \rangle$, isto é, $\neg a$ é um dos $A_i's$.

Com isto, resulta que $f(A_i) = 0$ para todo $i \in \{1, \ldots, n\}$. Portanto, pelo Teorema 64, $f(A_1 \vee A_2 \vee \cdots \vee A_n) = 0$. Assim, é falso que $Taut(A_1 \vee A_2 \vee \cdots \vee A_n)$. □

Definição 34 (Número de ocorrências de conectivos em fórmulas e em sequências de fórmulas). *Seja* $A \in Flas(\mathfrak{P})$. *Definimos o* número de ocorrências *de conectivos em* A, $noc(A)$, *como segue:*

1. *Se* $A \in Var(\mathfrak{P})$, *então* $noc(A) = 0$.
2. *Se* $A = \neg B$, *então* $noc(A) = 1 + noc(B)$.
3. *Se* $A = B \vee C$, *então* $noc(A) = noc(B) + 1 + noc(C)$.

Consideremos agora uma sequência finita de fórmulas $\langle A_1, \ldots, A_n \rangle$. Definimos o *número de ocorrências de conectivos em* $\langle A_1, \ldots, A_n \rangle$ como a soma dos números de ocorrências de conectivos em elementos de $\langle A_1, \ldots, A_n \rangle$:

$$NOC(\langle A_1, \ldots,\ A_n \rangle) = \sum_{i=1}^{n} noc(A_i).$$

Exemplo 1.

1. *Considere* $\varphi = p \vee \neg\neg q$, $\psi = \neg(r \vee \neg s) \vee t$ *e* $\theta = p \vee \neg\neg q$.

$$\begin{aligned} NOC(\langle \varphi, \psi, \theta \rangle) &= NOC(\langle p \vee \neg\neg q, \neg(r \vee \neg s) \vee t, p \vee \neg\neg q \rangle) \\ &= = noc(p \vee \neg\neg q) + noc(\neg(r \vee \neg s) \vee t) + noc(p \vee \neg\neg q) \\ &= 3 + 4 + 3 \\ &= 10. \end{aligned}$$

2. *Considere* $\varphi = p$, $\psi = \neg\neg q$, $\theta = \neg r$ *e* $\gamma = \neg(r \vee \neg s) \vee t$.

$$\begin{aligned} NOC(\varphi, \psi, \theta, \gamma) &= NOC(\langle p, \neg\neg q, \neg r, \neg(r \vee \neg s) \vee t \rangle) \\ &= noc(p) + noc(\neg\neg q) + noc(\neg r) + noc(\neg(r \vee \neg s) \vee t) \\ &= 0 + 2 + 1 + 4 \\ &= 7. \end{aligned}$$

Observe-se que a segunda sequência de fórmulas tem *mais* elementos do que a anterior, mas tem um *menor* número de ocorrências de conectivos.

Definição 35. *Denote-se por* $\mathcal{T}$ *o conjunto de sequências* $\langle S_1, S_2, \ldots, S_n \rangle$ *cuja disjunção é uma tautologia, isto é,*

$$\mathcal{T} = \{\langle S_1, S_2, \ldots, S_n \rangle : Taut(S_1 \vee S_2 \vee \cdots \vee S_n)\}.$$

LEMA 1. *Seja* $S = \langle S_1, \ldots, S_n\rangle$ *uma sequência de fórmulas. Então*

1. $Taut(\bigvee \langle \neg\neg B, S_2, \ldots, S_n\rangle) \Rightarrow Taut(\bigvee \langle B, S_2, \ldots, S_n\rangle)$.
2. $Taut(\bigvee \langle B \vee C, S_2, \ldots, S_n\rangle) \Rightarrow Taut(\bigvee \langle B, C, S_2, \ldots, S_n\rangle)$.
3. $Taut(\bigvee \langle \neg(B \vee C), S_2, \ldots, S_n\rangle) \Rightarrow Taut(\bigvee \langle \neg B, S_2, \ldots, S_n\rangle)$.
4. $Taut(\bigvee \langle \neg(B \vee C), S_2, \ldots, S_n\rangle) \Rightarrow Taut(\bigvee \langle \neg C, S_2, \ldots, S_n\rangle)$.
5. $Taut(\bigvee \langle S_1, \ldots, S_n\rangle) \Rightarrow Taut(\bigvee\langle S_j\rangle \circ \langle S_i : i \neq j, 1 \leq i \leq n\rangle),\ 1 \leq j \leq n$.

Prova. Exercício. □

Este lema sugere a definição da seguinte relação binária sobre $\mathcal{T}$.

DEFINIÇÃO 36. *Seja* $S = \langle S_1, \ldots, S_n\rangle$ *uma sequência de fórmulas. Definimos a relação binária* R *sobre* $\mathcal{T}$ *como segue:*

1. $\langle B, C, S_2, \ldots, S_n\rangle\, R\, \langle B \vee C, S_2, \ldots, S_n\rangle$.
2. $\langle B, S_2, \ldots, S_n\rangle\, R\, \langle \neg\neg B, S_2, \ldots, S_n\rangle$.
3. $\langle \neg B, S_2, \ldots, S_n\rangle\, R\, \langle \neg(B \vee C), S_2, \ldots, S_n\rangle$.
4. $\langle \neg C, S_2, \ldots, S_n\rangle\, R\, \langle \neg(B \vee C), S_2, \ldots, S_n\rangle$.
5. $\langle S_j\rangle \circ \langle S_i : i \neq j, 1 \leq i \leq n\rangle\, R\, \langle S_1, \ldots, S_n\rangle$, *quando* $n \geq 2, j \neq 1$ *e*

   $S_j \notin Var(\mathfrak{P}) \cup \widehat{\neg} Var(\mathfrak{P})$ *e* $S_k \in Var(\mathfrak{P}) \cup \widehat{\neg} Var(\mathfrak{P})$, *para* $k < j$.

Na última cláusula, a sequência da esquerda é obtida da sequência da direita por meio do deslocamento, para o início, da primeira fórmula que não é variável nem negação de variável.

O Lema 1 garante que para todo W, R e W', se $\bigvee W'$ pertence à disjunção $\mathcal{T}$, então a disjunção $\bigvee W$ também pertence à $\mathcal{T}$.

Para realizar indução sobre R a relação R tem que ser bem fundada.

PROPOSIÇÃO 1. *A relação* R *é bem fundada.*

Prova. (Esquema) A afirmação é consequência da boa fundação da relação $NOC(P) \leq NOC(S)$. Note-se que os átomos de R são as sequências $\langle S_1, \ldots, S_n\rangle$ tais que

$$Taut(\textstyle\bigvee_{i=1}^{n} S_i) \text{ e } S_i \in Var(\mathfrak{P}) \cup \widehat{\neg} Var(\mathfrak{P}),$$

isto é, as sequências finitas de variáveis e negações de variáveis cuja disjunção é uma tautologia. □

Será de utilidade formar a sequência de disjuntas que formam uma fórmula.

DEFINIÇÃO 37.

a) $seq(A) = \langle A\rangle$, *se* $A \in Var(\mathfrak{P})$.
b) $seq(\neg B) = \langle \neg B\rangle$.
c) $seq(B \vee C) = \langle B\rangle \circ seq(C)$.

TEOREMA 66. *Para toda a fórmula A de $\mathfrak{P}$, $Taut(A) \Longrightarrow \mathfrak{P} \vdash A$.*

Indução sobre R. Seja A uma tautologia e

$$S = \langle S_1, \ldots, S_n \rangle = seq(A).$$

Então $S \in \mathcal{T}$ e vamos considerar os casos em que S é, ou não, átomo.

(I) Se S é um átomo de R, isto é,

$$S_i \in \widehat{\neg} Var(\mathfrak{P}) \cup Var(\mathfrak{P}), 1 \leq i \leq n,$$

temos pelo Teorema 65 que $S_i = \neg S_j$, para $i, j \in \{1, 2, \ldots, \}$ e $i \neq j$. Desse modo,

$$S_i \vee S_j = \neg S_j \vee S_j,$$

isto é, $S_i \vee S_j$ é um axioma. Assim $\vdash S_i \vee S_j$ e, pelas regras de expansão e comutativa,

$$\vdash (S_i \vee S_j) \vee \bigvee_{k \neq i,j} S_k$$

Consequentemente,

$$\vdash S_{\ i} \vee (S_{\ j} \vee \bigvee_{k \neq i,j} S_k).$$

Duas aplicações do Teorema 63 fornecem o resultado esperado:

$$\vdash S_1 \vee \cdots \vee S_n.$$

(II) Se S não é um átomo, suponha-se que para qualquer sequência

$$\langle Q_1, \ldots, Q_m \rangle \in \mathcal{T}$$

tem-se a hipótese de indução

$$\langle Q_1, \ldots, Q_m \rangle R \langle S_1, \ldots, S_n \rangle \text{ implica } \vdash \bigvee Q.$$

Seja i o primeiro natural tal que A_i não é variável nem negação de variável. Depois do Teorema 63, sem perda de generalidade podemos supor que $i = 1$. Dividimos a situação em três casos.

1. S_1 é da forma $B \vee C$;
2. S_1 é da forma $\neg\neg B$;
3. S_1 é da forma $\neg(B \vee C)$.

Note-se que, se S_1 é uma negação, então não pode ser negação de uma variável. Portanto deve ser negação de uma negação ou negação de uma disjunção, o que explica os casos 2 e 3.

Caso 1. Se $S_1 = B \vee C$, da hipótese, temos que $Taut((B \vee C) \vee (S_2 \cdots \vee S_n))$. Disso, tem-se que $Taut(B \vee (C \vee (S_2 \cdots \vee S_n)))$. A Hipótese de Indução implica que $\vdash B \vee (C \vee (S_2 \cdots \vee S_n))$. Usando associatividade, obtém-se

$$\vdash (B \vee C) \vee (S_2 \cdots \vee S_n).$$

Caso 2. Se $S_1 = \neg\neg B$, pela hipótese, $Taut(\neg\neg B \vee (S_2 \cdots \vee S_n))$ e, portanto, $Taut(B \vee (S_2 \cdots \vee S_n))$. A Hipótese de Indução dá $\vdash B \vee (S_2 \cdots \vee S_n)$. Logo, pelo Teorema 57,

$$\vdash \neg\neg B \vee (S_2 \cdots \vee S_n).$$

Caso 3. Se $S_1 = \neg(B \vee C)$, então pela hipótese de indução conclui-se que $Taut(\neg(B \vee C) \vee (S_2 \cdots \vee S_n))$. Disso,

$$Taut(\neg B \vee (S_2 \cdots \vee S_n)) \text{ e} \qquad (\alpha)$$
$$Taut(\neg C \vee (S_2 \cdots \vee S_n)). \qquad (\beta)$$

A hipótese de indução aplicada a (α) e (β), respectivamente, dá

$$\vdash \neg B \vee (S_2 \cdots \vee S_n) \text{ e} \qquad (\gamma)$$
$$\vdash \neg C \vee (S_2 \cdots \vee S_n) \qquad (\delta)$$

Disso e do Teorema 59 obtém-se $\vdash \neg(B \vee C) \vee (S_2 \cdots \vee S_n)$, completando a prova do Teorema.

□

Observe-se que, se A é uma tautologia, então *existe uma prova* de A.

Um exame cuidadoso da demonstração de B revela que esta não é uma mera afirmação de existência, mas que de fato ela fornece um algoritmo para construir uma tal prova.

Com efeito, a demonstração de B não se limita às quatro linhas acima, mas consiste da sequência das demonstrações de *todos* os teoremas até chegar a B e elas prescrevem, passo a passo, como elaborar uma prova em $\mathfrak{P}$ de uma tautologia.

O diagrama de fluxo na página seguinte (Figura 1) descreve, *grosso-modo*, a maneira de se obter uma tal prova.

Para simplificar, não estão aqui explicitados todos os passos. Por exemplo, uma descrição detalhada do indicado na caixa que faz referência ao Teorema 63 daria lugar, por si só, a um diagrama de fluxo parcial. Situações semelhantes temos nas caixas referentes aos outros Teoremas.

Em particular, a instrução contida na caixa que faz referência ao Teorema 63 consiste em substituir $\vdash S_1 \vee S_2 \vee \cdots \vee S_n$ por $\vdash S_i \vee S_1 \vee S_2 \vee \cdots \vee S_{i-1} \vee S_{i+1} \vee \cdots \vee S_n$.

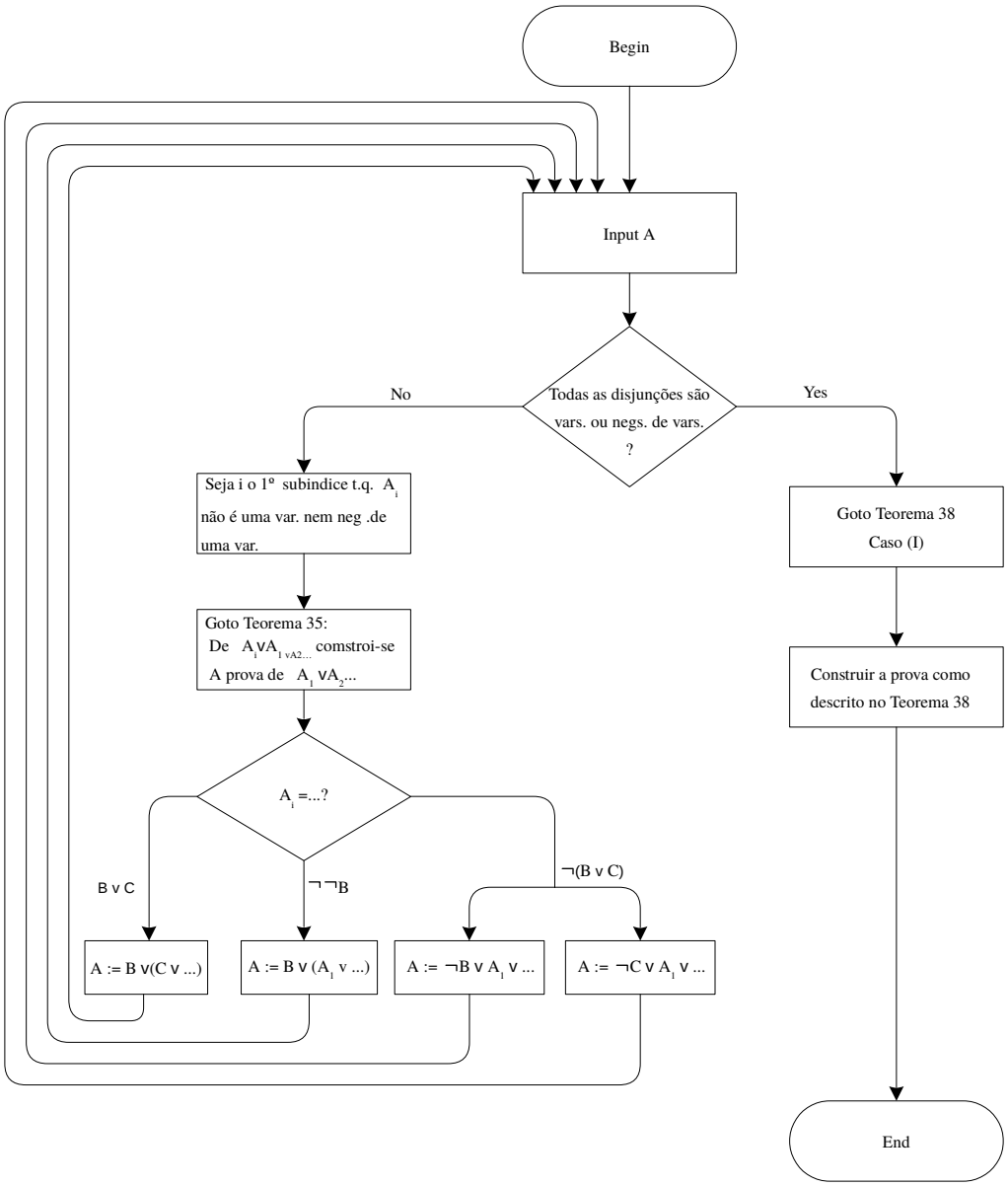


FIGURA 2.1. Flow-chart.

EXEMPLO 2. *Aplicamos o algoritmo à fórmula*

$$A = \neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q)).$$

Não é difícil verificar que A é uma tautologia e, pelo teorema da completude, um teorema de $\mathfrak{P}$. Assim, podemos construir uma prova para esta fórmula. Seguindo o Flow-chart procedemos da seguinte forma:

Input: $A = \neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q))$
No
i=1 (T63 – Do nothing!)

Usando o Teorema 59 e as provas de $F_1 = \neg\neg p \vee (\neg(r \vee p) \vee (r \vee q))$ e $F_2 = \neg q \vee (\neg(r \vee p) \vee (r \vee q))$ construímos a prova de A.
Nomeadamente, temos

$\vdash \neg\neg p \vee (\neg(r \vee p) \vee (r \vee q))$
$\vdash \neg q \vee (\neg(r \vee p) \vee (r \vee q))$
$\vdash \neg(\neg p \vee q) \vee (\neg p \vee q)$
$\vdash (\neg p \vee q) \vee \neg(\neg p \vee q)$
$\vdash \neg p \vee (q \vee \neg(\neg p \vee q))$
$\vdash (q \vee \neg(\neg p \vee q)) \vee (\neg(r \vee p) \vee (r \vee q))$
$\vdash q \vee (\neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q)))$
$\vdash \neg(\neg p \vee q) \vee (q \vee (\neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q))))$
$\vdash (q \vee (\neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q)))) \vee \neg(\neg p \vee q)$
$\vdash q \vee ((\neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q))) \vee \neg(\neg p \vee q))$
$\vdash ((\neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q))) \vee \neg(\neg p \vee q)) \vee (\neg(r \vee p) \vee (r \vee q))$
$\vdash (\neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q))) \vee (\neg(\neg p \vee q)) \vee (\neg(r \vee p) \vee (r \vee q)))$
$\vdash \neg(\neg p \vee q) \vee (\neg(r \vee p) \vee (r \vee q))$

Repetindo o procedimento temos as provas de F_1 e F_2.

$F_1 = \neg\neg p \vee (\neg(r \vee p) \vee (r \vee q))$

Goto (*)

No

i=1 (T63 – Do nothing!)

$\vdash p \vee (\neg(r \vee p) \vee (r \vee q))$
$\vdash \neg\neg p \vee \neg p$
$\vdash \neg p \vee \neg\neg p$
$\vdash (\neg(r \vee p) \vee (r \vee q)) \vee \neg\neg p$
$\vdash \neg\neg p \vee (\neg(r \vee p) \vee (r \vee q))$
$p \vee (\neg(r \vee p) \vee (r \vee q))$

Goto (*)

No

i=2

T63 $\vdash \vdots \vdash$

$\neg(r \vee p) \vee (p \vee (r \vee q))$

$\vdash \neg r \vee (p \vee (r \vee q))$
$\vdash \neg p \vee (p \vee (r \vee q))$
$\vdash \neg(r \vee p) \vee (r \vee p)$
$\vdash (r \vee p) \vee \neg(r \vee p)$
$\vdash r \vee (p \vee \neg(r \vee p))$
$\vdash (p \vee \neg(r \vee p)) \vee (p \vee (r \vee q))$
$\vdash p \vee (\neg(r \vee p) \vee (p \vee (r \vee q)))$
$\vdash \neg(r \vee p) \vee (p \vee (\neg(r \vee p) \vee (p \vee (r \vee q))))$
$\vdash (p \vee (\neg(r \vee p) \vee (p \vee (r \vee q)))) \vee \neg(r \vee p)$
$\vdash p \vee ((\neg(r \vee p) \vee (p \vee (r \vee q))) \vee \neg(r \vee p))$
$\vdash ((\neg(r \vee p) \vee (p \vee (r \vee q))) \vee \neg(r \vee p)) \vee (p \vee (r \vee q))$
$\vdash (\neg(r \vee p) \vee (p \vee (r \vee q))) \vee (\neg(r \vee p)) \vee (p \vee (r \vee q)))$
$\vdash \neg(r \vee p) \vee (p \vee (r \vee q))$

$F_{11} = \neg r \vee (p \vee (r \vee q))$

Yes

T11

$\vdash \neg r \vee r$
$\vdash (\neg r \vee r) \vee (p \vee q)$
$\vdash \neg r \vee (r \vee (p \vee q))$
$\vdots$
$\vdash \neg r \vee (p \vee (r \vee q))$

$F_{12} = \neg p \vee (p \vee (r \vee q))$

Yes

T11

$\vdash \neg p \vee p$
$\vdash (\neg p \vee p) \vee (r \vee q)$
$\vdash \neg p \vee (p \vee (r \vee q))$
$\vdots$
$\vdash \neg p \vee (p \vee (r \vee q))$

Para F_2 temos

$$F_2 = \neg q \vee (\neg(r \vee p) \vee (r \vee q))$$
Goto (*)
No
i=2
$$\text{T63} \left| \begin{array}{l} \vdash \\ \vdots \\ \vdash \end{array} \right.$$
$$\neg(r \vee p) \vee (\neg q \vee (r \vee q))$$

$\vdash \neg r \vee (\neg q \vee (r \vee q))$
$\vdash \neg p \vee (\neg q \vee (r \vee q))$
$\vdash \neg(r \vee p) \vee (r \vee p)$
$\vdash (r \vee p) \vee \neg(r \vee p)$
$\vdash r \vee (p \vee \neg(r \vee p))$
$\vdash (p \vee \neg(r \vee p)) \vee (\neg q \vee (r \vee q))$
$\vdash p \vee (\neg(r \vee p) \vee (\neg q \vee (r \vee q)))$
$\vdash \neg(r \vee p) \vee (p \vee (\neg(r \vee p) \vee (\neg q \vee (r \vee q))))$
$\vdash (p \vee (\neg(r \vee p) \vee (\neg q \vee (r \vee q)))) \vee \neg(r \vee p)$
$\vdash p \vee ((\neg(r \vee p) \vee (\neg q \vee (r \vee q))) \vee \neg(r \vee p))$
$\vdash ((\neg(r \vee p) \vee (\neg q \vee (r \vee q))) \vee \neg(r \vee p)) \vee (\neg q \vee (r \vee q))$
$\vdash (\neg(r \vee p) \vee (\neg q \vee (r \vee q))) \vee (\neg(r \vee p)) \vee (\neg q \vee (r \vee q)))$
$\vdash \neg(r \vee p) \vee (\neg q \vee (r \vee q))$

$F_{21} = \neg r \vee (\neg q \vee (r \vee q))$
Yes
T66
$\vdash \neg r \vee r$
$\vdash (\neg r \vee r) \vee (\neg q \vee q)$
$\vdash \neg r \vee (r \vee (\neg q \vee q))$
$\vdots$
$\vdash \neg r \vee (\neg q \vee (r \vee q))$

$F_{22} = \neg p \vee (\neg q \vee (r \vee q))$
Yes
T66
$\vdash \neg q \vee q$
$\vdash (\neg q \vee q) \vee (\neg p \vee r)$
$\vdash \neg q \vee (q \vee (\neg p \vee r))$
$\vdots$
$\vdash \neg p \vee (\neg q \vee (r \vee q))$

Na próxima seção, submetemos $\mathfrak{P}$ a um estudo mais amplo no nível de metalinguagem.

Abreviaturas. Uma definição estabelece uma igualdade, ou uma equivalência convencional, entre a palavra que define (*definiendum*) e o objeto definido (*definiens*). Desse modo, uma definição deve ter a forma

expressão que se está a definir $\cdots = \cdots$ *expressão que define* ou
expressão que se está a definir $\cdots$ se, e só se, $\cdots$ *expressão que define* ou
expressão que se está adefinir $\cdots \Longleftrightarrow \cdots$ *expressão que define.*

Uma vez que uma definição está anunciada como tal, a equivalência é subentendida e é estilisticamente aceito escreve-la na forma

expressão que se define se *expressão que define.*

Isto evita o repetitivo emprego da expressão *se e só se*, uma prática livremente adotada, ou não, aqui.

A utilização apenas dos símbolos $\neg$ e $\vee$ na construção de fórmulas, com frequência, é incômodo, de difícil leitura e interpretação não intuitiva. Essas dificuldades são ultrapassadas por meio de abreviaturas que oferecem uma melhor compreensão do significado das fórmulas. A ideia por trás dessas abreviaturas foi introduzida, informalmente, nas preliminares ao cálculo proposicional. Elas são:

a) $A \to B \iff \neg A \vee B$,
b) $A \wedge B \iff \neg(\neg A \vee \neg B)$ e
c) $A \leftrightarrow B \iff (A \to B) \wedge B \to A$.

Essas abreviações são chamadas, respectivamente, de implicação, conjunção e equivalência. As suas leituras são.

a) $A \to B$ lê-se A *implica* B ou
   - se A *então* B ou
   - *se* A, B ou
   - B, *se* A ou
   - A *é condição suficiente para* B ou
   - B *é condição necessária para* A.

b) $A \wedge B$ lê-se A *e* B.
c) $A \leftrightarrow B$ lê-se A *equivale a* B ou
   - A *é condição necessária e suficiente para* B ou
   - A *se e só se* B ou
   - A *sse* B.

O leitor reconhecerá que esta maneiras de falar forma parte do léxico comum da matemática. O leitor também pode verificar que a tabelas de verdade para estas fórmulas são, para $A \wedge B$, $A \longrightarrow B$ e $A \longleftrightarrow B$, respectivamente as seguintes:

A	$\wedge$	B
1	1	1
1	0	0
0	0	1
0	0	0

A	$\longrightarrow$	B
1	1	1
1	0	0
0	1	1
0	1	0

A	$\longleftrightarrow$	B
1	1	1
1	0	0
0	0	1
0	1	0

Convenção Sobre Parenteses. Tacitamente, temos usado parenteses da mesma maneira do que em matemática: utilizamos [e] além de (e). Adotamos uma convenção de omissão de parenteses segundo a qual se atribui aos conectivos um *grau de coesão* ou *ligação*, como se descreve a seguir. Uma parte da fórmula formada por um conectivo, apendada a outra parte mediante um conectivo de menor *grau*, não precisa de parenteses; se o grau for igual, parenteses devem ser usados. Os graus estabelecem uma ordem entre conectivos desta maneira:

$$\neg \ > \ \vee \ = \ \wedge > \rightarrow = \leftrightarrow .$$

Numa fórmula com um conectivo aplicado repetitivamente, aplicamos a convenção de associação à direita, como anteriormente com $\vee$. Exemplos:

(i) $A \vee B \longrightarrow B \iff (A \vee B) \longrightarrow C$.

(ii) $D \wedge C \longrightarrow [A \longleftrightarrow C \vee A] \iff (D \wedge C) \longrightarrow [A \longleftrightarrow (C \vee A)]$.

Neste capítulo, letras latinas maiúsculas em itálico referem-se, salvo indicação no contrário, à fórmulas proposicionais. Evita-se assim expressões repetitivas de frases como '*seja A uma fórmula*' e similares.

A seguir, damos uma lista de tautologias de uso frequente. Pode-se ver que formam parte dos raciocínios habituais.

Tautologias de Uso Frequente.

1. $A \longleftrightarrow \neg\neg A$ (Dupla negação).
2. $A \vee B \longleftrightarrow B \vee A$.
3. $A \wedge B \longleftrightarrow B \wedge A$.
4. $A \wedge (B \wedge C \longleftrightarrow (A \wedge B) \wedge C$.
5. $A \vee (B \wedge C) \longleftrightarrow (A \vee B) \wedge (A \vee C)$.
6. $A \wedge (B \vee C) \longleftrightarrow (A \wedge B) \vee (A \wedge C)$.
7. $(B \longrightarrow A) \longrightarrow (\neg A \longrightarrow \neg B)$ (Contraposição)
8. $(\neg A \longrightarrow \neg B) \longrightarrow (B \longrightarrow A)$ (Recíproca de Contraposição).
9. $A \longleftrightarrow A \vee A$.
10. $A \longleftrightarrow A \wedge A$.
11. $\neg A \vee A$ (*Tercium non datur*).
12. $(A \longrightarrow B \wedge \neg B) \longrightarrow \neg A$ (*Reductio ad absurdum*).

13. $(A \longrightarrow \neg A) \longrightarrow \neg A$ (*Reductio ad absurdum*).
14. $\neg(A \vee B) \longleftrightarrow (\neg A \wedge \neg B)$ (De Morgan).
15. $\neg(A \wedge B) \longleftrightarrow (\neg A \vee \neg B)$ (De Morgan).
16. $(A \longrightarrow B) \wedge (A \longrightarrow C) \longrightarrow (A \longrightarrow B \wedge C)$
17. $(A \longrightarrow B) \wedge (B \longrightarrow C) \longrightarrow (A \longrightarrow C)$.
18. $A \longleftrightarrow B \iff B \longleftrightarrow A$.
19. $A \longrightarrow (B \longleftrightarrow A \wedge B)$.
20. $[A \longrightarrow (B \longrightarrow C)] \longleftrightarrow [A \wedge B \longrightarrow C)]$.

As tautologias constituem uma ferramenta eficaz para demonstrar algumas propriedades acerca de conjuntos, como as que se seguem. Damos algumas provas como exemplo.

Teorema 67.

1. $A \subseteq A$.
2. $(A \subseteq B) \wedge (B \subseteq C) \longrightarrow (A \subseteq C)$.
3. $(A \subseteq B) \wedge (B \subseteq A) \longrightarrow (A = B)$.
4. $\cup$ *é comutativa.*
5. $\cup$ *é associativa.*
6. $A \cup \emptyset = A = \emptyset \cup A$.
7. $\cap$ *é comutativa.*
8. $\cap$ *é associativa.*
9. $A \cap \emptyset = \emptyset = \emptyset \cap A$.
10. $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$.
11. $A \cup (B \cap C) = (A \cap B) \cup (A \cap C)$.
12. $(C \setminus A) \cup (C \setminus B) = C \setminus (A \cap B)$.
13. $(C \setminus A) \cap (C \setminus B) = C \setminus (A \cup B)$.
14. $A \times \emptyset = \emptyset = \emptyset \times A$.
15. $\bigcup(A \cup B) = \bigcup A \cup \bigcup B$.

Prova.

(1) $x \in A \longrightarrow x \in A$.
(2) $[(x \in A \longrightarrow x \in B) \wedge (x \in B \longrightarrow x \in C)] \longrightarrow (x \in A \longrightarrow x \in C)$.
(6) Ponha-se $(p \wedge \neg p)$ em lugar de $\emptyset$.
(10) Utilizar **5** do teorema anterior.
(15) Basta olhar as equivalências

$$\begin{array}{rcl} x \in \bigcup(A \cup B) & \iff & x \in y, \text{ para algum } y \in A \cup B \\ & \iff & x \in y, \text{ para algum } y \text{ tal que } y \in A \text{ ou } y \in B \\ & \iff & [x \in y, \text{ para algum } y \text{ tal que } y \in A] \vee [x \in y, \text{ para algum } y \text{ tal q} \\ & \iff & [x \in \bigcup A] \vee [x \in \bigcup B] \\ & \iff & x \in \bigcup A \cup \bigcup B. \end{array}$$

□

Regras de inferência derivadas. Algumas regras derivadas de uso frequente e fáceis de demonstrar e indicadas a seguir.

1. De A infere-se $\neg\neg A$.
2. De $\neg\neg A$ infere-se A.
3. De A e B infere-se $A \wedge B$.
4. De $A \wedge B$ infere-se A e infere-se B.
5. De $A \longrightarrow B$ e A infere-se B. (*Modus Ponens).*
6. *De* $A \longrightarrow B$ *infere-se* $\neg B \longrightarrow \neg A$.
7. *De* $\neg A \longrightarrow \neg B$ *infere-se* $\neg B \longrightarrow \neg A$.

Equivalentemente:

1. $\mathfrak{P} \vdash A \Longrightarrow \mathfrak{P} \vdash \neg\neg A$.
2. $\mathfrak{P} \vdash \neg\neg A \Longrightarrow \mathfrak{P} \vdash A$.
3. $(\mathfrak{P} \vdash A)$ & $(\mathfrak{P} \vdash A) \Longrightarrow (\mathfrak{P} \vdash A \wedge B)$.
   Etc.

Essas regras, bem como combinações delas, serão usadas aqui sem referência explícita.

Uma regra de uso frequente é a *Modus Ponens*, que consiste em derivar B a partir de A e de $A \to B$. Esta regra, adotada como regra primitiva em diversas versões do cálculo proposicional, resulta ser uma consequência das regras primitivas adotadas aqui.

Teorema 68 (*Modus Ponens*).

De A *e* $A \to B$, *infere-se* B.

Prova. Suponha A e $A \to B$. Esta última é uma abreviação de $\neg A \vee B$. De A, por Expansão e Comutatividade, obtemos $B \vee A$ e $B \vee \neg A$. Daqui, por Corte, $B \vee B$ e, por Contração, B. □

Regras de Inferência *versus* **Teoremas.** Cada regra de inferência é refletida por um teorema e vice-versa. A seguir especificamos, para cada regra de inferência, qual é o teorema que a reflete.

(i) Expansão: $\vdash A \to A \vee A$.

(ii) Contração: $\vdash A \vee A \to A$.
(iii) Associativa: $\vdash A \vee (B \vee C) \to (A \vee B) \vee C$.
(iv) Corte: $\vdash (A \vee C) \wedge (B \vee \neg C) \to (A \vee B)$.

Reciprocamente, a partir destes teoremas, pode-se voltar, por meio de *Modus Ponens*, às regras de inferência originais.

Mas observe-se que da maneira em que o sistema é apresentado aqui, não é possível substituir as regras pelas suas contrapartes adotadas como axiomas. Isso porque, se ficar com um sistema sem regras de inferência, para aplicar as regras às suas premissas é preciso *Modus Ponens*.

Propriedades metamatemáticas de $\mathfrak{P}$

No início deste capítulo temos mencionado a diferença entre linguagem e a metalinguagem, ressaltando a separação entre ambas e como é na metalinguagem que é possível estudar e expressar propriedades de um sistema - estas são referidas como propriedades metamatemáticas do sistema. A seguir, examinaremos algumas dessas propriedades no caso do cálculo proposicional; elas exemplificam algumas das propriedades que, em geral, são de interesse em determinar se um sistema goza ou não da propriedade. Cabe aqui introduzir alguns símbolos metalinguísticos que facilitarão o discurso.

Símbolos Metalinguísticos. Usamos na metalinguagem $\widehat{\neg}, \widehat{\vee}, \&, \widehat{\exists}$, e $\widehat{\forall}$ para a negação, disjunção e quantificadores existencial e universal, respectivamente. Maiúsculas cursivas são sempre variáveis de fórmulas. Letras gregas maiúsculas serão conjuntos de fórmulas.

Decidibilidade. Num sistema formal, o problema de determinar por meios finitos se uma fórmula é ou não teorema, e se o é, oferecer um algoritmo para construir uma tal prova, é chamado de *problema da decisão.* Diz-se, neste caso, que o sistema é *decidível.* Por *meios finitos* e *algoritmo* significam uma rotina de raciocínio que, aplicada um número finito de vezes, conduz a um resultado ou resposta. Pelo que temos visto:

Teorema 69. $\mathfrak{P}$ *é decidível.*

Consistência. Uma motivação por trás do conceito de consistência diz respeito a expressar ausência de falsidade, ou contradição, e tem dois aspectos: o primeiro, de carácter semântico, visa que não haja afirmações (teoremas) do sistema que expressem falsidades no universo que o interpreta, propriedade que no caso de $\mathfrak{P}$ recebe o nome de *validade* e está assegurado pelo teorema A. O segundo é de carácter sintático e visa que não haja contradições internas ao sistema. Este

requerimento fica expressado pela condição de que não haja fórmula A tal que ela e a sua negação sejam teoremas do sistema. Usando $Consist(\mathfrak{P})$ para dizer que $\mathfrak{P}$ é consistente, definimos

DEFINIÇÃO 38. $Consist(\mathfrak{P})$: $\widehat{\neg}\widehat{\exists}A[(\mathfrak{P} \vdash A)\&(\mathfrak{P} \vdash \neg A)]$.

E fácil demonstrar que esta condição é equivalente a afirmação que *a conjunção de uma fórmula com a sua negação não é teorema* e equivalente a *existe alguma fórmula que não é teorema.*

TEOREMA 70. . *Estas três condições são equivalentes:*

1. $Consist(\mathfrak{P})$.
2. $\widehat{\neg}\exists A[\mathfrak{P} \vdash A \wedge \neg A]$.
3. $\widehat{\exists}A[\mathfrak{P} \nvdash A]$.

Prova. Para a primeira equivalência, podem ser usadas as tautologias: $A \rightarrow (B \rightarrow A \wedge B)$, $A \wedge B \rightarrow A$ e $A \wedge B \rightarrow B$. Para a segunda equivalência, usar $A \wedge \neg A \rightarrow B$, para qualquer B.

□

A última equivalência mostra que num sistema inconsistente não apenas as contradições mas *todas* as fórmulas são teoremas; isto faz que um sistema inconsistente não tenha interesse nenhum.

O teorema A conduz de imediato ao fato que $\mathfrak{P}$ é consistente.

TEOREMA 71. $Consist(\mathfrak{P})$.

Prova. Pelo teorema A: $\mathfrak{P} \nvdash A \wedge \neg A$.

□

Por outro lado, a consistência sintática de $\mathfrak{P}$, esá assegurada também pelo teorema A, pois todo o que se afirma no sistema - os seus teoremas - são taautologias, portanto não há contradições no aspecto sintático.

TEOREMA 72. $\mathfrak{P}$ *é sintaticamente consistente.*

O estudo das próximas propriedades metamatemáticas de $\mathfrak{P}$ demanda por um par de ferramentas: os conceitos de *prova a partir de hipóteses* e de *teorema da dedução.*

Provas a partir de hipóteses. Teorema da Dedução. No exercício dedutivo comum, com frequência se elabora argumentos a partir de suposições hipotéticas que podem ou não corresponder a um estado atual de circunstâncias, com o objetivo de refutar uma premissa ou um argumento, ou para escolher a mais apropriada dentre várias possibilidades de ação, etc. O mesmo procedimento

é adotado na matemática, onde é habitual construir uma prova sob a suposição de alguma hipótese H, obter uma conclusão C e terminar afirmando que $H \to C$. Por exemplo, num sistema de geometria euclídea $\mathfrak{G}$, a partir da suposição H de um triângulo ter dois lados iguais, se demonstra que os ângulos da base são iguais, (C). Conclui-se que, em $\mathfrak{G}$, tem-se $H \to C$; isto é, $\mathfrak{G} \vdash H \to C$.

Em Lógica este tipo de raciocínio está formalizado no conceito de *prova a partir de hipóteses*; em particular, em $\mathfrak{P}$ isso é capturado na definição seguinte.

Definição 39. *Uma prova em $\mathfrak{P}$ a partir da hipótese H é uma sequência de fórmulas $A_1, ..., A_n$, na qual cada A_i:*

1. *é um axioma ou*
2. *é H ou*
3. *é obtido a partir de fórmulas anteriores por meio das regras de inferência.*

Daqui em diante, usaremos $\mathfrak{P} \cup \{H\}$ para referirmos-nos ao sistema $\mathfrak{P}$, ampliado com H como uma hipótese extra inserida no sistema. A adoção de H como hipótese equivale à sua incorporação em $\mathfrak{P}$, como um novo axioma, o que dá lugar a um novo sistema $\mathfrak{P} \cup \{H\}$. Naturalmente, tanto H como qualquer axioma, pode aparecer ou não numa prova neste novo sistema.

Definição 40. *$\mathfrak{P} \cup \{H\} \vdash C$ significa que existe em $\mathfrak{P} \cup \{H\}$ uma prova de C (a partir de H).*

Se está claro que o sistema de referência é $\mathfrak{P}$, pode-se escrever simplesmente

$$H \vdash C.$$

Pode haver várias hipóteses, mas basta considerar apenas uma. É fácil generalizar a qualquer número. Mais explicitamente:

Definição 41. *Uma prova a partir de um conjunto $\{H_1, ..., H_k\}$ de fórmulas (hipóteses), é uma sequência $A_1, ..., A_n$, tal que cada A_i*

1. *é um axioma ou*
2. *um dos $H_i's$ ou*
3. *é obtido a partir de fórmulas anteriores por meio das regras de inferência.*

Notação 6.

$$H_1, \ldots, H_k \vdash C \iff \textit{existe uma prova de } C \textit{ a partir de } H_1, \ldots, H_k.$$

Pode-se generalizar a definição para quaisquer conjuntos de fórmulas proposicionais. Usaremos letras gregas maiúsculas, $\Sigma, \Theta, \Gamma, \ldots$ para fazer referência a conjuntos de fórmulas proposicionais.

DEFINIÇÃO 42. *Seja Σ um conjunto (finito ou infinito) de fórmulas proposicionais. Então,* $\Sigma \vdash C \iff (\exists H_1, \ldots, H_k \in \Sigma)[H_1, \ldots, H_k \vdash C]$.

Estes conceitos não são exclusivos de $\mathfrak{P}$; são comuns a qualquer sistema formal, como é o caso do exemplo no início desta subsecção. Em particular, é imediato da definição que

$$C \in \Sigma \Longrightarrow \Sigma \vdash C.$$

As seguintes propriedades resultam ser úteis.

TEOREMA 73 (Propriedades da relação $\vdash$).

1. $A \vdash A$.
2. $A \vdash B \Longrightarrow A \vdash B \vee C$.
3. $\Sigma \vdash B \Longrightarrow \Sigma \cup \{A\} \vdash B$.
4. $\Sigma \vdash B \Longrightarrow \Sigma \cup \{A\} \vdash B$.

O conceito de prova a partir de hipóteses está intimamente relacionado com o *Teorema da Dedução.*

Este afirma que, se há uma demonstração de C no sistema ampliado $\mathfrak{P} \cup \{H\}$, então há uma demonstração de $H \to C$ no sistema original $\mathfrak{P}$, justificando assim o que é prática comum em matemática.

TEOREMA 74 (Teorema da Dedução). $\mathfrak{P} \cup \{H\} \vdash C \iff \mathfrak{P} \vdash H \to C$.

Prova.

Da direita para a esquerda o resultado é fornecido por *Modus Ponens.* No sentido contrário, seja $A_1, \ldots, A_n = C$ uma prova de C a partir da hipótese H em que $H \in \{A_1, \ldots, A_n\}$. Demonstramos que para todo o n, é o caso que $\mathfrak{P} \vdash H \to C$. A demonstração é por indução sobre o comprimento da prova.

Para $n = 1$, a prova consiste de apenas *uma* fórmula, $A_1 = C$, a qual só pode ser

(i) um axioma proposicional, ou
(ii) H.

Em ambos os casos $H \to A_1$ é uma tautologia e, assim, um teorema de $\mathfrak{P}$. Consequentemente $\mathfrak{P} \vdash H \to C$.

Para $n = 2$, a prova é A_1, C. Como o corte precisa de duas premissas, sem considerar casos triviais, C só pode ser derivada de A_1 por expansão, contração ou associativa. É fácil verificar que em todos estes casos $H \to C$ é uma tautologia e, portanto, $\mathfrak{P} \vdash H \to C$.

Para o último passo da indução, a hipótese indutiva é para cada $k < n$ *existe uma prova de comprimento k.* Demonstramos que existe uma prova $H \to C$. Para $i, j < n$ temos os seguintes possíveis casos:

(i) C é inferido de A_i por meio da regra de expansão.
(ii) C é inferido de $A_i \vee A_i$ por meio da regra de contração.
(iii) C é inferido de $D \vee (E \vee F)$ por meio da regra asssociativa.
(iv) C é inferido de $D \vee E$ e $\neg D \vee F$ por meio da regra de corte.

Cada um desses casos é verificado a seguir.

(i) C é da forma $E \vee A_i$.
Pela hipótese indutiva tem-se $\vdash H \to A_i$.
Também tem-se que $\vdash A_i \to E \vee A_i$.
Daqui $\vdash H \to E \vee A_i$, isto é, $\vdash H \to C$.

(ii) C é A_i.
Pela hipótese indutiva $\vdash H \to A_i \vee A_i$.
Também tem-se que $\vdash A_i \vee A_i \to A_i$.
Daqui $\vdash H \to A_i$, isto é, $\vdash H \to C$.

(iii) C é $(D \vee E) \vee F$.
Segundo a hipótese indutiva: $\vdash H \to D \vee (E \vee F)$.
Aliás, tem-se $\vdash [D \vee (E \vee F)] \to [(D \vee E) \vee F]$.
Portanto $\vdash H \to [(D \vee E) \vee F]$, isto é, $\vdash H \to C$.

(iv) C é $E \vee F$.
A hipótese indutiva dá: $\vdash H \to D \vee E$ e $\vdash H \to \neg D \vee F$.
Daqui $\vdash H \to [(D \vee E) \wedge (\neg D \vee F)]$.
Portanto $\vdash H \to E \vee F$, isto é, $\vdash H \to C$.

□

Uma forma mais geral do teorema da dedução é

$$H_1, ..., H_k \vdash C \iff \mathfrak{P} \vdash H_1 \wedge ... \wedge H_k \longrightarrow C,$$

que se obtém aplicando a forma original iterativamente à $H_1, ..., H_k$.

Se o sistema de referência é claro pelo contexto, o teorema tem a forma

$$H \vdash C \iff \vdash H_1 \wedge ... \wedge H_k \to C.$$

O material desenvolvido até aqui permite examinar, para além das já vistas, outras propriedades metamatemáticas de $\mathfrak{P}$ que são de interesse na lógica e nos fundamentos da matemática.

Completude Semântica. Quando se estabelece um sistema formal para se falar acerca de alguma realidade ou universo, se espera descrever um setor desse universo. Por exemplo, a teoria de grupos descreve e demonstra certos fatos que acontecem nos grupos, mas não descreve *todos* os fatos que acontecem num grupo particular, que pode ser ou não ser comutativo, finito, etc. No caso do cálculo proposicional, em virtude do teorema de completude, temos que *tudo* o

que acontece - isto é, é verdadeiro - no universo {0,1} com as suas operações $*$ e $\triangledown$ é demonstrável no sistema formal, o que se expressa dizendo que o cálculo proposicional é *completo*. Uma vez que o conceito de *completude* estabelece uma conexão entre o sistema formal e a sua interpretação, este é referido como *completude semântica*. Com esta conotação, o resultado da seção anterior é reformulado como

TEOREMA 75. *$\mathfrak{P}$ é semanticamente completo.*

Um maneira sugestiva de expressar o mesmo é que há uma correspondência *total* entre o sistema formal e a sua realidade alvo, uma situação ideal que em geral não acontece com teorias.

Completude Sintática. Por outro lado, há o conceito de *completude sintática*, que consiste em que não é possível enriquecer estritamente o sistema formal acrescentando novos axiomas; *estritamente*, no sentido que ao se adotar um novo axioma ou teorema, nada seria acrescentado. É fácil ver que um sistema formal é sintaticamente completo neste sentido se, e somente se, a introdução de um novo axioma (estritamente) resulta na inconsistência do sistema. Uma maneira gráfica, que usaremos aqui, de descrever a situação é dizendo que o sistema é *saturado por teoremas*, no sentido em que não pode ter mais teoremas do que aqueles que já tem.

DEFINIÇÃO 43. *Diremos aqui que um sistema formal é sintaticamente completo, ou saturado por teoremas, se a introdução no sistema de uma fórmula (que não seja teorema) como um novo axioma provoca a inconsistência do sistema resultante.*

TEOREMA 76. *$\mathfrak{P}$ não é saturado por teoremas.*

Prova. Considere-se qualquer contingência B de $\mathfrak{P}$. Mostramos que a introdução de B como um novo axioma em $\mathfrak{P}$ não compromete a consistência no sistema $\mathfrak{P} \cup \{B\}$.

Suponhamos o contrário. Então, a partir de B existe em $\mathfrak{P} \cup \{B\}$ uma prova de $C \wedge \neg C$, isto é, $\mathfrak{P} \cup \{B\} \vdash C \wedge \neg C$. Pelo teorema da dedução temos $\mathfrak{P} \vdash B \rightarrow C \wedge \neg C$. Isto significa que $B \rightarrow C \wedge \neg C$ é uma tautologia, e daqui, que B é uma contradição (todos os seus valores são 0), o que contradiz a escolha de B. Concluímos que $\mathfrak{P} \cup \{B\}$ é consistente e portanto $\mathfrak{P}$ não é saturado por teoremas. □

Mais um conceito de completude sintática. Outro conceito de completude sintática diz respeito à negação. Diremos *aqui* que um sistema é *completo*

com respeito à negação ou, simplesmente, *por negações*, se para toda a fórmula A tem-se que A é um teorema do sistema ou $\neg A$ é um teorema do sistema. Mais à frente veremos que as propriedades de saturação e de completude por negações são equivalentes.

TEOREMA 77. *$\mathfrak{P}$ não é completo por negações.*

Prova. Seja B uma contingência de $\mathfrak{P}$. Claramente, nem B nem $\neg B$ são teoremas de $\mathfrak{P}$. □

Mais acima, vimos que $\mathfrak{P}$ não é saturado por teoremas.

A situação é diferente caso se acrescente a $\mathfrak{P}$ uma nova regra de inferência: a *regra de substituição*. Isto é, uma regra que permite inferir de uma fórmula qualquer fórmula que resulte da substituição de uma variável por uma outra fórmula, em todos os lugares nos quais a dita variável ocorre. Chamemos $\mathfrak{P} \cup \{Subst\}$ a este novo sistema.

TEOREMA 78. *$\mathfrak{P} \cup \{Subst\}$ é saturado de teoremas.*

Prova. Acrescente-se uma fórmula A aos axiomas de $\mathfrak{P} \cup \{Subst\}$. Chamemos $[\mathfrak{P} \cup \{Subst\}] \cup \{A\}$ ao sistema assim obtido. A não deve ser uma tautologia, pois seria redundante. Já que A não é uma tautologia, seja v uma valoração tal que $v(A) = 0$. Considere-se as variáveis x de A tais que $v(x) = 0$. Substitua-se em A cada variável x por $x \wedge \neg x[?????]$. Com isto, obtém-se uma fórmula A', que é uma contradição. Devido ao fato que A' é obtido a partir de A por substituição, a adoção de A como teorema conduz a aceitar A' como teorema de $[\mathfrak{P} \cup \{Subst\}] \cup \{A\}$, o que mostra que $[\mathfrak{P} \cup \{Subst\}] \cup \{A\}$ é inconsistente. □

É claro que $\mathfrak{P}$ não é completo por negações. Pois, se A é uma fórmula que não é tautologia e se adotarmos o valor 1 para alguma atribuição de valores, então nem A nem $\neg A$ são teoremas.

Extensões de $\mathfrak{P}$. A não saturação de $\mathfrak{P}$ significa que este não é um sistema fechado e indica que está aberto à possibilidade de ser expandido em diversas direções, incorporando contingências como novos axiomas. Isto leva a estudar as propriedades metamatemáticas, anteriormente limitadas a $\mathfrak{P}$, num contexto mais amplo: o de *conjuntos de fórmulas*. Estes conjuntos de fórmulas são concebidos em geral como *sistemas proposicionais*. Para o que nos interessa aqui, eles são extensões de $\mathfrak{P}$. Por conseguinte a linguagem, as regras de inferência e os axiomas proposicionais continuam presentes.

Neste capítulo, usaremos letras gregas maiúsculas para fazer referência a conjuntos de fórmulas proposicionais; uma letra grega maiúscula terá este significado.

Os novos sistemas terão a forma $\mathfrak{P} \cup \Sigma$. Uma *prova de A em $\mathfrak{P} \cup \Sigma$* não é outra coisa além de uma prova em $\mathfrak{P}$ a partir (das hipóteses) em Σ, ou seja,

$\mathfrak{P} \cup \Sigma \vdash A$. Por brevidade, em lugar de $\mathfrak{P} \cup \Sigma \vdash A$, frequentemente escreveremos simplesmente $\Sigma \vdash A$.

O conceito de consistência semântica em $\mathfrak{P}$ estava descrito pela condição de *validade* e consistia em *ser verdade sempre*: um teorema deve ser *válido*. No contexto de conjuntos de fórmulas, este critério não é aplicável: as novas fórmulas desempenham o papel de axiomas e as fórmulas derivadas deles são os teoremas, mas não são verdades sempre, só *às vezes*. O conceito de não contradição neste caso é expressado pela noção de *satisfatibilidade*, a qual se refere à possibilidade de *todas* as fórmula de Σ serem simultaneamente satisfeitas por alguma atribuição de valores às variáveis de $\mathfrak{P}$. Usaremos a notação $Sat(\Sigma)$ como abreviatura de Σ *é satisfazível*. Se apreciará que esta é uma versão do Teorema A, no novo contexto.

DEFINIÇÃO 44. $Sat(\Sigma) \iff \widehat{\exists} v \widehat{\forall} \varphi \in \Sigma(v(\varphi) = 1)$.

Assim como na prova do teorema A, se mostra que a aplicação das regras de inferência preservam a propriedade de ser tautologia. É fácil provar que elas preservam também a satisfatibilidade.

A consistência sintática é reformulada no novo contexto de maneira natural:

DEFINIÇÃO 45. $Consist(\Sigma) \iff \widehat{\neg}\widehat{\exists} A(\Sigma \vdash A \wedge \neg A)$.

De resto, todos os conceitos metamatemáticos referidos a $\mathfrak{P}$ são reformulados dentro do novo contexto de maneira natural. Basta substituir, nas definições anteriores de completude, etc, $\mathfrak{P}$ por $\mathfrak{P} \cup \Sigma$ ou, mais brevemente, por Σ. O mesmo é aplicado às regras de inferência primitivas e derivadas de $\mathfrak{P}$.

No que segue, se não houver declaração explícita no sentido contrário, um sistema formal sempre será considerado consistente.

Uma condição equivalente à consistência é dada pelo

TEOREMA 79. $\widehat{\neg} Consist(\Sigma) \iff \widehat{\forall} A(\Sigma \vdash A)$.

Prova. Trivial, dada pelo Teorema da Dedução e por $\vdash A \wedge \neg A \longrightarrow A$. □

O próximo teorema oferece uma condição necessária e suficiente a cumprir pelas fórmulas que podem ser agregadas a um sistema sem comprometer a consistência: serão as negações daquelas que não são teorema de Σ e a aquelas cuja negação não é teorema de Σ; o qual está resumido no

TEOREMA 80. *Se* Σ *é consistente, então* $\Sigma \nvdash A \iff Consist(\Sigma \cup \{\neg A\})$.

Prova. Suponha-se que Σ é consistente. Se $\Sigma \vdash A$, temos $\Sigma \cup \{\neg A\} \vdash A$ como propriedades da relação $\vdash$.

Também temos $\Sigma \cup \{\neg A\} \vdash \neg A$ (propriedades de $\vdash$), o que mostra que

$$\widehat{\neg} Consist(Sigma \cup \{\neg A\}).$$

Por outro lado, suponha-se que $\widehat{\neg} Consist(\Sigma \cup \{\neg A\})$. Então

$$\Sigma \cup \{\neg A\} \vdash A$$

pois num sistema inconsistente deriva-se qualquer fórmula. Pelo teorema da dedução, $\Sigma \vdash \neg A \longrightarrow A$, ou seja,

$$\Sigma \vdash \neg\neg A \vee A.$$

Portanto $\Sigma \vdash A \vee A$ e daqui, finalmente, $\Sigma \vdash A$ por contração. □

Uma consequência do teorema anterior é que dada qualquer fórmula, pode ser agregada a Σ ela ou a sua negação, preservando a consistência.

Teorema 81. *Para qualquer fórmula A tem-se que*

$$Consist(\Sigma) \Longrightarrow Consist(\Sigma \cup \{A\}) \widehat{\vee} Consist(\Sigma \cup \{\neg A\}).$$

Prova. Demonstramos que se Σ é consistente, um dos disjuntos no lado direito deve ser consistente. Assim, suponha-se tanto que $Consist(\Sigma)$ quanto que $\widehat{\neg} Consist(\Sigma \cup \{A\})$. Então

$$\begin{aligned}
\widehat{\neg} Consist(\Sigma \cup \{A\}) &\Longrightarrow \Sigma \cup \{A\}) \vdash \neg A \\
&\Longrightarrow \Sigma \cup \{A\}) \vdash \neg A \\
&\Longrightarrow \Sigma \vdash A \longrightarrow \neg A \\
&\Longrightarrow \Sigma \vdash \neg A \vee \neg A \\
&\Longrightarrow \Sigma \vdash \neg A \\
&\Longrightarrow Consist(\Sigma \cup \{\neg A\}).
\end{aligned}$$

□

Teorema 82. *Se Σ é saturado por teoremas, então*

$$Consist(\Sigma \cup \{A\}) \iff \Sigma \vdash A.$$

Teorema 83. *Se Σ é consistente, então*

$$\Sigma \text{ é completo por negações} \iff \Sigma \text{ é saturado por teoremas.}$$

Prova. Suponha-se que Σ é completo por negações. Seja $\Sigma \nvdash A$. Então $\Sigma \vdash \neg A$ e a introdução de A em Σ produz $\Sigma \cup \{\neg A\} \cup \{A\}$, um sistema inconsistente.

Reciprocamente, se Σ é saturado por teoremas, seja A tal que $\Sigma \nvdash A$. Pelo teorema anterior, $Consist(\Sigma \cup \{\neg A\})$. Daqui, $\Sigma \vdash \neg A$. □

Após algumas preparações, veremos que todo conjunto de fórmulas (de $\mathfrak{P}$) consistente tem uma extensão completa. Antes, vejamos como os conceitos se relacionam.

Obviamente, $\mathfrak{P}$ não é completo com respeito à negação: como visto, dada uma fórmula que seja uma contingência, nem ela nem a sua negação são teoremas e o cálculo proposicional pode ser expandido para uma extensão completa neste sentido. Isto nos leva a estudar de que maneira se relacionam os conceitos de *consistência* e *satisfatibilidade*.

Consistência e satisfatibilidade. Temos critérios de consistência sintática e semântica para qualquer conjunto de fórmulas Σ. Queremos ver de que maneira estes dois conceitos se relacionam. É fácil ver que a segunda implica a primeira, como estabelece o

TEOREMA 84. $Sat(\Sigma) \Longrightarrow Consist(\Sigma)$.

Prova. Se Σ não é consistente, então existe um subconjunto finito dele cuja conjunção implica $A \wedge \neg A$, o que obriga a que o seu valor seja sempre 0. Donde, esse subconjunto não é satisfazível.

Agora, suponha-se que Σ é inconsistente; então $\Sigma \vdash C \wedge \neg C$ e há um subconjunto finito $\{H_1, \ldots, H_n\}$ de Σ tal que

$$\{H_1, \ldots, H_n\} \vdash C \wedge \neg C.$$

Disto, por meio de repetidas aplicações do teorema da dedução:

$$\mathfrak{P} \vdash H_1 \to (\cdots \to (H_n \to C \wedge \neg C) \cdots).$$

Donde, $\mathfrak{P} \vdash H_1 \wedge \cdots \wedge H_n \to C \wedge \neg C$.

Mas isto implica que o valor de $H_1 \wedge \cdots \wedge H_n$ é sempre 0, com o qual Σ não é satisfazível, contradizendo a suposição inicial. Concluímos que Σ é consistente. □

No caso de Σ ser finito, o recíproco também é certo:

TEOREMA 85. *Se Σ é finito, então* $Consist(\Sigma) \Longrightarrow Sat(\Sigma)$.

Prova. Se Σ é finito, é da forma $\Sigma = \{H_1, \ldots, H_n\}$.

A consistência de Σ implica que a partir dela não se deriva contradição. Pelo teorema da dedução, a conjunção dos elementos de Σ não implica contradição. Assim, essa implicação não é teorema e, portanto, alguma atribuição de valores dá a esta implicação o valor 0. Ora, essa atribuição deve dar à conjunção dos

$H_{i's}$ o valor 1. Em símbolos:

$$\begin{aligned}
Consist(\Sigma) &\Longrightarrow \widehat{\neg}\widehat{\exists}H_1,\ldots,H_n\ [\{H_1,\ldots,H_n\}\vdash A\wedge\neg A]\\
&\Longrightarrow \widehat{\neg}\widehat{\exists}H_1,\ldots,H_n[\vdash H_1\wedge\cdots\wedge H_n\longrightarrow A\wedge\neg A]\\
&\Longrightarrow \widehat{\forall}H_1,\ldots,H_n\widehat{\neg}[\vdash H_1\wedge\cdots\wedge H_n\longrightarrow A\wedge\neg A]\\
&\Longrightarrow \widehat{\forall}H_1,\ldots,H_n\widehat{\neg}[Taut(H_1\wedge\cdots\wedge H_n\longrightarrow A\wedge\neg A)]\\
&\Longrightarrow \widehat{\forall}H_1,\ldots,H_n\widehat{\exists}v[v(H_1\wedge\cdots\wedge H_n\longrightarrow A\wedge\neg A)=0]\\
&\Longrightarrow \widehat{\forall}H_1,\ldots,H_n\widehat{\exists}v[v(H_1\wedge\cdots\wedge H_n)=1]\\
&\Longrightarrow Consist(\Sigma).
\end{aligned}$$

□

Surge aqui a questão sobre se este teorema continua a valer para conjuntos infinitos de fórmulas. Um exame da demonstração anterior mostra que Σ é consistente se e somente se todos os seus subconjunto finitos são satisfatíveis. Para ver isto, repara-se que os teoremas de Σ são fórmulas demonstradas a partir dum número finito de fórmulas de Σ.

Teorema 86. $Consist(\Sigma\ ) \Longleftrightarrow\ (\widehat{\forall}\Gamma\subseteq_{fin}\Sigma)[Sat(\Gamma)]$.

Prova. É vista nas equivalências

$$\begin{aligned}
Consist(\Sigma) &\Longleftrightarrow \Sigma\nvdash A\wedge\neg A\\
&\Longleftrightarrow \widehat{\forall}\Gamma\subseteq_{fin}\Sigma[Consist(\Gamma)]\\
&\Longleftrightarrow \widehat{\forall}\Gamma\subseteq_{fin}\Sigma[Sat(\Gamma)].
\end{aligned}$$

Alternativamente,

$$\begin{aligned}
\widehat{\neg}Consist\Sigma &\Longleftrightarrow \Sigma\vdash A\wedge\neg A\\
&\Longleftrightarrow \widehat{\exists}\Gamma\subseteq_{fin}\Sigma(\Gamma\vdash A\wedge\neg A)\\
&\Longleftrightarrow \widehat{\exists}\Gamma\subseteq_{fin}\Sigma[\widehat{\neg}Sat(\Gamma)].
\end{aligned}$$

□

Generalizando o conceito de "saturado por teoremas" cabe dar aqui um conceito de completude para conjuntos de fórmulas.

Completude (por negações).

Definição 46. $Compl(Sigma) \Longleftrightarrow \widehat{\forall}A\in Flas[(A\in\Sigma)\nabla(A\notin\Sigma)])$.

Quando houver necessidade de distinguir este conceito, de outros conceitos de completude nos referiremos a ele como *completude por negações*. Esta denominação não é a habitual na literatura.

Um sistema consistente e completo é fechado por teoremas no sentido do seguinte

TEOREMA 87. *Se* $Consist(\Sigma)$ *e* $Compl(\Sigma)$, *então* $\Sigma \vdash A \Longrightarrow A \in \Sigma$.

Prova. Seja $\Sigma \vdash A$. Se $A \notin \Sigma$, então $\neg A \in \Sigma$, contra a consistência de Σ. □

Para estabelecer a equivalência entre consistência e satisfatibilidade, sem a limitação da finitude é necessário mostrar que dado um conjunto consistente Σ, existe uma atribuição de valores às variáveis proposicionais de Σ que satisfaz todas as fórmulas de Σ. Em particular, se uma variável proposicional pertence a Σ, obviamente essa variável deve adotar o valor 1; se a sua negação pertence a *Sigma*, então deve adotar o valor 0. Mas pode haver variáveis ou negações de variáveis que, sem pertencer a Σ, ocorrem *dentro* das suas fórmulas. Não há maneira de determinar os valores que devem adotar estas últimas. Este problema desaparece se Σ for completo (por negações): bastaria atribuir 1 às variáveis que estão em Σ e 0 às variáveis cuja negação está em Σ. Como, em geral, Σ não é completo, podemos alargá-lo a uma extensão completa Θ. Se Θ é satisfazível, *a fortiori*, Σ também o é.

Procedemos a construção de uma extensão completa de Σ. Mas, antes, observe-se que há tantas fórmulas proposicionais quanto números naturais. Isto é consequência do dito nas Preliminares acerca de conjuntos contáveis,

$$\begin{aligned} F_n \text{ é enumerável} &\Longrightarrow \text{as negações de elementos de } F_n \text{ é enumerável.} \\ &\Longrightarrow \text{as disjunções de elementos de } F_n \text{ é enumerável.} \\ &\Longrightarrow \text{A reunião de enumeráveis é enumerável.} \end{aligned}$$

Consequentemente, se F_n é contável então F_{n+1} é contável. Portanto

TEOREMA 88. $Flas(\mathfrak{P})$ *é contável.*

Estabelecido o fato de haver tantas fórmulas de $\mathfrak{P}$ como números naturais, seja $A_0, A_1, \ldots$ uma enumeração das fórmulas de $\mathfrak{P}$. Com ela, podemos definir uma sequência de conjuntos $\langle \Psi_n \rangle_{\in \omega}$ por recursão sobre naturais como segue (lembrar aqui o Teorema 61).

DEFINIÇÃO 47.

1. $\Psi_0 = \Sigma$.
2. $\Psi_{n+1} = \begin{cases} \Psi_n \cup \{A_n\} & se \;\; Consist(\Psi_n \cup \{A_n\}) \\ \Psi_n \cup \{\neg A_n\} & se \;\; \widehat{\neg} Consist(\Psi_n \cup \{A_n\}) \end{cases}$.
3. $\Theta = \bigcup_{n \in \omega} \Psi_n$.

É claro que $\Psi_i \subseteq \Psi_j$ para $i < j$. Vejamos que todos os $\Psi_{i's}$ são consistentes:

TEOREMA 89. $\forall n \in \mathbb{N}[Consist(\Psi_n)]$.

Prova. Indução sobre n.

1. Para $n = 0$, é claro.
2. Hipótese indutiva: suponhamos $Consist(\Psi_n)$.
   (i) Se $\Psi_{n+1} = \Psi_n \cup \{A_n\}$, então Ψ_{n+1} é consistente por definição.
   (ii) Se $\Psi_{n+1} = \Psi_n \cup \{\neg A_n\}$, então Ψ_{n+1} é consistente por teorema .... XXXXXXX [????]

□

Obtemos, assim, uma sequência estritamente crescente de subconjuntos de $Flas(\mathfrak{P})$: $\Sigma \subsetneqq \Psi_1 \subsetneqq \Psi_2 \ldots$, cuja união resulta em

$$\Theta = \bigcup_{n \in \omega} \Psi_n.$$

Veremos que Θ é uma extensão consistente e completa (por negações) de Σ. As propriedades de Θ que nos interessam são resumidas no seguinte

TEOREMA 90.

1. $\Sigma \subseteq \Theta$.
2. $Consist(\Theta)$.
3. $Compl(\Theta)$.

Prova. .

1. Está incluído na definição de Θ.
2. Suponha-se que $\widehat{\neg} Consist(\Theta)$. Então existem $B_1, \ldots, B_n \in \Theta$ tais que

   $$B_1, \ldots, B_n \vdash A \wedge \neg A$$

   Pela construção de Θ, existe $k \in \mathbb{N}$ tal que $\{B_1, \ldots, B_n\} \subseteq \Psi_k$. Então $\Psi_k \vdash A \wedge \neg A$, o que contradiz a consistência de Ψ_k. Isto mostra a consistência de Θ.
3. Suponha-se $A \notin \Theta$. Sabemos que $A = A_n$ para algum natural n e, em particular, $A_n \notin \Psi_{n+1}$. Por definição de Ψ_{n+1},

   $$\widehat{\neg} Consist(\Psi_n \cup \{A_n\}),$$

   donde $\Psi_{n+1} = \Psi_n \cup \{\neg A_n\}$, mostrando que $\neg A \in \Theta$ e que Θ é completa relativamente à negação.

□

Resumindo,

TEOREMA 91.

1. $Consist(\Sigma) \Longrightarrow \widehat{\exists}\Theta\ [\Sigma \subseteq \Theta\ \&\ Consist(\Theta)\ \&\ Compl(\Theta))]$.

2. $Consist(\Sigma) \Longrightarrow \widehat{\exists}\Psi\ [Consist(\Psi)\ \&\ Compl(\Psi)\ \&\ (\Sigma \subseteq \Psi)]$.

Nota. Observe-se que a definição de Θ não é decidível. Com efeito, é verdade que para qualquer A_n, ou A_n ou $\neg A_n$ deve ser consistente com Ψ_n. Porém, não há método que permita determinar qual dessas duas possibilidades é a certa em cada caso. No próximo capítulo, se poderá apreciar que o mesmo fenômeno se apresenta em outras circunstâncias relacionadas com um axioma de particular importância: o *axioma da escolha*.

A existência de Θ permite eliminar a condição de finitude de Σ na equivalência $Consist(\Sigma) \iff Sat(\Sigma)$ e generalizá-la a qualquer conjunto de fórmulas, estabelecendo uma íntima relação entre sintaxe e semântica.

Teorema 92. $Consist(\Sigma) \Longleftrightarrow Sat(\Sigma)$.

Prova. Da direita para a esquerda, já foi discutido acima.

No sentido contrário, a demonstração decorre por indução sobre fórmulas.

Primeiro consideramos uma extensão Θ, consistente e completa de Σ, da maneira feita acima.

Segundo, construímos uma valoração v que atribui valor 1 a todas as fórmulas de Θ e, portanto, às de Σ, como requerido.

Claramente, Θ contém todas as variáveis ou as suas negações. Definimos

$$v : Var \longrightarrow \{0,1\} \text{ por } \begin{cases} v(A) = 1 & \text{se } A\Theta \\ v(A) = 0 & \text{se } A \notin \Theta. \end{cases}$$

Estendemos v, da maneira canônica e para uma atribuição que também chamaremos v, para valores de todas as fórmulas de $\mathfrak{P}$. Para isso, definimos.

- Se $A = \neg B$, então $v(A) = v(B)^*$.
- Se $A = B \vee C$, então $v(A) = v(B) \triangledown v(C)$.

Afirmamos: Para todo o $A \in Flas$ tem-se

- Se $A \in \Theta$, então $v(A) = 1$.
- Se $A \notin \Theta$, então $v(A) = 0$.

Seja $A \in \Theta$.

1. Para $A \in Var$, a afirmação é certa por definição.

2a. Seja $A = \neg B$. Hipótese Indutiva:

- Se $B \in \Theta$, então $v(B) = 1$.
- Se $B \notin \Theta$, então $v(B) = 0$.

Como $A = \neg B \in \Theta$, pela completude de Θ tem-se $B \notin \Theta$. Pela Hipotese Indutiva $v(B) = 0$, donde, $v(A) = v(\neg B) = v(B)^* = 0^* = 1$.

2b. Seja $A = B \vee C$. Hipótese Indutiva:

- Se $B \in \Theta$, então $v(B) = 1$.
- Se $B \notin \Theta$, então $v(B) = 0$.
- Se $C \in \Theta$, então $v(C) = 1$.
- Se $C \notin \Theta$, então $v(C) = 0$.

Suponhamos que $v(A) = 0$, isto é, $v(B \vee C) = 0$. Ora, $v(B \vee C) = v(B) \nabla v(C) = 0$. Daqui, $v(B) = v(C) = 0$. Pela Hipótese Indutiva, $B \notin \Theta$ e $C \notin \Theta$. Pela completude de Θ, tem-se que $\neg B \in \Theta$ e $\neg C \in \Theta$. Também da completude de Θ, vem $\neg B \wedge \neg C \in \Theta$. Finalmente, $\neg(B \vee C) \in \Theta$, em contradição com $A = (B \vee C) \in \Theta$.

□

Validade. Para abreviar, escreveremos $Sat(v, A)$ para dizer que v *satisfaz* A, isto é, que $v(A) = 1$. Diremos que v satisfaz Σ, e o denotaremos por $Sat(v, \Sigma)$, se v satisfaz simultaneamente a todas as fórmulas de Σ. Aliás, diremos que uma fórmula A é *válida num conjunto de fórmulas* Σ se toda atribuição que satisfaz a todas as fórmulas de Σ satisfaz, também, A, o que é abreviado por $\Sigma \vDash A$. Em símbolos:

Definição 48.

1. $Sat(v, A) \iff v(A = 1)$.
2. $Sat(v, \Sigma) \iff \widehat{\forall} A \in \Sigma[v(A) = 1]$.
3. A *é válida em* $\Sigma \iff \forall v[\ Sat(v, \Sigma) \Longrightarrow Sat(v, A)]$.
4. $\Sigma \vDash A \iff A$ *é válida em* Σ.

Completude. Anteriormente, foi estabelecida a relação entre consistência e satisfatibilidade. Agora, nos ocuparemos em examinar a relação entre demonstrabilidade e satisfatibilidade. O Teorema B, da completude de $\mathfrak{P}$, diz que toda fórmula válida é demonstrável. Não podemos esperar que o mesmo aconteça com Σ, mas temos sim uma versão que leva a situação a outro nível. Antes, toda tautologia era demonstrável em $\mathfrak{P}$; agora, toda fórmula válida em Σ é demonstrável a partir de Σ.

Teorema 93 (da Completude). $\Sigma \vDash A \Longrightarrow \Sigma \vdash A$.

Prova. Suponhamos $\Sigma \vDash A$. Logo $\widehat{\neg} Sat(\Sigma \cup \neg A)$. Se $\Sigma \nvdash A$, tem-se $Consist(\Sigma \cup \{\neg A\})$. Portanto $Sat(\Sigma \cup \{\neg A\})$, contradizendo o dito na primeira linha desta prova. Concluímos: $\widehat{\neg}(\Sigma \nvdash A)$. □

Observação. Se no teorema anterior pusermos $\Sigma = \{\neg A \vee A\}$ ou, mais precisamente, $\Sigma = \{\neg A \vee A : A \in Flas(\mathfrak{P})\}$, então o teorema se reduz a $\mathfrak{P} \vDash A \Longrightarrow \mathfrak{P} \vdash A$, o que é o mesmo que o teorema B de completude de $\mathfrak{P}$ visto anteriormente. Isto parece ser um círculo vicioso, mas não o é, pois esta prova

do Teorema B repousa sobre a existência da extensão completa Θ e é, de fato, independente da anterior. É importante observar que esta prova, tal como a "construção" de Θ, não é decidível, enquanto que a prova anterior sim o é.

Compacidade. Um conjunto de fórmulas se diz *finitamente satisfatível* se todos os seus subconjuntos finitos são satisfatíveis. Semelhantemente, um conjunto de fórmulas se diz *finitamente consistente* se todos os seus subconjuntos finitos são consistentes. Usaremos $FinSat(\Sigma)$ e $FinCons(\Sigma)$, como abreviaturas de, respectivamente, Σ *é finitamente satisfazível* e Σ *é finitamente consistente*.

O teorema anterior permite demonstrar o *Teorema de Compacidade para o Cálculo Proposicional*: um conjunto finitamente satisfazível de fórmulas é satisfazível.

Teorema 94 (Compacidade do Cálculo Proposicional).

$$FinSat(\Sigma) \Longrightarrow Sat(\Sigma)].$$

Prova. Usando o teorema de completude para conjuntos de fórmulas proposicionais: $FinSat(\Sigma) \Longrightarrow FinConsist(\Sigma) \Longrightarrow Consist(\Sigma) \Longrightarrow Sat(\Sigma)$. □

O teorema seguinte é trivial, mas não está a mais registrá-lo. Diz que se todo subconjunto finito de Σ é consistente, então Σ é consistente. E reciprocamente.

Teorema 95 (Compacidade Sintática para o Cálculo Proposicional).

$$\left(\widehat{\forall}_{\Phi \subseteq_{fin} \Sigma}\ Consist(\Phi)\right) \Longleftrightarrow Consist(\Sigma).$$

Prova. Da direita para a esquerda é obvio. No outro sentido, suponhamos que $\widehat{\neg} Consist(\Sigma)$. Então

$$\exists \Phi \subseteq_{fin} \Sigma(\Phi \vdash C \wedge \neg C),$$

mas isto contradiz a consistência de todos os subconjuntos finitos de Σ. □

Aplicações do Cálculo Proposicional

Temos visto como o Cálculo Proposicional, sendo o sistema mais simples da lógica formal, ilustra e goza de importantes propriedades de interesse em qualquer sistema matemático, como consistência, completude, satisfatibilidade, etc. Aparte do seu valor lógico como ferramenta de raciocínio e análise de expressões, é parte da linguagem lógica como *língua franca* da matemática, o cálculo proposicional tem variadas aplicações; uma delas pode ser apreciada na prova das propriedades das operações básicos da teoria de conjuntos; quanto às outras, não podemos deixar de mencionar uma que é talvez a mais popular: a sua aplicação na descrição e representação de circuitos eléctricos. Devido ao fato de as

variáveis adotarem valores "0" ou "1", elas podem ser interpretadas como interruptores numa rede elétrica, governando a passagem ou interrupção da corrente elétrica. Por meio de conexões em série ou em paralelo é possível representar qualquer fórmula proposicional como uma rede eléctrica, como está indicado na figura 2.2 a seguir

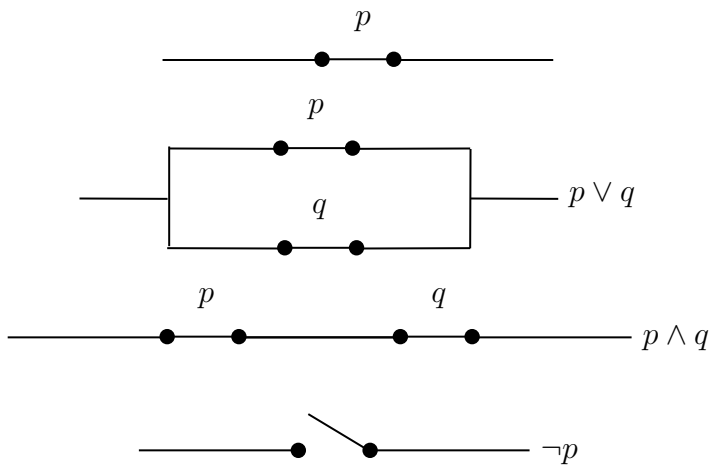


FIGURA 2.2. Representação de conectivos proposicionais por circuitos eléctricos

Uma conexão em série representa uma conjunção e uma conexão em paralelo representa uma disjunção; a negação requer algum dispositivo mecânico para inverter o efeito do interruptor. Como se pode ver em livros de computação, esta interpretação é implementada como dispositivos chamados *portas lógicas*, que são modelos físicos de certas fórmulas. As portas lógicas são expressões físicas das fórmulas $\neg A$, $A \wedge B$, $A \vee B$, $\neg(A \leftrightarrow B)$ e $A \leftrightarrow B$.

Limitações do Cálculo Proposicional. O Cálculo Proposicional constitui apenas uma parte reduzida da Lógica e está longe de representar todas as modalidades do raciocínio humano. Isto é devido a que a sua linguagem é projetada para falar apenas acerca da verdade ou a falsidade das sentenças, sem se ocupar da sua estrutura interna. Duas sentenças quaisquer são consideradas equivalentes se têm o mesmo valor de verdade, sem se importar com o que elas expressam. A lógica tem a ver com afirmações acerca do que acontece num universo e de como se deve raciocinar com estas afirmações. Uma afirmação, (fórmula), sempre diz algo (predica), acerca de algum individuo do universo (sujeito), ou acerca da totalidade de indivíduos, ou acerca da existência de algum ou alguns indivíduos.

Exemplos.

1. *2 é Par.*

2. *0 não é sucessor de nenhum número.*
3. *todo número tem um sucessor.*
4. *se x e y são impares, $x + y$ é par.*
5. O silogismo clássico "*Todos os homens são mortais, Sócrates é homem,* portanto *Sõcrates é mortal*".

Nenhuma destas expressões tem lugar em $\mathfrak{P}$. Em resumo, as proposições do Cálculo Proposicional são blocos sem estrutura interna; nele não há referência a indivíduos, às propriedades desses indivíduos, nem a sua universalidade ou existência. Tecnicamente, isso se reduz ao fato que não há expressões do tipo $P(x)$, $P(x, y)$, $\forall x P(x)$ e nem $\exists x P(x)$.

Esse tema será desenvolvido no capítulo sobre Lógica de Primeira Ordem, momento em que esses comentários serão aprofundados.

Índice

Bibliografia

[1] John Bell and Moshe Machover
A Course In Mathematical Logic,
North-Holland Publishing Company, Amsterdam, New York, Oxford, 1977

[2] C. Chang and H. Keisler.
Model theory.
Elsevier Publishers, 1973.

[3] Alonzo Church.
Introduction to Mathematical Logic.
Princeton University Press. 1956.

[4] H. B. Enderton.
A mathematical introduction to logic.
Academic Press. 1972.

[5] A. Fraenkel.
Abstract Set Theory.
North-Holland Publishing Company. Amsterdam-

[6] A. Fraenkel, Y. Bar-Hillel, A. Levy.
Foundations of Set Theory.
North-Holland Publishing Company. Amsterdam-London. 1973

[7] P. R. Halmos.
Naive Set Theory,
D. Van Nostrand Compaby, Inc., Toronto, New York, London, 1961.

[8] A.Hamilton. *Numbers, sets and axioms. The apparatus of mathematics.*
Cambridge university press, 1982.

[9] Wilfrid Hodges.
Model theory.
Cambridge University Press, 1993.

[10] Akihiro Kanamory.
The Mathematical Import of Zermelo's Well-Ordering Theorem.
The Bulletin of Symbolic Logic, Vol. 3. Nº 3. Sept. 1997.

[11] Seymour Lipschutz,
Schaum's Outline of Set Theory and Related Topics,
McGraw Hill 1998.

[12] María Manzano Arjona
Teoria de Modelos
Alianza Editorial. Madrid 1989

[13] E. Mendelson.

Introduction to mathematical logic.
D. Van Nostrand Company, Inc. Princeton, 1964.

[14] A.J. Franco de Oliveira.
Teoria de Conjuntos: Intuitiva e Axiomática,
Livrairia escolar Editora, 1982.

[15] Giusepe Peano
The principles of arithmetic presented by a new method.
Turin. 1889.

[16] Walter Rudin
Principles of Mathematical Analysis.
McGraw-Hill Book Company, Inc.. 1953.

[17] Michael Spivak.
Calculus.
Editorial Reverté, S. A. Barcelona. 1979.

[18] J. Shoenfield.
Mathematical logic.
Addison-Wesley Publishing Company, 1967.

[19] G.T. Kneebone.
Matematical Logic and the Foundations of Mathematics.
D. Van Nostrand Company Ltd.
358, Kensington High Street, London W14. 1963.

I.S.B.N. 978-65-02-02812-4