Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

Noções Básicas de Infinito e Números Cardinais[†]

por

Alessandro Mignac Carneiro Leão

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

fevereiro/2014
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

.

L436n Leão, Alessandro Mignac Carneiro.
Noções básicas de infinito e números cardinais / Alessandro Mignac Carneiro Leão.-- João Pessoa, 2014.
57p.
Orientador: Bruno Henrique Carvalho Ribeiro
Dissertação (Mestrado) - UFPB/CCEN
1. Matemática. 2. Cantor. 3. Teoria dos Conjuntos. 4.Números cardinais. 5. Números transfinitos. 6. Aritmética cardinal.

UFPB/BC CDU: 51(043)

Noções Básicas de Infinito e Números Cardinais

por

Alessandro Mignac Carneiro Leão

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada por:

Prof. Dr. Bruno Henrique Carvalho Ribeiro -UFPB (Orientador)

Prof. Dr. Joedson Silva dos Santos - UFPB

Prof. Dr. Marcelo Fernandes Furtado - UnB

fevereiro/2014

Agradecimentos

A *Deus* por estar sempre presente em minha vida e por permitir essa nova conquista nos meus estudos. À minha esposa *Michely Alves Carneiro Leão* e minha querida filha *Clarissa Mignac Carneiro Leão*, pelo amor, carinho e apoio incondicional. À coordenação e a todos os professores do PROFMAT. Aos membros da banca, ao meu orientador *Professor Doutor Bruno Henrique Carvalho Ribeiro*, pelo incentivo constante e pelas contribuições, sugestões e críticas que muito contribuíram para a elaboração deste trabalho.

Aos colegas da turma 2012 pelo companheirismo desde o início dessa jornada, em especial aos meus amigos e componentes do meu grupo de estudos, *Washington Gonçalves de Lima*, *Magnun César Nascimento dos Santos*, *André Soares Rodrigues* e *Cybele Verde Aragão de Almeida*. Aos familiares, em especial à minha mãe *Laurinete Mignac* e meu pai *Marcos Antonio Carneiro Leão* e amigos que sempre me incentivaram e apoiaram nessa jornada. Meu muito obrigado a todos.

Dedicatória

A minha amada, querida, doce e inesquecível avó Dorotea de Oliveira Mignac (in memorian) e ao meu maior exemplo de caráter e dignidade, meu avô Walter Mignac (in memorian), meus maiores e mais verdadeiros exemplos de vida. Vocês estarão para sempre vivos em minha mente e, principalmente, em meu coração. Que Deus os tenha para todo o sempre...

Resumo

Neste trabalho, mostramos um pouco a teoria sobre os chamados números transfinitos e sua aritmética cardinal. Para tanto, trabalhamos também alguns resultados envolvendo conjuntos, bem como equipotência, conjuntos finitos, infinitos, conjuntos enumeráveis e não-enumeráveis.

Palavras-chave: Cantor, Teoria dos Conjuntos, Números Cardinais, Números Transfinitos, Aritmética Cardinal

Abstract

In this work, we show basic results about the so-called transfinite numbers and their cardinal arithmetic. For these purpose, we also show some results involving the set theory, as well as equinumerosity, finite sets, infinite sets, countable sets and uncountable sets.

Keywords: Cantor, Set Theory, Cardinal Numbers, Transfinite Numbers, Cardinal Arithmetic.

Sumário

Introdução

Os gregos sempre evitaram lidar com o infinito, pois esse conceito lhes trazia dificuldades que eles nunca souberam resolver, e por isso eles nunca trataram os conjuntos infinitos. Nem eles nem seus sucessores das civilizações helenística, árabe e da Europa medieval. Foi só no século XIX que os matemáticos começaram a estudar conjuntos infinitos de maneira sistemática. E o primeiro a fazer isso foi *Bernhard Bolzano*(*1781-1848*), que nasceu, viveu e morreu em Praga. Era sacerdote católico que, além de se dedicar a estudos de Filosofia, Teologia e Matemática, tinha grandes preocupações com os problemas sociais de sua época. Seu ativismo em favor de reformas educacionais, sua condenação do militarismo e da guerra, sua defesa de liberdade de consciência e em favor da diminuição das desigualdades sociais custaram-lhe sérios embaraços com o governo. As ideias de Bolzano em Matemática não foram menos avançadas. É até admirável que, vivendo em relativo isolamento em Praga, afastado do principal centro científico da época, que era Paris, ele tenha tido sensibilidade para problemas de vanguarda no desenvolvimento da Matemática. Infelizmente, seus trabalhos permaneceram praticamente desconhecidos por várias décadas após a sua morte. **(ver [2])**

Figura 1: Bernhard Bolzano

Bolzano produziu vários trabalhos matemáticos importantes, mas aqui vamos nos limitar apenas a mencionar seu pioneirismo no tratamento de conjuntos infinitos.

Ele escreveu um livro sobre os paradoxos do infinito, publicado postumamente em 1859, no qual aborda várias questões de natureza filosófica e matemática acerca dos conjuntos infinitos. Depois de Bolzano, devemos mencionar *Richard Dedekind* (*1831-1916*), um grande nome da Matemática do século XIX. Ele foi mais longe que Bolzano, utilizando a noção de conjunto na construção dos números reais.

Figura 2: Richard Dedekind

Mas foi *Georg Cantor* (*1845-1918*) quem mais avançou no estudo dos conjuntos. No capítulo 1 deste nosso trabalho, apresentamos resultados os quais julgamos preliminares envolvendo a teoria dos conjuntos que serão muito úteis nos capítulos subsequentes.

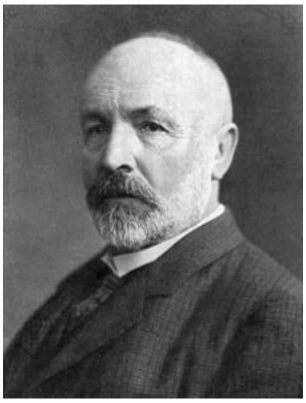

Figura 3: Georg Cantor

Em 1872 Cantor estava iniciando sua carreira profissional e se ocupava do estudo da representação das funções por meio de séries trigonométricas. Nessa ocupação ele foi levado a investigar os conjuntos de pontos de descontinuidade de tais funções, os mais simples dos quais são os conjuntos com apenas um número finito de pontos.

Mas o aparecimento de conjuntos cada vez mais complicados acabou levando Cantor a investigar conjuntos infinitos em sua generalidade. Nesse estudo ele introduziu um conceito simples, que logo se revelaria da maior importância, qual seja, o conceito de *equipotência de conjuntos*, que será abordado no capítulo 2 deste nosso trabalho.

No caso de conjuntos finitos, serem equipotentes corresponde a terem o mesmo número de elementos. E no caso dos conjuntos infinitos? Bem, nesse caso não faz sentido falar em *número de elementos do conjunto*, pois tais conjuntos sempre tem infinitos elementos. Mas como o conceito de cardinalidade é válido tanto para conjuntos finitos como para conjuntos infinitos, e como tal conceito corresponde exatamente ao conceito de número de elementos no caso de conjuntos finitos, é esse conceito que estende, para conjuntos infinitos, a noção de *número de elementos do conjunto*.

Assim, de um modo geral, diz-se que dois conjuntos quaisquer A e B são equipotentes se eles tiverem a mesma *cardinalidade*. A cardinalidade de um conjunto corresponde ao número de elementos que este conjunto possui. Essa definição, no caso dos conjuntos finitos, não traz nada de novo. Mas, como veremos, estende, para conjuntos infinitos, a noção de *número de elementos de um conjunto*. Tais números são os chamados *números transfinitos*, o qual abordaremos no capítulo 3 deste trabalho.

Chama-se *conjunto enumerável* todo conjunto equipotente a $\mathbb{N}$. Assim, o conjunto dos números pares positivos é enumerável, pois, como mostraremos no capítulo 2, ele é equipotente a $\mathbb{N}$. Não deixa de ser supreendente, para quem adquire esse conhecimento pela primeira vez, constatar que existem subconjuntos próprios de $\mathbb{N}$ que são equipotentes a $\mathbb{N}$. Não apenas o conjunto dos pares positivos, mas também o conjunto dos números ímpares, o conjunto dos quadrados dos inteiros $\{1, 4, 9, 16, 25, 36, ...\}$ e muitos outros mais, todos equipotentes a $\mathbb{N}$. Esse fenômeno é uma peculiaridade dos conjuntos infinitos e pode ser usado para caracterizar tais conjuntos.

Será que todos os conjuntos infinitos são enumeráveis? Ou seja, equipotentes a $\mathbb{N}$? Veremos que não é assim. Estabeleceremos, no capítulo 2, a enumerabilidade dos números racionais, um resultado já em si surpreendente. Verificaremos no capítulo 2 deste trabalho, que o conjunto dos números reais $\mathbb{R}$ é não enumerável. E, diante deste resultado, Cantor mostrou que existem *pelo menos* dois tipos de infinito: o conjunto dos números naturais e o conjunto dos números reais.

No tocante aos números cardinais, que será abordado no capítulo 2, temos que a utilização da noção de função bijetiva entre conjuntos é a abordagem adequada para comparar o *tamanho* de dois conjuntos. Esta abordagem também foi introduzida por Cantor e, surpreendentemente, conduz a existência de diferentes tamanhos de infinitos. Motivamos este trabalho levantando as seguintes questões: Que conjunto seria *maior*, o conjunto $\mathbb{N}$ dos números naturais, ou o conjunto $\mathbb{Q}$ dos números racionais? O que se pode dizer quanto ao conjunto dos números reais e o intervalo

$(0, 1)$? Os reais seriam *maiores* do que o intervalo $(0, 1)$? O conjunto $\mathbb{Z}$ dos números inteiros é infinito e o conjunto dos números reais também, mas, há alguma relação entre eles com respeito à quantidade de elementos?

Cantor provou outro fato não menos pertubador: Dado um conjunto qualquer, é sempre possível construir outro conjunto maior ainda, maior no sentido de que ele contém o primeiro conjunto como parte própria e não é equipotente a essa sua parte própria. Sendo assim, esses dois conjuntos têm cardinalidades diferentes. Isso permite ordenar as cardinalidades dos conjuntos criando o que chamamos de *números transfinitos*. Um tal número nada mais é que a cardinalidade de um conjunto. Abordaremos esse assunto no capítulo 3 deste trabalho.

Ainda, no capítulo 3, destacamos a chamada *Aritmética Cardinal*. Já existe uma aritmética cardinal para os números cardinais finitos. Por exemplo, se x e y são dois números cardinais finitos, temos que a soma $x+y$ e o produto xy tem seus significados tradicionais. Neste capítulo, além de abordar a aritmética dos cardinais finitos, generalizamos estes conceitos de modo a cobrir os números cardinais transfinitos também. Ou seja, uma aritmética que se aplica a todos os números cardinais, finitos e infinitos, que preserve os significados e propriedades tradicionais da aritmética dos números cardinais finitos.

No apêndice deste trabalho, apresentamos, de uma forma breve, a *Hipótese do Contínuo*. A hipótese do contínuo é uma conjectura proposta por Georg Cantor. Esta conjectura consiste no seguinte:

Não existe nenhum conjunto com mais elementos do que o conjunto dos números inteiros e menos elementos do que o conjunto dos números reais.

Aqui mais elementos e menos elementos tem um sentido muito preciso. Esta hipótese foi o número um dos *23 Problemas de Hilbert* apresentados na conferência do Congresso Internacional de Matemática de 1900, o que levou a que fosse estudada profundamente durante o século XX.

Capítulo 1

Resultados Preliminares de Teoria dos Conjuntos

A Teoria dos Conjuntos foi desenvolvida de forma rigorosa e moderna no final o século dezenove por *Georg Cantor* (*1845-1918*) para abordar certas questões sutis da teoria das funções. As ideias revolucionárias de Cantor, de início incompreendidas por serem demasiado abstratas para a época, foram rapidamente se impondo como elemento unificador de vários ramos da matemática, a ponto de se tornarem o meio pelo qual é formalizada toda a matemática contemporânea.

A teoria contribuiu decisivamente para que se passasse a encarar sob outra perspectiva os problemas da matemática, desde os que surgem nos fundamentos da disciplina até os que são típicos de ramos especializados da álgebra, da análise e da geometria.

As aplicações da teoria dos conjuntos à solução de questões relativas à estrutura algébrica de vários tipos de conjuntos e a questões relativas às suas propriedades operatórias abriram novos rumos para os matemáticos, ressaltando, entre outras aplicações, a extensão dos conceitos de medida e de integral, a introdução das noções de espaço abstrato, definido como conjuntos de elementos com dadas propriedades, e bem assim notáveis inovações no campo da integração e no do estudo das funções, examinadas à luz da correspondência entre conjuntos.

Neste primeiro capítulo deste trabalho, procuramos apresentar, de uma maneira clara e objetiva, alguns resultados que julgamos importantes da teoria dos conjuntos, em alguns momentos sem o rigor matemático apropriado, com o objetivo de fazer com que o leitor venha a compreender, além destes resultados preliminares, outros importantes conceitos para que, finalmente, venhamos a abordar as chamadas *Noções Básicas de Infinito e Números Cardinais.*

1.1 A Linguagem dos Conjuntos

Esta seção foi elaborada a partir das seguintes referências bibliográficas: [1], [3], [7], [11].

Os termos *conjunto* e *elemento* e a relação de um elemento pertencer a um conjunto são conceitos primitivos; ou seja, não serão definidos. Usamos o termo *coleção* como sinônimo de conjunto. A afirmação que um elemento x pertence ao conjunto A é simbolizada por $x \in A$ e a sua negação é simbolizada por $x \notin A$.

Definição 1.1.1 *Dois conjuntos são considerados iguais, se eles têm os mesmos elementos. Mais precisamente, temos que $A = B$ se, e somente se, todo elemento de A é elemento de B e todo elemento de B é elemento de A.*

A condição de que todo elemento de um conjunto A pertence a um conjunto B, estabelece uma relação entre A e B, chamada *relação de inclusão*. Quando existir uma tal relação entre A e B escreveremos $A \subset B$ ou $B \supset A$, que se lê A está contido em B ou A é subconjunto de B, ou ainda, B contém A.

Proposição 1.1.1 *A relação de inclusão possui as seguintes propriedades:*

(1) $A \subset A$, para todo conjunto A;

(2) $A = B$ se, e somente se, $A \subset B$ e $B \subset A$;

(3) Se $A \subset B$ e $B \subset C$, então $A \subset C$.

A negação de $A \subset B$, ou seja, o fato de A não ser subconjunto de B, é simbolizada por $A \not\subset B$ e significa que existe pelo menos um elemento de A que não pertence a B. Se $A \subset B$ e $A \neq B$, diremos que A é *subconjunto próprio* de B. Neste caso, escrevemos $A \subsetneqq B$. No que se segue, admitiremos o leitor familiarizado com o conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, 4 \cdots\}$ e com o conjunto dos números inteiros: $\mathbb{Z} = \{\cdots - 3, -2, -1, 0, 1, 2, 3, \cdots\}$.

O conjunto $\mathbb{Q}$, dos números racionais, é formado pelas frações $\frac{p}{q}$, onde p e q pertencem a $\mathbb{Z}$, sendo $q \neq 0$. Em símbolos, temos que

$$\mathbb{Q} = \{p/q; p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}.$$

Lê-se: "$\mathbb{Q}$ é o conjunto das frações p/q tais que p pertence a $\mathbb{Z}$, q pertence a $\mathbb{Z}$ e q é diferente de zero".

A maioria dos conjuntos encontrados em matemática não são definidos especificando-se, um a um, os seus elementos. O método mais frequente de definir um conjunto é por meio de uma propriedade comum e exclusiva dos seus elementos. Mais precisamente, parte-se de uma propriedade P. Ela define um conjunto X, assim: se um elemento x goza da propriedade P, então $x \in X$; se não goza de P, então $x \notin X$. Escreve-se

$$X = \{x; \text{ goza da propriedade } P\}.$$

Lê-se: "X é o conjunto dos elementos x tais que x goza da propriedade P".

Muitas vezes a propriedade P se refere a elementos de um conjunto fundamental A. Neste caso, escreve-se

$$X = \{x \in A; x \text{ goza da propriedade } P\}.$$

Por exemplo, seja $\mathbb{N}$ o conjunto dos números naturais e consideremos a seguinte propriedade, que se refere a um elemento genérico $x \in \mathbb{N}$:

"x é maior do que 5".

A propriedade P, de um número natural ser maior do que 5, define o conjunto $X = \{6, 7, 8, 9 \cdots\}$, ou seja,

$$X = \{x \in \mathbb{N}; x > 5\}.$$

Lê-se: "X é o conjunto dos x pertencentes a $\mathbb{N}$ tais que x é maior do que 5".

Às vezes, ocorre que nenhum elemento de A goza da propriedade P. Neste caso, o conjunto $\{x \in A; \ x \text{ goza de } P\}$ não possui elemento algum. Isto é o que se chama um conjunto vazio. Para representá-lo, usaremos o símbolo $\emptyset$.

Portanto, o conjunto vazio é definido assim: Qualquer que seja x, tem-se $x \notin \emptyset$.

Alguns exemplos:

- $\{x \in A; x \neq x\} = \emptyset$;
- $\{x \in \mathbb{N}; 1 < x < 2\} = \emptyset$;
- $\{x; x \neq x\} = \emptyset$.

Definição 1.1.2 *Afirmamos que $\emptyset \subset A$, para qualquer que seja o conjunto A.*

Esta afirmação parece estranha à primeira vista, mas vejamos como é natural a falsidade de sua negação (isto é, sua veracidade). A afirmação $\emptyset \not\subset A$, para algum conjunto A, significa que existe pelo menos um $x \in \emptyset$ tal que $x \notin A$ e isto é claramente falso, visto que o conjunto $\emptyset$ não possui qualquer elemento.

1.1.1 Operações com Conjuntos

Dada uma coleção qualquer de conjuntos, admitiremos a existência de um conjunto tal que cada um de seus elementos pertence a pelo menos um dos conjuntos da coleção. Tal conjunto será chamado de *união* dos conjuntos da coleção.

Definição 1.1.3 *Dados dois conjuntos* A *e* B*, a união de* A *e* B *é o conjunto* $A \cup B = \{x; x \in A \text{ ou } x \in B\}$.

As propriedades a seguir decorrem imediatamente das definições.

Proposição 1.1.2 *Para todos os conjuntos* A*,* B *e* C*, temos que:*

(1) $A \cup \emptyset = A$ *e* $A \cup A = A$*;*

(2) $A \subset A \cup B$ *e* $B \subset A \cup B$*;*

(3) $A \cup B = B \cup A$*;*

(4) $(A \cup B) \cup C = A \cup (B \cup C)$.

Proposição 1.1.3 *Dados conjuntos* A, A', B *e* B'*, com* $A \subset B$ *e* $A' \subset B'$*, então* $A \cup A' \subset B \cup B'$.

Prova. Se $A \cup A' = \emptyset$, a asserção é verdadeira. Suponha que $A \cup A' \neq \emptyset$. Se $x \in A \cup A'$, temos que $x \in A$ ou $x \in A'$, e como $A \subset B$ e $A' \subset B'$, segue-se que $x \in B$ ou $x \in B'$. Isto posto, $x \in B \cup B'$. Portanto, provamos que $A \cup A' \subset B \cup B'$.
■

Corolário 1.1.1 $A \cup B = A$ *se, e somente se,* $B \subset A$.

Prova. Suponhamos que $A \cup B = A$. Como $B \subset A \cup B$, segue-se que $B \subset A$. Reciprocamente, suponha que $B \subset A$. Como $A \subset A$, segue-se da proposição que $A \cup B \subset A \cup A = A$. Logo, $A \cup B \subset A$. Como $A \subset A \cup B$, segue-se que $A \cup B = A$.
■

Definição 1.1.4 *Dados dois conjuntos* A *e* B*, a interseção de* A *e* B *é o conjunto* $A \cap B = \{x; x \in A \text{ e } x \in B\}$*. Quando* $A \cap B = \emptyset$*, dizemos que os conjuntos* A *e* B *são disjuntos.*

As propriedades a seguir decorrem das definições:

Proposição 1.1.4 *Para todos os conjuntos* A, B *e* C*, temos que:*

(1) $A \cap B = \emptyset$ *e* $A \cap A = A$*;*

(2) $A \cap B$ *e* $A \cap B \subset B$*;*

(3) $A \cap B = B \cap A$*;*

(4) $(A \cap B) \cap C = A \cap (B \cap C)$*.*

Proposição 1.1.5 *Dados conjuntos* A, B *e* C *quaisquer, temos que* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$*.*

Prova. Inicialmente, provemos a inclusão $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Se $A \cap (B \cup C) = \emptyset$, nada temos a provar. Suponha que $A \cap (B \cup C) \neq \emptyset$. Seja x um elemento qualquer de $A \cap (B \cup C)$. Logo, temos que $x \in A$ e $x \in B \cup C$. Seja $x \in B$, então $x \in A \cap B$. Se $x \in C$, então $x \in A \cap C$. Em qualquer caso, temos que $x \in (A \cap B) \cup (A \cap C)$. Agora, provemos a inclusão $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Se o conjunto da esquerda for vazio, a inclusão é verificada. Suponha que tal conjunto é não vazio, e seja x um elemento qualquer dele. Logo, $x \in A \cap B$ ou $x \in A \cap C$. Em qualquer caso, $x \in A$ e temos que $x \in B$ ou $x \in C$. Isto posto, $x \in A \cap (B \cup C)$.
■

Proposição 1.1.6 *Dados conjuntos* A*,* B *e* C*, quaisquer, temos que* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$*.*

Definição 1.1.5 *Dados dois conjuntos* A *e* B*, a diferença* A *menos* B*, é o conjunto* $A - B = \{x; x \in A \text{ e } x \notin B\}$*. Quando* $B \subset A$*, a diferença* $A - B$ *é denotada por* $\complement_A(B)$ *e é chamada de complementar de* B *em* A*.*

Por exemplo, se $A = \{a, b, c\}$ e $B = \{b, c, d\}$, então $A - B = \{a\}$.

Proposição 1.1.7 *Para todos os conjuntos* A *e* B*, temos que:*

(1) $A - \emptyset = A$ *e* $A - A = \emptyset$*;*

(2) Se $A \cap B = \emptyset$*, então* $A - B = A$ *e* $B - A = B$*;*

(3) $\complement_A(\emptyset) = A$ *e* $\complement_A(A) = \emptyset$*.*

Proposição 1.1.8 *Sejam* B *e* B' *subconjuntos de* A*. Se* $B \subset B'$*, então* $\complement_A(B') \subset \complement_A(B)$*.*

Prova. Suponha que $B \subset B'$. Se $\complement_A(B') = \emptyset$, nada temos a provar. Se $\complement_A(B') \neq \emptyset$ e seja x um elemento qualquer de $\complement_A(B')$. Isto posto, $x \notin B'$. Segue-se que $x \notin B$ pois, caso contrário, como $B \subset B'$, teríamos $x \in B'$. Consequentemente, $x \in \complement_A(B)$.
■

Proposição 1.1.9 *Sejam B e B' subconjuntos de A. Temos que $\complement_A(B \cup B') = \complement_A(B) \cap \complement_A(B')$.*

Prova. A proposição decorre da seguinte cadeia de equivalências:

$$x \in \complement_A(B \cup B') \Leftrightarrow x \notin B \cup B' \Leftrightarrow x \notin B \text{ e } x \notin B' \Leftrightarrow x \in \complement_A(B) \cap \complement_A(B'),$$

para todo elemento x de A. ■

Proposição 1.1.10 *Sejam B e B' subconjuntos de A. Temos que $\complement_A(B \cap B') = \complement_A(B) \cup \complement_A(B')$.*

1.1.2 Conjunto de Partes e Produto Cartesiano

Definição 1.1.6 *Dado um conjunto A qualquer, admitiremos a existência de um conjunto $\wp(A)$, cujos elementos são todos subconjuntos de A, chamado conjunto das partes ou conjunto potência de A.*

Definição 1.1.7 *Um par ordenado (a, b) de elementos de A é o elemento de $\wp(\wp(A))$ dado por $\{\{a\}, \{a, b\}\}$. Não é difícil convencer-se que $(a, b) = (a', b')$ se, e somente se, $a = a'$ e $b = b'$.*

Definição 1.1.8 *Dados dois conjuntos A e B, o produto cartesiano de A e B é o conjunto $A \times B$ de todos os pares ordenados (a, b) de elementos de $A \cup B$ tais que $a \in A$ e $b \in B$. Simbolicamente, escrevemos $A \times B = \{(a, b); a \in A \text{ e } b \in B\}$.*

Por exemplo, se $A = \{a, b\}$ e $B = \{c, d\}$, temos que $A \times B = \{(a, c), (a, d), (b, c), (b, d)\}$ e $B \times A = \{(c, a), (c, b), (d, a), (d, b)\}$.

Note que, em geral, $A \times B \neq B \times A$. Temos também que $A \times B = \emptyset$ se, e somente se, $A = \emptyset$ ou $B = \emptyset$.

1.1.3 Família de Conjuntos

Definição 1.1.9 *Seja I um conjunto não vazio qualquer. Uma família indexada por I é uma coleção de conjuntos A_i com $i \in I$. Uma tal família será denotada por $(A_i)_{i \in I}$.*

Definição 1.1.10 *A união dos elementos de uma família é $\bigcup_{i \in I} A_i = \{x; x \in A_i$ para algum $i \in I\}$ e a sua interseção é $\bigcap_{i \in I} A_i = \{x; x \in A_i$ para todo $i \in I\}$.*

De fato, para todo $j \in I$, temos que $A_j \subset \bigcup_{i \in I} A_i$ e $\bigcap_{i \in I} A_i \subset A_j$.

1.2 Funções

Esta seção foi elaborada a partir das seguintes referências bibliográficas: [3], [11], [12].

Definição 1.2.1 *Dados dois conjuntos não vazios X e Y, uma* ***relação*** *de X em Y (ou entre X e Y, nessa ordem), é um subconjunto R do produto cartesiano $X \times Y$, isto é, R é um conjunto de pares ordenados do tipo (x, y), com $x \in X$ e $y \in Y$. Se R é uma relação de X em X, diremos simplesmente que R é uma relação em X.*

No exemplo que se segue, dados $X = \{1, 2, 3\}$ e $Y = \{2, 3, 4, 5\}$, o conjunto $R = \{(x, y) \in X \times Y; x \geq y\}$ é a relação de X em Y dada por $R = \{(2, 2), (3, 2), (3, 3)\}$; de fato, esses são os únicos pares ordenados (x, y) com $x \in \{1, 2, 3\}, y \in \{2, 3, 4, 5\}$ e tais que $x \geq y$. Se R é uma relação de X em Y, então $R \subset X \times Y$ por definição.

Reciprocamente, escolhido um par ordenado $(x, y) \in X \times Y$, pode ocorrer que $(x, y) \in R$ ou $(x, y) \notin R$ (isto é, que x e y sejam relacionados ou não por R). No primeiro caso, vamos denotar por xRy. Temos que: $xRy \Leftrightarrow (x, y) \in R$.

Definição 1.2.2 *Uma relação binária em um conjunto $X \neq \emptyset$ é uma sentença aberta xRy no conjunto $X \times X$.*

São exemplos de relações binárias a igualdade $x = y$ entre elementos de um conjunto X e a relação de desigualdade $x \leq y$ em $\mathbb{Z}$.

Proposição 1.2.1 *Uma relação binária xRy em um conjunto $X \neq \emptyset$ será chamada relação de equivalência, se possuir as seguintes propriedades:*

*(i) xRx é verdadeira para todo $x \in X$ (**Propriedade Reflexiva**);*

*(ii) Se xRy é verdadeira, então yRx é verdadeira (**Propriedade Simétrica**);*

*(iii) Se xRy e yRz são verdadeiras, então xRz é verdadeira (**Propriedade Transitiva**).*

Definição 1.2.3 *Dada uma relação de equivalência $\equiv$ em um conjunto X, definimos a classe de equivalência de um elemento $a \in X$ como sendo o conjunto $[a] = \{x \in X; x \equiv a\}$ e o elemento a será chamado de representante da classe $[a]$.*

Por exemplo, se a relação de equivalência é a igualdade entre os elementos de um conjunto X, temos que $[a] = \{a\}$, para todo $a \in X$.

Definição 1.2.4 *Sejam dados dois conjuntos não vazios X e Y. Uma função f de X em Y é uma regra que associa a cada $x \in X$ um único $y \in Y$. Os conjuntos X e Y são chamados respectivamente de domínio e contradomínio da função. Denominaremos $X = D(f), Y = CD(f)$ e $f(X)$ como sendo a imagem da função f. Temos que $f(X) \subset Y$.*

As três definições a seguir explicitam alguns tipos extremamente úteis de funções.

Definição 1.2.5 *Dados conjuntos não vazios X e Y, e fixado um elemento $c \in Y$, a função constante c de X em Y é a função $f : X \to Y$ tal que $f(x) = c$ para todo $x \in X$.*

No caso extremo da função constante e igual a c, definida acima, todo $x \in X$ está associado a um mesmo $y \in Y$, a saber, $y = c$. Contudo, as condições impostas na definição são plenamente satisfeitas, isto é, todo $x \in X$ está associado a um *único* $y \in Y$.

Definição 1.2.6 *Dado um conjunto não vazio X, a* ***função identidade*** *de X, denotada por $Id_X : X \to X$, é a função dada por $Id(x) = x$ para todo $x \in X$.*

Definição 1.2.7 *Duas funções $f : X \to Y$ e $g : W \to Z$ são* ***iguais*** *se $X = W, Y = Z$ e $f(x) = g(x)$ para todo $x \in X$.*

Se duas funções $f : X \to Y$ e $g : W \to Z$ forem iguais, escrevemos $f = g$. A definição acima significa a igualdade dos domínios, $X = W$, e dos contradomínios, $Y = Z$, assim como a validade da função $f(x) = g(x)$ para todo $x \in X$. Se funções f e g não forem iguais, escrevemos $f \neq g$ e diremos que f e g são funções *diferentes* ou *distintas*.

1.2.1 Composição de Funções

Dadas duas funções $f : X \to Y$ e $g : Y \to Z$, temos, em última análise, regras bem definidas partindo de $x \in X$ via f, obter $y = f(x) \in Y$ e, via g, obter $g(z) \in Z$. Parece muito razoável que possamos formar uma função que nos permita sair de X diretamente para Z. Este é de fato o caso, e a função resultante é denominada a função *composta* de f e g, de acordo com o seguinte:

Definição 1.2.8 *Dadas as funções $f : X \to Y$ e $g : Y \to Z$, a* ***função composta*** *de f e g, nessa ordem, é a função $g \circ f : X \to Z$ definida, para cada $x \in X$, por $(g \circ f)(x) = g(f(x))$. De uma forma geral, basta que tenhamos $f(X) \subset Y$ para que a função $g \circ f$ faça sentido.*

Apesar de não ser comutativa, a operação de composição de funções é associativa, conforme segue:

Proposição 1.2.2 *Dadas funções $f : X \to Y$, $g : Y \to Z$ e $h : Z \to W$, temos que $h \circ (g \circ f) = (h \circ g) \circ f$.*

Prova. Veja primeiro que as ambas $h \circ (g \circ f)$ e $(h \circ g) \circ f$ são funções de X em W. Portanto, para serem iguais, é suficiente que associem cada $x \in A$ em um mesmo elemento de W. Para ver isto, basta notar que $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h((g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. ■

A proposição acima é muito importante pois, se tivermos funções f, g e h e pudermos compô-las (nessa ordem), podemos denotar a função composta por $h \circ g \circ f$ simplesmente, não nos preocupando com qual composição efetuar primeiro.

Definição 1.2.9 *Uma função $f : X \to Y$ é dita:*

(a) ***Injetora**, **injetiva** ou ainda uma **injeção**, se para quaisquer $x_1, x_2 \in X$ tais que $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$;*

(b) ***Sobrejetora**, **sobrejetiva** ou ainda uma **sobrejeção**, se sua imagem for todo o conjunto Y, isto é, $f(X) = Y$;*

(c) ***Bijetora**, **bijetiva** ou ainda uma **bijeção** se for ao mesmo tempo injetiva e sobrejetiva.*

Teorema 1.2.1 *Se $X \subset \mathbb{R}$ é um conjunto não vazio e $f : X \to X$ é uma função tal que $f(f(x)) = x$ para todo x, então f é bijetiva.*

Prova. Sejam x_1 e x_2 números reais tais que $f(x_1) = f(x_2)$. Para mostrarmos que f é injetiva é suficiente provar que $x_1 = x_2$. Para tanto, observe que $f(x_1) = f(x_2) \Rightarrow f(f(x_1)) = f(f(x_2))$. Logo, $x_1 = x_2$ por hipótese. A sobrejetividade de f é imediata. Fixado $y \in X$ e tomando $f(y) \in X$, temos $f(f(y)) = y$. Isto posto, concluímos que $y \in f(X)$. ■

A proposição a seguir ensina como se comportam funções injetivas, sobrejetivas e bijetivas em relação à composição.

Proposição 1.2.3 *Sejam $f : X \to Y$ e $g : Y \to Z$ duas funções dadas. Então:*

(a) $g \circ f$ injetiva $\Rightarrow f$ injetiva, mas a recíproca nem sempre é verdadeira.

(b) $g \circ f$ sobrejetiva $\Rightarrow g$ sobrejetiva, mas a recíproca nem sempre é verdadeira.

(c) g, f injetivas $\Rightarrow g \circ f$ injetiva.

(d) g, f sobrejetivas $\Rightarrow g \circ f$ sobrejetiva.

(e) g, f bijetivas $\Rightarrow g \circ f$ bijetiva.

Prova.
(a) Para x_1 e x_2 em X, temos que $f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow x_1 = x_2$, onde na última passagem usamos o fato de $g \circ f$ ser injetiva. Temos agora que dar um exemplo no qual f seja injetiva mas $g \circ f$ não o seja. Para tanto, basta tomarmos $X = Y = Z = \mathbb{R}$, $f(x) = x$ e $g(x) = x^2$.

(b) Dado arbitrariamente $z \in Z$, a sobrejetividade de $g \circ f$ garante a existência de pelo menos um $x \in X$ tal que $z = (g \circ f)(x)$. Mas aí, $z = g(f(x))$ e g também é sobrejetiva. Para o exemplo necessário à segunda parte, tomemos novamente $X = Y = Z = \mathbb{R}, g(x) = x$ e $f(x) = x^2$.

(c) Usando sucessivamente as injetividades de g e de f, temos para x_1 e x_2 em X que $(g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, e $g \circ f$ também é injetiva.

(d) Dado arbitrariamente $z \in Z$, a sobrejetividade de g garante a existência de $y \in Y$ tal que $z = g(y)$. Por outro lado, a sobrejetividade de f assegura a existência de $x \in X$ tal que $f(x) = y$. Então, temos que $(g \circ f)(x) = g(f(x)) = g(y) = z$, donde $g \circ f$ também é sobrejetiva.

(e) Segue dos itens (c) e (d) que g e f bijetoras $\Rightarrow g$ e f são injetivas e sobrejetivas $\Rightarrow g \circ f$ injetiva e sobrejetiva $\Rightarrow g \circ f$ bijetiva. ■

1.2.2 Inversão de Funções

Consideremos uma função $f : X \to Y$ bijetiva. Temos que os elementos de X e Y estão em *correspondência biunívoca*, ou seja, a cada elemento de X corresponde um e só um elemento de Y via f, e vice-versa. Quando tal ocorrer, podemos obter uma outra função $g : Y \to X$, simplesmente exigindo que $f(x) = y \Leftrightarrow g(y) = x$.

Definição 1.2.10 *Diremos que uma função $g : Y \to X$ é uma inversa à esquerda de f se $g \circ f = Id_X$ e g é uma inversa à direita de f se $f \circ g = Id_Y$.*

Uma pergunta natural a esta altura é por que não podemos usar a declaração acima para definir a inversa de uma função bijetiva. De um ponto de vista intuitivo, se f não fosse sobrejetiva, existiria um elemento y de Y que não seria imagem por

f de nenhum elemento de X. Assim, não teríamos uma maneira natural de definir $g(y)$ a partir de f. Por outro lado, se f não fosse injetiva, existiriam elementos distintos x_1 e x_2 em X com uma mesma imagem $y \in Y$ via f. Quando tentássemos definir g por meio de f, também não haveria maneira natural de decidirmos quem, dentre x_1 e x_2, deveria ser igual a $g(y)$.

Voltando ao caso em que f é bijetiva, não é difícil ver que g, definida como acima, é de fato uma função, e ademais tal que $(g \circ f)(x) = x$ para todo $x \in X$ e $(f \circ g)(y) = y$ para todo $y \in Y$. De outro modo, temos $g \circ f = Id_X$ e $f \circ g = Id_Y$. Reciprocamente, se $f : X \to Y$ e $g : Y \to X$ são funções tais que $g \circ f = Id_X$ e $f \circ g = Id_Y$, então f deve ser, de fato uma bijeção, e g é a única função que satisfaz tais igualdades de composição.

Definição 1.2.11 *Seja $f : X \to Y$ uma bijeção dada. A **função inversa** de f é a função $g : Y \to X$ tal que, para $x \in X, y \in Y$, temos que $g(y) = x \Leftrightarrow y = f(x)$.*

Daqui em diante, denotaremos a inversa de uma bijeção $f : X \to Y$ por $f^{-1} : Y \to X$. Observe que o expoente -1 na notação da função inversa não tem nenhum significado aritmético. Ele simplesmente chama atenção para o fato de que f^{-1} faz o *caminho inverso* de f, isto é, aplica Y em X em vez de X em Y, revertendo as setas das associações feitas por f.

Proposição 1.2.4 *Uma função é sobrejetiva se, e somente se, ela admite inversa à direita.*

Prova. Seja $f : X \to Y$ uma função sobrejetiva. Então, para cada $y \in Y$ é possível escolher pelo menos um $x \in X$ tal que $y = f(x)$. Fixe um tal x para cada y. Defina $g : Y \to X$ tal que $g(y) = x$ (note que em geral toda função g não é unicamente determinada, ela o será se f é injetiva). Segue-se então que, para todo $y \in Y$, $f \circ g(y) = f(g(y)) = f(x) = y$. Isto posto, $f \circ g = Id_Y$ e, portanto, g é uma inversa à direita de f. Reciprocamente, suponha que $f \circ g = Id_Y$ para alguma função $g : Y \to X$. Como Id_Y é sobrejetiva, segue-se que f é também sobrejetiva. ■

Proposição 1.2.5 *Uma função é injetiva se, e somente se, ela admite uma inversa à esquerda.*

Prova. Seja $f : X \to Y$ uma função injetiva. Então, cada $y \in f(X)$ determina um único $x \in X$ tal que $y = f(x)$. Defina $g : Y \to X$ como a seguir:

$$g(y) = \begin{cases} x, & \text{se} \quad y \in f(X) \\ a, & \text{se} \quad y \notin f(X) \end{cases}$$

onde a é um elemento qualquer fixado de X. Note que em geral g não é unicamente determinada, ela o será se f for sobrejetiva. Segue-se então que $g \circ f(x) = g(f(x)) =$

$g(y) = x$, para todo $x \in X$. Isto posto, $g \circ f = Id_X$ e, portanto, g é uma inversa à esquerda de f. Suponha reciprocamente que existe $g : Y \to X$ tal que $g \circ f = Id_X$. Como Id_X é injetiva, segue-se que f é injetiva. ■

Proposição 1.2.6 *Se uma função admite uma inversa à esquerda e uma inversa à direita, então estas são iguais.*

Prova. Sejam $g_1, g_2 : Y \to X$, respectivamente, uma inversa à direita e uma inversa à esquerda de uma função $f : X \to Y$. Segue-se que $g_1 = Id_X \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ Id_Y = g_2$. ■

Lema 1.2.1 *Sejam A e B conjuntos não vazios. Existe uma uma função sobrejetiva $f : A \to B$ se, e somente se, existe uma função injetiva $g : B \to A$.*

Prova. Com efeito, se existe uma sobrejeção $f : A \to B$, segue-se que, para cada $x \in B$, podemos escolher um único $y \in A$ tal que $f(y) = x$. Então, definimos $g : B \to A$, tal que $g(x) = y$. Note que isso é, evidentemente, uma injeção. Reciprocamente, se existe $g : B \to A$ injetiva, fixando um $a \in B$ qualquer, define-se $f : A \to B$ tal que $f(x) = g^{-1}(x)$, se $x \in g(B)$ e $f(x) = a$, se $x \notin g(B)$. Note que f é evidentemente sobrejetiva. ■

Proposição 1.2.7 *Uma função admite inversa se, e somente se, ela é bijetiva.*

Prova. Seja f uma função bijetiva. Logo, f admite uma inversa à esquerda e uma inversa à direita. Logo, estas são iguais, definindo uma função inversa para f. A recíproca segue do explicitado acima. ■

Proposição 1.2.8 *Se $f : X \to Y$ e $g : Y \to Z$ são funções bijetivas, então $g \circ f : X \to Z$ é bijetiva e $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Prova. Já sabemos que $g \circ f$ é bijetiva. Por outro lado, como $(g \circ f)^{-1}$ e $f^{-1} \circ g^{-1}$ são ambas funções de Z em X, a fim de verificar que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ é suficiente, pela unicidade da inversa, notar que $(f^{-1} \circ g^{-1}) \circ (g \circ f) = Id_X$ e $(g \circ f) \circ (f^{-1} \circ g^{-1}) = Id_Z$. ■

1.2.3 Conjunto de Funções

Definição 1.2.12 *Dados dois conjuntos não vazios X e Y. Denotaremos por $\mathcal{F}(X, Y)$ o conjunto de todas as funções de X em Y.*

A composição de duas funções determina em $\mathcal{F}(X, X)$ uma operação que já vimos, é associativa. Esta operação tem o elemento neutro Id_X e não é comutativa, se X tem dois ou mais elementos.

De fato, sejam $a, b \in X$, com $a \neq b$, e definamos $f : X \to X$, tal que $f(x) = a$, para todo $x \in X$ e $g : X \to X$, tal que $g(x) = b$, para todo $x \in X$. Agora, observe que $f(g(a)) = a$ e $g(f(a)) = b$ e, portanto, $f \circ g \neq g \circ f$.

Em matemática, frequentemente, um mesmo objeto pode vir apresentado de vários modos distintos. Por exemplo, quando $X = \{1, 2\}$ e $Y \neq \emptyset$, o conjunto $\mathcal{F}(X, Y)$ pode ser naturalmente identificado com o conjunto $Y^2 = Y \times Y$. De fato, para cada função $f : \{1, 2\} \to Y$, associamos o par $(f(1), f(2))$. Esta associação estabelece uma bijeção natural entre $\mathcal{F}(X, Y)$ e Y^2.

1.3 Boa Ordenação

Definição 1.3.1 *Seja X um subconjunto de números naturais. Diz-se que um número $p \in X$ é o menor elemento de X (ou elemento mínimo de X) quando se tem $p \leq n$ para todo $n \in X$.*

Por exemplo, 1 é o menor elemento do conjunto $\mathbb{N}$ de todos os números naturais. Com maior razão, qualquer que seja $X \subset \mathbb{N}$ com $1 \in X$, 1 é o menor elemento de X.

Definição 1.3.2 *Dado $X \subset \mathbb{N}$, se $p \in X$ e $q \in X$ são ambos os menores elementos de X então $p \leq q$ e $q \leq p$, donde $p = q$. Assim o menor elemento de um conjunto é único.*

Definição 1.3.3 *Analogamente, se $X \subset \mathbb{N}$, um número $p \in X$ chama-se o maior elemento de X (ou elemento máximo de X)quando se tem $p \geq n$ para todo $n \in X$.*

Nem todo conjunto de números naturais possui um elemento máximo. Por exemplo, o próprio $\mathbb{N}$ não tem o maior elemento já que, para todo $n \in \mathbb{N}$ tem-se $n+1 > n$.

Corolário 1.3.1 *Se existir o elemento máximo de um conjunto $X \subset \mathbb{N}$, ele é único.*

Prova. Com efeito, se $p \in X$ e $q \in X$ são ambos máximos então $p \geq q$ e $q \geq p$, donde $p = q$. ■

Um resultado de grande importância, até mesmo como método de prova, é o fato de que todo conjunto não vazio de números naturais possui um menor elemento. Este fato é conhecido como *Princípio da Boa Ordenação*. Para tanto, utilizaremos em sua prova o seguinte axioma:

(**Princípio da Indução**) Se $X \subset \mathbb{N}$ *é um subconjunto tal que* $1 \in X$ *e, para todo* $n \in X$ *tem-se também* $s(n) \in X$*, então* $X = \mathbb{N}$*. Definamos* $s(n)$ *como o sucessor de* n*.*

Teorema 1.3.1 *(**Princípio da Boa Ordenação**) Todo conjunto não vazio* $A \subset \mathbb{N}$ *possui um menor elemento.*

Prova. Usando a notação $I_n = \{p \in \mathbb{N}; 1 \leq p \leq n\}$, consideremos o conjunto $X \subset \mathbb{N}$, formado pelos números $n \in \mathbb{N}$ tais que $I_n \subset \mathbb{N} - A$. (Assim, dizer que $n \in X$ significa afirmar que $n \notin A$ e que todos os números naturais menores do que n também não pertencem a A). Se tivermos $1 \in A$, o teorema estará demonstrado pois 1 será o menor elemento de A. Se, porém, for $1 \notin A$ então $1 \in X$. Por outro lado, temos $X \neq \mathbb{N}$. (Pois $X \subset \mathbb{N} - A$ e $A \neq \emptyset$. Assim, X cumpre a primeira parte da hipótese de indução (contém 1) mas não satisfaz à conclusão (não é igual a $\mathbb{N}$). Logo, não pode cumprir a segunda parte da hipótese. Isto quer dizer: deve existir algum $n \in X$ tal que $n+1 \notin X$. Seja $a = n+1$. Então todos os inteiros desde 1 até n pertencem ao complementar de A mas $a = n+1$ pertence a A. Desta maneira, a é o menor elemento do conjunto A, o que prova o teorema. ■

Do Princípio da Boa Ordenação decorre uma proposição conhecida como o *Segundo Princípio da Indução*, que provaremos agora.

Teorema 1.3.2 *(**Segundo Princípio da Indução**) Seja* $X \subset \mathbb{N}$ *um conjunto com a seguinte propriedade: Dado* $n \in \mathbb{N}$*, se* X *contém todos os números naturais* m *tais que* $m < n$*, então* $n \in X$*. Nestas condições,* $X = \mathbb{N}$*.*

Prova. Seja $Y = \mathbb{N} - X$. Afirmamos que $Y = \emptyset$. Com efeito, se Y não fosse vazio, existiria um menor elemento $p \in Y$. Então, para todo número natural $m < p$, seria $m \in X$. Pela hipótese feita sobre X, teríamos $p \in X$, o que gera uma contradição. ■

O Segundo Princípio da Indução constitui um método útil para demonstração de proposições referentes a números naturais. Ele também pode ser anunciado assim:

Teorema 1.3.3 *Seja* $\mathcal{P}$ *uma propriedade relativa a números naturais. Se, dado* $n \in \mathbb{N}$*, do fato de todo número natural* $m < n$ *gozar da propriedade* $\mathcal{P}$ *puder ser inferido que* n *goza da propriedade* $\mathcal{P}$*, então todo número natural goza de* $\mathcal{P}$*.*

Um número natural chama-se *primo* quando $p \neq 1$ e não se pode escrever $p = m \cdot n$ com $m < p$ e $n < p$. O chamado Teorema Fundamental da Aritmética diz que todo número natural se decompõe, de modo único, como produto de fatores primos. A prova utiliza o Segundo Princípio da Indução. Com efeito, dado $n \in \mathbb{N}$, suponhamos que todo número natural menor do que n possa ser decomposto como produto de fatores primos. Então, ou n é primo (e neste caso n é, de modo trivial, um produto de fatores primos) ou então $n = m \cdot k$, com $m < n$ e $k < n$. Pela hipótese de indução, m e k são produtos de fatores primos. Segue-se que n também o é. Pelo Segundo Princípio da Indução, concluímos que todo número natural é produto de números primos.

Capítulo 2

Definições e Propriedades Básicas dos Números Cardinais

Quando comparamos dois conjuntos finitos, dizemos que sua equipotência se dá quando ambos têm o mesmo número de elementos. Não se pode dizer o mesmo de conjuntos infinitos, e quando falamos de conjunto de números infinitos nos referimos à sua correspondência biunívoca, ou que pode nos transmitir uma ideia de justa proporção entre estes conjuntos.

Mas com a descoberta de Cantor de que os números reais são *mais infinitos* que os números naturais, percebemo-nos em três níveis de enumerabilidade, ou seja: os conjuntos finitos propriamente, enumeráveis pelos seus próprios termos, os números infinitos enumeráveis, que podem ser justapostos como os números naturais, e finalmente o conjunto dos números que extrapolam esta correspondência, que seriam os enfim os *conjuntos não-enumeráveis*. É interessante esta maneira cantoriana de desvendar o infinito, e é talvez nesta perspectiva que se esconde grande parte do valor da teoria de Cantor dos números transfinitos. Ele nos mostra que o conjunto infinito, tal como o conjunto finito segue uma mesma regra, e que, ao contrário do que pensam alguns restricionistas, nos é passível de compreensão.

A intuição que se esconde por trás disso é o que o infinito enumerável é um infinito que se atualiza aos nossos olhos, isto é, não importa em que ponto de seu desenrolar estejamos, ele sempre seguirá as mesmas regras. Não se intimidando com o tamanho do infinito, Cantor postula uma tese de geração do infinito, tomando cada infinito como uma unidade e somando a este mais para obter um segundo infinito. À mesma maneira com que somamos um número ao outro, Cantor nos demonstra que é possível se fazer com o infinito enumerável em uma sucessão algorítmica inesgotável.

Por isso e apesar disso, Cantor postula uma terceira lei de geração em complemento às duas anteriores que ficam subentendidas na geração do infinito enumerável e na sucessão enumerável do mesmo.

Um infinito absoluto não pode ser provado matematicamente, porém os demais, e quaisquer infinitos de diferente potência podem, sem restrição alguma, ser bem ordenados, no sentido de que seus elementos estejam relacionados entre si por uma sucessão; há um primeiro elemento no conjunto, todo elemento, exceto o último, tem um antecessor, e finalmente, para cada elemento do dado conjunto bem ordenado, infinito ou não, há um determinado elemento que é o sucessor imediato de todos os elementos que compõem o conjunto.

Neste capítulo, apresento resultados importantes envolvendo equipotência, conjuntos finitos e infinitos, bem como conjuntos enumeráveis e não-enumeráveis. Os resultados precedentes sobre números cardinais nos fornecem uma visão inicial, intuitiva, porém incompleta do conceito de cardinais. Agora, formalizaremos o conceito de maneira a preservar o que foi visto, ampliando as possibilidades de entendimento para contextos mais ricos, ou mais especificamente, para um conjunto com muito mais elementos.

2.1 Conjuntos Equipotentes

Esta seção foi elaborada a partir das seguintes referências bibliográficas: [1], [4], [5], [6], [8], [11].

Definição 2.1.1 *Dizemos que um conjunto A é equipotente a um conjunto B se existir uma bijeção de A em B. Denotaremos por $A \sim B$ (lemos: A é equipotente a B).*

Teorema 2.1.1 *$\sim$ é uma relação de equivalência.*

Prova. Com efeito, a função identidade $Id : A \to A$, definida por $Id(a) = a$, para todo $a \in A$ é uma função bijetiva e, assim, $A \sim A$. Se $A \sim B$, existe uma função bijetiva $f : A \to B$ que admite uma inversa $f^{-1} : B \to A$, também bijetiva. Logo, $B \sim A$. Se $A \sim B$ e $B \sim C$, então existem funções $f : A \to B$ e $g : B \to C$ bijetivas. A composta de $(g \circ f) : A \to C$ é também bijetiva e assim $A \sim C$. ∎

O conceito de cardinalidade de conjuntos advém naturalmente do conceito de equipotência e tem a incumbência, na teoria dos conjuntos, de indicar a quantidade de elementos desse conjunto. Para conjuntos finitos essas concepções são bastante intuitivas, mas para o mesmo não se dá para os chamados conjuntos *transfinitos*, que vão além do infinito.

Definição 2.1.2 *Para cada conjunto A vamos associar um elemento x que chamaremos de número cardinal do conjunto A, o qual denotaremos por $|A|$. Dois conjuntos A e B são equipotentes se $|A| = |B|$.*

Definição 2.1.3 *x é um número cardinal se existir um conjunto A tal que $x = |A|$.*

Os números cardinais associados a conjuntos são denotados como se segue: $0 = |\emptyset|, 1 = |\{\emptyset\}|, 2 = |\{\emptyset, \{\emptyset\}\}|, ...$ e, dando continuidade, podemos associar de uma maneira recursiva aos algarismos que definem os números naturais de conjuntos de tal forma que, um conjunto tem n elementos se e somente se seu número cardinal for exatamente n.

Definição 2.1.4 *Sejam x e y dois números cardinais. $x \leq y$ se houver conjuntos A e B tais que $x = |A|$ e $y = |B|$ tal que A é equipotente a um subconjunto de B , para uma escolha particular de A e B.*

Definição 2.1.5 *Para qualquer conjunto A, indicamos por*

$$2^A = \{f; f : A \to \{0, 1\}\}.$$

Proposição 2.1.1 *Se A é um conjunto, tal que $A \neq \emptyset$, então $\wp(A) \sim 2^A$, em que $\wp(A)$ é o conjunto das partes de A.*

Prova. Para $B \subseteq A$, seja $f_B : A \to \{0, 1\}$ a função característica de B, isto é,

$$f_B(a) = \begin{cases} 0, & \text{se} \quad a \notin B \\ 1, & \text{se} \quad a \in B \end{cases}$$

A função $g : \wp(A) \to 2^A$ definida por $g(B) = f_B$ é bijetiva. ∎

Teorema 2.1.2 *Sejam A e B conjuntos quaisquer. Se $|A| = |B|$, então $|\wp(A)| = |\wp(B)|$.*

Prova. Se $|A| = |B|$, então existe uma bijeção $f : A \to B$. Seja $g : \wp(A) \to \wp(B)$, dada por $g(X) = f(X)$(a imagem do conjunto X pela função f). Vamos, agora, mostrar que g é bijetiva.

(i) **Injetividade**: Se $g(X) = g(Y)$, então $f(X) = f(Y)$. Daí como f é bijetiva, temos que $X = f^{-1}(f(X)) = f^{-1}(f(Y)) = Y$.

(ii) **Sobrejetividade**: Seja $Y \in \wp(B)$ e consideremos a imagem inversa de Y como $f^{-1}(Y) \in \wp(A)$.

Então, $g(f^{-1}(Y)) = f(f^{-1})(Y) = Y$ pois f é bijetiva. Isto posto, $\wp(A) \to \wp(B)$ é bijetiva. ∎

Teorema 2.1.3 ***(Cantor)*** *Seja A um conjunto não vazio qualquer e denotemos $\wp(A)$ o conjunto das partes de A. Temos que $|A| < |\wp(A)|$.*

Prova. Sabemos que a aplicação $f : A \to \wp(A)$, tal que $f(a) = \{a\}$ é injetiva, então, de maneira imediata, $|A| \leq |\wp(A)|$. Para mostrar que, adicionalmente, se tem $|A| \neq |\wp(A)|$ é necessário provar agora que não existe nenhuma bijeção entre A e $\wp(A)$. Logo, basta mostrar que não há nenhuma função de A em $\wp(A)$ que seja sobrejetiva ou, dito de outro modo, que para toda a função $f : A \to \wp(A)$ existe um subconjunto X de $\wp(A)$ que não é imagem de f de nenhum elemento de A. Tal prova devemos a Cantor, que introduziu o conjunto $X = \{x \in A; x \notin f(x)\}$ provando em seguida que não existe qualquer $b \in A$ para o qual se tenha $f(b) = X$. De fato, seja $x \in A$ qualquer. Então ou $x \notin X$ ou $x \in X$. Se $x \notin X$, da definição de X resulta que $x \in f(x)$ e, portanto, $f(x) \neq X$. Consequentemente, $f(x)$ não é uma função sobrejetiva, como foi afirmado. ■

Vimos que $\wp(A)$ é o conjunto das partes de um conjunto A. Considerando o conjunto de dois elementos $\{0, 1\}$, veremos agora que existe uma bijeção $h : \wp(A) \to \mathcal{F}(A; \{0, 1\})$. A cada $X \in \wp(A)$, associamos a função $h_X : A \to \{0, 1\}$ chamada função característica do conjunto X. Temos que:

$$h_X(x) = \begin{cases} 1, & \text{se} \quad x \in X \\ 0, & \text{se} \quad x \notin X \end{cases}$$

A correspondência $X \mapsto h_X$ é uma bijeção de $\wp(A)$ sobre $\mathcal{F}(A; \{0, 1\})$. Sua inversa associa a cada função $f : A \to \{0, 1\}$ o conjunto X dos pontos $x \in A$ tais que $f(x) = 1$. Como $\{0, 1\}$ tem dois elementos, temos que nenhuma função $r : A \to \mathcal{F}(A; \{0, 1\})$ é sobrejetiva. Consequentemente, nenhuma função $s : A \to \wp(A)$ é sobrejetiva. (Se fosse, $r = h \circ s : A \to \mathcal{F}(A; \{0, 1\})$ também seria sobrejetiva). Mas existe uma função injetiva evidente $f : A \to \wp(A)$, definida por $f(x) = \{x\}$. De fato, como provado no teorema anterior, temos que $|A| < |\wp(A)|$ para todo conjunto A.

Definição 2.1.6 *Quando há uma função injetiva de A em B indicamos por $A \preceq B$ e quando há função injetiva e A não é equipotente a B, indicamos por $A \prec B$. Isto posto, para cada conjunto A vale $A \prec \wp(A)$.*

Lema 2.1.1 *Se $C \subseteq A$ e $A \preceq C$, então $A \sim C$.*

Prova. Seja $f : A \to C$ uma função injetiva e consideremos $A_0 = A - C, A_1 = f(A_0), ..., A_{n+1} = f(A_n)$. Definamos uma função $g : A \to C$ e provemos que g é bijetiva:

$$g(a) = \begin{cases} a, & \text{se} \quad a \notin \bigcup_{n \in \mathbb{N}} A_n \\ f(a), & \text{se} \quad a \in \bigcup_{n \in \mathbb{N}} A_n \end{cases}$$

Mostremos que g é bijetiva:

(a) g é injetiva:

Sejam $a, b \in A$ com $a \neq b$.

Se $a \notin \bigcup_{n\in\mathbb{N}} A_n$ e $b \notin \bigcup_{n\in\mathbb{N}} A_n$, então $g(a) = a$ e $g(b) = b$. Isto posto, $g(a) = g(b)$.

Se $a \notin \bigcup_{n\in\mathbb{N}} A_n$ e $b \in \bigcup_{n\in\mathbb{N}} A_n$, então $g(a) = a$ e $g(b) = f(b)$. Daí, $g(a) = a \notin \bigcup_{n\in\mathbb{N}} A_n$ e $g(b) = f(b) \in \bigcup_{n\in\mathbb{N}} A_n$. Isto posto, $g(a) \neq g(b)$.

Se $a \in \bigcup_{n\in\mathbb{N}} A_n$ e $b \in \bigcup_{n\in\mathbb{N}} A_n$, então $g(a) = f(a)$ e $g(b) = f(b)$. Uma vez que f seja injetiva, então $g(a) \neq g(b)$ e g também é injetiva.

(b) g é sobrejetiva:

Seja $c \in C$. Se $c \notin \bigcup_{n\in\mathbb{N}} A_n$, então $g(c) = c$.

Se $c \in \bigcup_{n\in\mathbb{N}} A_n$, como $c \notin A - C = A_0$, então $c \in A_j$, para algum $j \geq 1$. Logo, existe $b \in A_{j-1}$ tal que $c = f(b) = g(b)$.

Portanto, g é sobrejetiva e, como também é injetiva, concluímos que g é bijetiva.

■

Segue uma proposição que servirá de apoio para a prova do teorema de Cantor-Schroder-Bernstein:

Proposição 2.1.2 *Se $B \subset A$ e $|A| \leq |B|$, então $|A| = |B|$, ou seja, se $B \subset A$, existe uma função injetiva $f : A \to B$, então $|A| = |B|$.*

Teorema 2.1.4 *(**Cantor-Schroder-Bernstein**) Dados dois conjuntos A e B, se $|A| \leq |B|$ e também $|B| \leq |A|$, então $|A| = |B| \Rightarrow A \sim B$.*

Prova. Com efeito, tomando as funções injetivas $f : A \to B$ e $g : B \to A$, tem-se que $f^* : A \to f(A)$, onde $f^*(x) = f(x)$, é uma bijeção entre A e $f(A) \subset B$. Logo, $(f^* \circ g) : B \to f(A)$ é uma função injetiva. Como $f(A) \subset B$, temos que $|f(A)| = |B|$ ou, em outras palavras, existe uma função bijetiva $h : f(A) \to B$. Notemos, então que $(h \circ f^*) : A \to B$ é composição de funções bijetivas e, portanto, é uma função bijetiva. Portanto, $A \sim B$. ■

Proposição 2.1.3 ***(Princípio da Casa dos Pombos)*** *Se a cardinalidade de A é estritamente maior do que a cardinalidade de B, então não existe injeção de A em B.*

Prova. Basta ver que se $|A| \leq |B|$ e se houvesse uma injeção $f : A \to B, f : A \to f(A)$ seguiria que $|A| \leq |B|$ e, pelo *Teorema de Cantor-Schroder-Bernstein*, isso implicaria que $|A| = |B|$, o que prova a nossa proposição. ■

2.2 Conjuntos Finitos e Infinitos

Esta seção foi elaborada a partir das seguintes referências bibliográficas: [1], [4], [11].

Pelo que já foi explicitado neste trabalho, é imediato constatar que a relação de equipotência entre conjuntos é uma relação de equivalência. Como já vimos na seção anterior, escrevemos $A \sim B$ para representar que A e B são equipotentes.

Podemos agora formalizar a definição de conjunto finito do seguinte modo:

Definição 2.2.1 *Um conjunto A é chamado finito se for vazio ou existir um número $m \in \mathbb{N}$ tal que $A \sim I_m = \{1, 2, 3, ..., m\}$. Um conjunto que não é finito é chamado infinito.*

A questão que se coloca naturalmente é saber se o número natural m é univocamente determinado por A e pela existência de uma bijeção de I_m em A. Bem, a resposta é positiva e decorre do resultado a seguir:

Definição 2.2.2 *Se A for um conjunto finito, o número $m \in I_m$ tal que $A \sim I_m$ é, como se sabe, o cardinal do conjunto A que se denota por $|A|$.*

O objetivo agora é darmos um significado à noção de cardinalidade no caso de conjuntos infinitos. Antes, porém, consideremos o seguinte resultado:

Teorema 2.2.1 *Sejam m e n dois números naturais. Se $m > n > 0$, então não existe nenhuma função injetiva de I_m em I_n.*

Prova. Afirmamos que basta provar o teorema quando $m = n+1$. De fato, suponha que a asserção do teorema válida para $m = n + 1$. Se $m > n + 1$ e se existisse uma função injetiva de I_m em I_n, a sua restrição a I_{n+1} também seria injetiva, o que seria uma contradição. Para provar o teorema, usemos indução em n. A afirmação é válida para $n = 1$ e suponha que é válida para n. Provemos, então, que é válida para $n + 1$. Suponha, por absurdo, que a afirmação para $n + 1$ é falsa. Logo, existe $f : I_{n+2} \to I_{n+1}$ injetiva. Duas possibilidades podem ocorrer:

(a) $n+1 \notin f(I_{n+2})$. Nesse caso, a função $g : I_{n+1} \to I_n$, definida por $g(x) = f(x)$ para todo $x \in I_{n+1}$ é injetiva, o que é uma contradição.

(b) $n+1 \in f(I_{n+2})$. Seja x' o único elemento de I_{n+2} tal que $f(x') = n+1$. Consideraremos, agora, dois subcasos:

(b') $x' = n+2$. Neste caso, $g : I_{n+1} \to I_n$ definida por $g(x) = f(x)$, $\forall x \in I_{n+1}$ é bem definida e injetiva, absurdo.

(b'') $x' \neq n+2$. Como f é injetiva, temos que $f(n+2) \neq f(x') = n+1$.

Isto posto, a função $g : I_{n+1} \to I_n$ definida por

$$g(x) = \begin{cases} f(x), & \text{se} \quad x \notin x' \\ f(n+2), & \text{se} \quad x \in x' \end{cases}$$

é bem definida e injetiva, o que também é uma contradição. ■

Suponha agora que dado um conjunto A, existam números naturais m e n com $m > n > 0$ e duas bijeções $f : I_m \to A$ e $g : I_n \to A$. Segue-se então que $g^{-1} \circ f : I_m \to I_n$ é uma bijeção, portanto, injetiva o que não é possível pelo teorema.

Consequentemente, dado um conjunto finito A, o número natural m para o qual existe uma bijeção de $I_m \to A$ é univocamente determinado por A e é chamado de *cardinalidade* de A. Diremos, neste caso, que A tem m elementos. A cardinalidade do conjunto vazio $\emptyset$ é zero, por definição.

Corolário 2.2.1 ***(Princípio de Dirichlet)*** *Dados dois conjuntos X e Y respectivamente com m e n elementos, se $m > n > 0$, então não existe nenhuma função injetiva de X em Y.*

Prova. Existem bijeções $f : I_m \to X$ e $g : I_n \to Y$. Se existisse uma função injetora $h : X \to Y$, teríamos que $f^{-1} \circ h \circ f : I_m \to I_n$ é injetiva, o que não seria possível pelo teorema. ■

Corolário 2.2.2 *Seja X um conjunto com m elementos e Y um conjunto com n elementos. Se $m < n$, então não existe nenhuma função sobrejetiva de X em Y.*

Prova. Suponha $m > 0$ e que exista uma função sobrejetiva de $f : X \to Y$. Logo, sabemos do capítulo anterior que a função f admitiria uma inversa à direita $g : Y \to X$. Portanto, $f \circ g = Id_Y$. Segue-se então que g admite uma inversa à esquerda. Isto posto, temos que g é injetiva, o que contradiz o Princípio de Dirichlet. Se $m = 0$, o resultado vale por vacuidade, pois não existem sequer funções de $\emptyset$ em Y. ■

Corolário 2.2.3 *Sejam X e Y dois conjuntos finitos de mesma cardinalidade. Uma função $f : X \to Y$ é injetiva se, e somente se, ela é sobrejetiva.*

Prova. Suponha que f seja injetiva e suponha, por absurdo, que não é sobrejetiva. Seja $y' \in Y$ não pertencente a $f(X)$. Logo, a função:

$$\begin{array}{rccc} f_1 : & X & \to & Y \\ & x & \mapsto & f(x) \end{array}$$

é bem definida e injetiva, o que é uma contradição pelo Princípio de Dirichlet. Suponha agora que f seja sobrejetiva e mas não injetiva. Logo, existem x' e x'' tais que $f(x') = f(x'')$. Isto posto a função:

$$\begin{array}{rccc} f_2 : & X - \{x'\} & \to & Y \\ & x & \mapsto & f(x) \end{array}$$

é bem definida e sobrejetiva, o que também gera uma contradição pelo corolário anterior. ■

Teorema 2.2.2 *Todo o conjunto infinito contém um subconjunto equipotente a* $\mathbb{N}$.

Prova. Seja A um conjunto infinito qualquer. A é não vazio e, portanto, possui um elemento $a_1 \in A$. O conjunto $A \setminus \{a_1\}$ é não vazio pois se não fosse A seria o conjunto finito $\{a_1\}$. Consequentemente existirá $a_2 \in A \setminus \{a_1\}$. Analogamente, o conjunto $A \setminus \{a_1, a_2\}$ não pode ser vazio e, portanto, existirá $a_3 \in A \setminus \{a_1, a_2\}$. Procedendo assim sucessivamente obteremos um subconjunto $\{a_1, a_2, ...,\}$ de A que é equipotente a $\mathbb{N}$. ■

Este teorema revela que o conjunto $\mathbb{N}$ é, de certo modo, o *menor conjunto infinito*, já que cada conjunto infinito possui um subconjunto equipotente a $\mathbb{N}$. Com base no teorema anterior podemos agora definir conjunto finito a partir da noção de conjunto infinito sem exigir o conhecimento prévio do conjunto $\mathbb{N}$. Tal definição se deve a ***Dedekind***.

De acordo com este resultado todos os subconjuntos infinitos de $\mathbb{N}$ são equipotentes a $\mathbb{N}$. Estão neste caso, por exemplo, os conjuntos dos números pares positivos, dos números ímpares positivos, dos números primos, etc.

Proposição 2.2.1 *O conjunto dos números inteiros $\mathbb{Z}$ é infinito.*

Prova. Se existissem um número natural m e uma bijeção $f : I_m \to \mathbb{Z}$ teríamos uma função injetiva $f^{-1} : \mathbb{Z} \to I_m$ e, portanto a função restrição $g : I_{m+1} \to I_m$ seria injetiva, o que é impossível. Portanto, $\mathbb{Z}$ é infinito. ■

2.2.1 O Paradoxo do Hotel Infinito de Hilbert

David Hilbert foi um grande entusiasta das descobertas de Cantor, chegando a afirmar que *ninguém nos expulsará do paraíso que Cantor criou para nós.* Para ilustrar o conceito de infinitude e enumerabilidade, Hilbert imaginou um hotel de infinitos quartos. Vamos explorar a ideia de Hilbert com uma dose extra de ficção.

O Hotel de Hilbert fica ao bordo do Mar Mediterrâneo, em Saint Tropez, na badalada Cote d'Azur. Seu edifício, cinza e branco, construído em 1925 é um belo exemplo de estilo art-decor dos anos 20 e 30 do século XX. Grande e confortável, o hotel tem uma infinidade enumerável de quartos suficientes para hospedar clientes dos mais diversos gostos. Desde aqueles em busca de dias tranquilos e ensolarados aos que preferem noites em boates agitadas. O gerente, o próprio David Hilbert, é um homem muito gentil, de barba bem tratada que nunca é visto sem seus óculos e chapéu branco. O Grande Hotel de Hilbert tinha uma infinidade de quartos, nu-

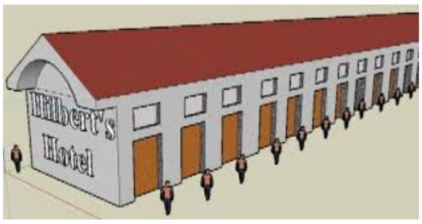

Figura 2.1: O Hotel de Hilbert

merados consecutivamente, uma para cada número natural. Todos eram igualmente confortáveis. Num fim de semana prolongado, o hotel estava com seus quartos todos ocupados, quando chega um viajante. A recepcionista vai logo dizendo:

-Sinto muito, mas não há vagas.

Ouvindo isto, o gerente interveio:

-Podemos abrigar o cavalheiro, sim senhora.

E a ordena:

-Transfira o hóspede do quarto 1 para o quarto 2, passe do quarto 2 para o quarto 3 e assim por diante. Quem estiver no quarto n, mude para o quarto $n+1$. Isto manterá todos alojados e deixará disponível o quarto 1 para o recém-chegado. Logo depois chegou um ônibus com 1000 passageiros, todos querendo hospedagem. A recepcionista, tendo aprendido a lição, removeu o hóspede de cada quarto n para o quarto $n+1000$ e acolheu todos os passageiros do ônibus. Mas ficou sem saber o que fazer quando, horas depois, chegou um trem com uma infinidade de passageiros (estes passageiros devem ser indexados por $\mathbb{N}$). Desesperada, apelou para o gerente que prontamente respondeu o problema dizendo:

-Passe cada hóspede do quarto n para o quarto $2n$. Isto deixará vagos todos os apartamentos de número ímpar, nos quais poremos os novos hóspedes.

-Pensando melhor: mude quem está no quarto n para o quarto $3n$. Os novos hóspedes, ponha-os no quarto de número $3n + 2$. Deixaremos vagos os quartos de número $3n + 1$. Assim, sobrarão ainda infinitos quartos vazios e eu poderei ter sossego por algum tempo.

2.3 Conjuntos Enumeráveis e Não-Enumeráveis

Esta seção foi elaborada a partir das seguintes referências bibliográficas: [1], [4], [9], [11].

Definição 2.3.1 *Um conjunto X é enumerável quando é finito ou quando existe uma bijeção $f : \mathbb{N} \to X$. No segundo caso, X é chamado de infinito enumerável e, pondo $x_1 = f(1), x_2 = f(2), ..., x_n = f(n), ...$ temos $X = \{x_1, x_2, x_3, ..., x_n, ...\}$. Cada bijeção $f : \mathbb{N} \to X$ chamamos uma enumeração (dos elementos) de X.*

A bijeção $f : \mathbb{N} \to \mathbb{P}, f(n) = 2n$, mostra que o conjunto $\mathbb{P}$ dos números naturais pares é infinito enumerável. Analogamente, $g : n \mapsto 2n - 1$ define uma bijeção de $\mathbb{N}$ sobre o conjunto dos números naturais ímpares, o qual é, portanto, infinito enumerável. Também o conjunto $\mathbb{Z}$ dos números inteiros é enumerável. Basta notar que a função $h : \mathbb{Z} \to \mathbb{N}$, definida por:

$$h(x) = \begin{cases} 2n, & \text{se} \quad n > 0 \\ -2n + 1, & \text{se} \quad n \leq 0 \end{cases}$$

é uma bijeção. Isto posto, $h^{-1} : \mathbb{N} \to \mathbb{Z}$ é uma enumeração de $\mathbb{Z}$.

Valem as seguintes propriedades sobre conjuntos:

Proposição 2.3.1 *Seguem as seguintes afirmações:*

(1) Se X é um conjunto infinito, então $|X| \geq |\mathbb{N}|$;

(2) Um subconjunto de conjunto finito é necessariamente finito;

(3) Uma união finita de conjuntos é finita;

(4) Um subconjunto de um conjunto enumerável é necessariamente enumerável;

(5) Uma união enumerável de conjuntos enumeráveis é necessariamente enumerável;

(6) Um produto finito de conjuntos enumeráveis é enumerável.

Teorema 2.3.1 *Todo conjunto infinito X contém um subconjunto infinito enumerável.*

Prova. Basta definirmos uma função injetiva $f : \mathbb{N} \to X$. Para isso, começaremos escolhendo, em cada subconjunto não vazio $A \subset X$, um elemento $x_A \in A$. Em seguida, definimos f por indução. Colocamos $f(1) = x_X$ e, supondo já definidos $f(1), f(2), ..., f(n)$, escrevemos $A_n = X - \{f(1), f(2), ..., f(n)\}$. Como X não é finito, A_n é não vazio. Colocaremos então $f(n+1) = x \in A_n$. Isto completa a definição indutiva da função $f : \mathbb{N} \to X$. Afirmamos que f é injetiva. Com bastante efeito, dados $m \neq n$ em $\mathbb{N}$ com $m < n$. Então, $f(m) \in \{f(1), f(2), ..., f(n-1)\}$ enquanto que $f(n)$ está no complementar de $\{f(1), f(2), ..., f(n-1)\}$. Logo, $f(m) \neq f(n)$. A imagem de $\mathbb{N}$ é, portanto, um subconjunto infinito enumerável de X. ∎

Teorema 2.3.2 *Todo conjunto de $X \subset \mathbb{N}$ é enumerável.*

Prova. Se X for finito, é enumerável. Se for infinito, definiremos por indução uma bijeção $f : \mathbb{N} \to X$. Coloquemos $f(1), f(2), ..., f(n)$ definidos de modo a satisfazerem as seguintes condições:

(a) $f(1) < f(2) < ... < f(n)$;

(b) Pondo $B_n = X - \{f(1), f(2), ..., f(n)\}$ temos $f(n) < x$ para todo $x \in B_n$.

Em seguida, percebendo que $B_n \neq \emptyset$ (uma vez que X é infinito), definimos $f(n+1)$ como o menor elemento de B_n. Isto completa a definição de $f : \mathbb{N} \to X$, de modo a serem mantidas as condições (a) e (b) para todo $\mathbb{N}$. Segue-se de (a) que f é injetiva. Por outro lado, (b) implica que f é sobrejetiva pois se existisse algum $x \in X - f(\mathbb{N})$, teríamos $x \in B_n$ para todo n e, portanto, $x > f(n)$, qualquer que fosse $n \in \mathbb{N}$. Então o conjunto infinito $f(\mathbb{N}) \subset \mathbb{N}$ seria limitado, uma contradição. ∎

Teorema 2.3.3 *Seja X um conjunto enumerável. Se $f : X \to Y$ é sobrejetiva, então Y é enumerável.*

Prova. Existe $g : Y \to X$ tal que $f \circ g = Id_Y$. Logo, f admite uma inversa à esquerda de g e, portanto, g é injetiva. Segue-se, então, que Y é enumerável. ∎

Teorema 2.3.4 *Sejam X e Y conjuntos enumeráveis. O produto cartesiano $X \times Y$ é enumerável.*

Prova. Existem funções injetivas $r : X \to \mathbb{N}$ e $s : Y \to \mathbb{N}$. Logo, $g : X \times Y \to \mathbb{N} \times \mathbb{N}$, dada por $g(x, y) = (r(x), s(y))$ é injetiva. Isto posto, basta provarmos que $\mathbb{N} \times \mathbb{N}$ é enumerável. Para isso, tomemos a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, em que $f(m, n) = 2^m \cdot 3^n$. Pela unicidade da decomposição em fatores primos, f é injetiva, o que fornece uma bijeção de $\mathbb{N} \times \mathbb{N}$ sobre o conjunto enumerável $f(\mathbb{N} \times \mathbb{N}) \subset \mathbb{N}$. ∎

Teorema 2.3.5 *O conjunto $\mathbb{Q}$ dos números racionais é enumerável.*

Prova. De fato, o conjunto $\mathbb{Z} - \{0\}$ é um conjunto enumerável. Daí, também é um conjunto enumerável o produto cartesiano $\mathbb{Z} \times \mathbb{Z} - \{0\}$. Ora, a função $f : \mathbb{Z} \times \mathbb{Z} - \{0\} \to \mathbb{Q}$, definida por $f(m,n) = \dfrac{m}{n}$ é sobrejetiva. Isto posto, concluímos que $\mathbb{Q}$ é enumerável. ■

Corolário 2.3.1 *Sejam $X_1, X_2, ..., X_n, ...$ conjuntos enumeráveis. A união $X = \bigcup_{n=1}^{\infty} X_n$ é enumerável.*

Prova. Em palavras, uma união enumerável de conjuntos enumeráveis é um conjunto enumerável. Para provarmos tomemos, para cada $m \in \mathbb{N}$, uma função sobrejetiva $f_m : \mathbb{N} \to X_m$. Em seguida, definamos uma função $f : \mathbb{N} \times \mathbb{N} \to X$ colocando $f(m,n) = f_m(n)$. Observemos que f é sobrejetiva. Como $\mathbb{N} \times \mathbb{N}$ é enumerável, concluímos que X é enumerável. ■

Em particular, uma união finita $X = X_1 \cup ... \cup X_n$ de conjuntos enumeráveis é também um conjunto enumerável. Basta aplicar o corolário acima, com $X_{n+1} = X_{n+2} = ... = \emptyset$.

Vimos que dois conjuntos finitos tem o mesmo número cardinal se, e somente se, possuem o mesmo número de elementos. Se X for infinito enumerável temos $|X| = |Y|$ se, e somente se, Y for infinito enumerável.

Lembramos que, como visto no capítulo 1, dados dois conjuntos X e Y, o símbolo $\mathcal{F}(X;Y)$ representa o conjunto de todas as funções $f : X \to Y$.

Teorema 2.3.6 *Sejam X um conjunto arbitrário e Y um conjunto contendo pelo menos dois elementos. Nenhuma função $s : X \to \mathcal{F}(X;Y)$ é sobrejetiva.*

Prova. Dada $r : X \to \mathcal{F}(X;Y)$, indicaremos com r_x o valor de r no ponto $x \in X$. Dessa forma, r_x é uma função de X em Y. Construiremos, agora, uma função $f \in \mathcal{F}(X;Y)$ tal que $r_x \neq f$ para todo $x \in X$. Isto é feito escolhendo, para cada $x \in X$, um elemento $f(x) \in Y$, diferente de r_x. Como Y contém pelo menos dois elementos, isto é possível. A função $f : X \to Y$ assim obtida é tal que $f(x) \neq r_x(x)$ e, portanto, $f \neq r_x$, para todo $x \in X$. Isto posto, $f \notin r(X)$ e, portanto, r não é sobrejetiva. ■

Corolário 2.3.2 *Sejam $X_1, X_2, X_3, ..., X_n, ...$ conjuntos infinitos enumeráveis. O produto cartesiano $\prod_{n=1}^{\infty} X_n$ não é enumerável.*

Prova. Basta considerar o caso em que todos os X_n são iguais a $\mathbb{N}$. Nesse caso, $\prod X_n = \mathcal{F}(\mathbb{N};\mathbb{N})$, o que não é enumerável. ■

Teorema 2.3.7 *O conjunto dos números reais $\mathbb{R}$ não é enumerável.*

Prova. Cada número real x tal que $0 \leq x \leq 1$ admite uma representação decimal da forma $0, a_1a_2a_3...a_n...$, sendo que cada a_i um algarismo, isto é, tal que $a_i \in \{0, 1, 2, \cdots, 9\}$ e, ademais, tal representação decimal é única se não tivermos $a_i = 9$ para todo índice maior que algum índice i_0 fixado. Se o conjunto de todos os números reais x tais que $0 \leq x \leq 1$ fosse enumerável, poderíamos rotular suas representações decimais por números naturais, como:

$$
\begin{array}{c}
x_1 = 0, a_{11}a_{12}a_{13}...a_{1n}... \\
x_2 = 0, a_{21}a_{22}a_{23}...a_{2n}... \\
x_3 = 0, a_{31}a_{32}a_{33}...a_{3n}... \\
.... \\
x_n = 0, a_{n1}a_{n2}a_{n3}...a_{nn}.... \\
....
\end{array}
$$

Definamos agora, por sua representação decimal, um número real x tal que $0 \leq x < 1$ e $x \neq x_n$ para todo índice n, o que estabelecerá uma contradição e, portanto, mostrará que o conjunto em questão não pode ser enumerável. Construímos x como segue: para cada natural n, o n-ésimo algarismo da representação decimal de x é igual a qualquer inteiro b_n tal que $0 \leq b_n < 9$ e $b_n \neq a_{nn}$, de forma que $x = 0, b_1b_2b_3...b_n....$ Isto posto, temos $x \neq x_n$ para cada índice n, uma vez que as representações decimais de x e x_n diferem pelo menos em seus n-ésimos algarismos. ■

Observação 2.3.1 *O conjunto dos números irracionais é não-enumerável.*

Prova. De fato, denotemos por $\mathbb{I}$ o conjunto dos números irracionais. Por absurdo se $\mathbb{I}$ fosse enumerável, então como $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ concluiríamos que $\mathbb{R}$ deveria ser enumerável pois seria uma união de conjuntos enumeráveis, o que é um absurdo. ■

Corolário 2.3.3 *Se A é um conjunto infinito e B é finito, dada uma função $f : A \to B$, existe pelo menos um x tal que $f^{-1}(x)$ é um conjunto de cardinalidade infinita.*

Prova. Temos que, se B é finito e existe uma função $f : A \to B$ tal que $f^{-1}(x)$ é finito, para todo $x \in B$, teríamos que $\bigcup_{x \in B} f^{-1}(x)$ é uma união finita de conjuntos finitos e A, portanto, seria finito. ■

Capítulo 3

Números Transfinitos e Aritmética Cardinal

Existe, depois do finito, um transfinito, ou seja, uma escala ilimitada de modos determinados, que por natureza são infinitos, e que no entanto podem ser definidos de maneira precisa, tal como o finito, por números determinados, bem definidos e distintos uns dos outros.

Cantor chegou à noção de infinito real sem considerar diretamente os números, mas sim os conjuntos. Para isso, procurou atribuir *tamanhos*, que ele chamou de cardinalidade, aos diversos tipos de conjuntos de infinitos elementos. A essas potências deu o nome de *números transfinitos*.

Cantor se fazia então várias perguntas: Se haviam vários números transfinitos, será que era possível ordená-los? Haveria um infinito maior que todos os outros?

Para tentar responder essas perguntas, Cantor, que era um teórico conciencioso, desenvolve então uma aritmética do infinito, isto é, uma extensão, para os números que lhe servem como medida do infinito, das regras de aritmética que se aplicam aos números naturais, usados para medir o que é finito (adição, multiplicação, exponenciação, etc.).

Este capítulo tem como objetivo apresentar resultados importantes envolvendo os chamados números transfinitos, bem como apresentar uma aritmética na qual estes números são, de fato, contemplados, é a chamada *aritmética cardinal*.

3.1 Números Cardinais

Esta seção foi elaborada a partir das seguintes referências bibliográficas: [1], [4], [7], [10].

O primeiro cardinal infinito (***transfinito***) é o cardinal de $\mathbb{N}$, usualmente denotado por $\aleph_0$. O símbolo $\aleph$ é a primeira letra do alfabeto hebraico e chama-se ***alef***. Em geral, denotamos os cardinais transfinitos por $\aleph$ com algum índice.

Os cardinais formam uma sequência transfinita iniciada pelos números naturais (que são cardinais) e por $\aleph_0$. A sequência constituída pelos primeiros cardinais tem então o seguinte aspecto:

$$0 < 1 < 2... < \aleph_0.$$

Mas a sequência de cardinais nunca termina, $\aleph_1$ denota o menor cardinal que é maior que $\aleph_0$, depois, $\aleph_2$ denota o menor dos cardinais que é maior que $\aleph_1$, e assim sucessivamente, permitindo avançar na sequência acima para obter

$$0 < 1 < 2 < ... < \aleph_0 < \aleph_1 < \aleph_2 < ... < \aleph_n < ....$$

Definição 3.1.1 *O cardinal $\aleph_1$ é definido como o cardinal do conjunto $\wp(A)$ onde A é um conjunto cujo cardinal é $\aleph_0$. $\aleph_2$ é definido como o cardinal do conjunto $\wp(B)$ onde B é um conjunto cujo número cardinal é $\aleph_1$, e assim sucessivamente.*

Teorema 3.1.1 *(**Sanduíche de Cardinais**) Sejam B, C e D conjuntos. Se $D \subseteq C \subseteq B$ e $D \sim B$, então $D \sim C \sim B$.*

Prova. Como $D \sim B$ existe uma bijeção $f : B \to D$. Como $D \subseteq C$, então $f : B \to C$ é injetiva, ou seja, $B \preceq C$. Como $C \subseteq B$, segue-se que $C \preceq B$. Logo, pelo Teorema de Cantor-Schroder-Bernstein, temos que $C \sim B$ e $D \sim C$. ∎

3.1.1 Relação de Ordem entre Cardinais

Definindo uma ordem sobre os cardinais podemos indicar quando um conjunto tem cardinalidade maior que o outro. Nesse caso, diremos que o primeiro conjunto tem uma quantidade maior de elementos.

Definição 3.1.2 *Dados dois conjuntos A e B, a cardinalidade de A é menor ou igual que a cardinalidade de B quando existe um $C \subseteq B$ tal que C é equipotente a A, ou seja:*

$$|A| \leq |B| \Leftrightarrow \textit{existe um } C \subseteq B \textit{ tal que } A \sim C.$$

Nesse caso dizemos também que $|B| \geq |A|$ e que a relação $\geq$ (maior ou igual) é a relação inversa de $\leq$. Naturalmente, se $|B| \leq |A|$ e B não é equipotente a A, então $|B|$ é menor que $|A|$ e escreve-se $|B| < |A|$ ou ainda $|A| > |B|$. Isso significa que A tem uma quantidade maior de elementos que B.

3.2 Aritmética Cardinal

Esta seção foi elaborada a partir das seguintes referências bibliográficas: [1], [4], [5], [6], [8].

3.2.1 Adição de Cardinais

Definição 3.2.1 *Dados dois cardinais* $\mathfrak{a}$ *e* $\mathfrak{b}$ *tais que* $|A| = \mathfrak{a}$ *e* $|B| = \mathfrak{b}$*, temos que* $|A \cup B| = \mathfrak{a} + \mathfrak{b}$ *se* $A \cap B = \emptyset$*. Esta soma de cardinais é unica.*

Para observarmos que existe tal cardinal procederemos como se segue. Dados dois cardinais quaisquer $\mathfrak{a}$ e $\mathfrak{b}$ existem conjuntos C e D tais que $|C| = \mathfrak{a}$ e $|D| = \mathfrak{b}$. De fato, $C \times \{0\}$ e $D \times \{1\}$ são equipotentes a C e D, respectivamente. Denotemos $A = C \times \{0\}, B = D \times \{1\}$ então $|A| = |C| = \mathfrak{a}, |B| = |D| = \mathfrak{b}$, e $A \cap B = \emptyset$, portanto existem conjuntos A e B como apresentamos na definição no tocante à adição. Nos referiremos a $\mathfrak{a} + \mathfrak{b}$ como a soma de $\mathfrak{a}$ e $\mathfrak{b}$.

Proposição 3.2.1 *Para todos os conjuntos* A *e* B*, não necessariamente disjuntos, temos que* $|A \cup B| \leq |A| + |B|$*.*

Prova. Se $A \cap B = \emptyset$, temos que $|A \cup B| = |A| + |B|$. Se $|A \cap B| \neq \emptyset$, temos que $|A \cup B| = |A| + |B| - |A \cap B|$. Logo, temos que $|A \cup B| < |A| + |B|$. Portanto, $|A \cup B| \leq |A| + |B|$. ∎

Proposição 3.2.2 ***(Propriedades Básicas da Adição de Cardinais).***

(i) *(Associativa).* $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$

(ii) *(Comutativa).* $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$.

(iii) *A relação de ordem para adição.* $\mathfrak{a} \geq \mathfrak{b} \Leftrightarrow$ *existe um* $\mathfrak{c}$ *tal que* $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$.

(iv) *Monotonicidade da adição.* $\mathfrak{a} \leq \mathfrak{b}$ *e* $\mathfrak{c} \leq \mathfrak{d} \Rightarrow \mathfrak{a} + \mathfrak{c} \leq \mathfrak{b} + \mathfrak{d}$.

Prova. (i) Sejam A, B e C conjuntos tais que $|A| = \mathfrak{a}$, $|B| = \mathfrak{b}$ e $|C| = \mathfrak{c}$. Sabemos que $A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C)$. Isto posto, pela definição 3.2.1, temos que $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$. ∎

Prova. (ii) Existem conjuntos A e B tais que $|A| = \mathfrak{a}$ e $|B| = \mathfrak{b}$. Temos que $|A \cup B| = \mathfrak{a} + \mathfrak{b}$, e $|B \cup A| = \mathfrak{b} + \mathfrak{a}$. Mas, sabemos que $A \cup B = B \cup A$. Portanto, $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$. ∎

Prova. (iii) Sejam A e B conjuntos tais que $|A| = \mathfrak{a}$ e $|B| = \mathfrak{b}$. Como $\mathfrak{a} \geq \mathfrak{b}$, temos que $|B| \leq |A|$. Consideremos um conjunto X, $X \subseteq A$ tal que $|B| = |X|$. Daí, temos

$|X| = |B| = \mathfrak{b}$. Tomemos um conjunto C tal que $C = A - X$. Logo, $A = X \cup C$ e $X \cap C = \emptyset$, onde $|A| = |X| + |C|$. Fazendo $|C| = \mathfrak{c}$, temos que $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$. ■

Prova. (iv) Sejam A, B, C e D conjuntos tais que $|A| = \mathfrak{a}, |B| = \mathfrak{b}$, $|C| = \mathfrak{c}$ e $|D| = \mathfrak{d}$. Assumamos que os conjuntos B e D são disjuntos, isto é $B \cap D = \emptyset$, e além disso, $A \subseteq B$ e $C \subseteq D$. Temos que $|A| \leq |B|$, o que nos permite afirmar que o conjunto A possui a mesma cardinalidade de algum subconjunto de B. Podemos substituir A por este subconjunto, desde que ele possua cardinalidade $\mathfrak{a}$. O mesmo se aplica para o conjunto C. Se $A \cap C = \emptyset$ e $B \cap D = \emptyset$, temos que $|A \cup C| = \mathfrak{a} + \mathfrak{c}$ e $|B \cup D| = \mathfrak{b} + \mathfrak{d}$ e se $A \subseteq B$ e $C \subseteq D$, onde $A \cup C \subseteq B \cup D$, temos $\mathfrak{a} + \mathfrak{c} \leq \mathfrak{b} + \mathfrak{d}$. ■

Observação 3.2.1 *A operação de adição de números naturais coincide com a operação de adição dos cardinais. Em particular, a soma de dois quaisquer números cardinais finitos é um número cardinal.*

Proposição 3.2.3 *Para todo cardinal finito n, temos que $\aleph_0 + n = \aleph_0$.*

Prova. Uma vez que n é finito, temos que $n < \aleph_0$. Portanto, existe um cardinal $\mathfrak{c}$ tal que $\aleph_0 = n + \mathfrak{c}$. Logo, $\mathfrak{c} = \aleph_0$ ou $\mathfrak{c}$ é um cardinal finito. Se $\mathfrak{c}$ era um cardinal finito, então também $n + \mathfrak{c}$ era finito, o que contradiz $n + \mathfrak{c} = \aleph_0$. Portanto, $\mathfrak{c} = \aleph_0$ e temos que $n + \aleph_0 = \aleph_0$. ■

Proposição 3.2.4 *Para todo cardinal $\mathfrak{a} \geq \aleph_0$ e para todo cardinal finito n, temos que $\mathfrak{a} + \mathfrak{n} = \mathfrak{a}$. Em particular, $\aleph_\alpha + n = \aleph_\alpha$.*

Prova. Se $\mathfrak{a} \geq \aleph_0$, então existe um cardinal $\mathfrak{c}$ tal que $\mathfrak{a} = \aleph_0 + \mathfrak{c}$ e portanto $\mathfrak{a} + n = (\aleph_0 + \mathfrak{c}) + n = (\mathfrak{c} + \aleph_0) + n = \mathfrak{c} + (\aleph_0 + n) = \mathfrak{c} + \aleph_0 = \mathfrak{a}$. ■

Proposição 3.2.5 *Para todo cardinal $\mathfrak{a}, \mathfrak{a} + 1 = \mathfrak{a}$ se e somente se $\mathfrak{a} \geq \aleph_0$.*

Prova. Se $\mathfrak{a} \geq \aleph_0$ então $\mathfrak{a} + 1 = \mathfrak{a}$. Por outro lado, se $\mathfrak{a} + 1 = \mathfrak{a}$, seja A um conjunto de cardinalidade $\mathfrak{a}$ e b um elemento tal que $b \notin A$. Isto posto, $|A \cup \{b\}| = |A| + |\{b\}| = \mathfrak{a} + 1 = \mathfrak{a} = |A|$. Consequentemente, $A \cup \{b\}$ é equipotente ao próprio subconjunto A, o que implica que A é um conjunto infinito e, portanto, $\mathfrak{a} = \mathfrak{a} + 1 = |A \cup \{b\}| \geq \aleph_0$. ■

Observação 3.2.2 *O teorema 3.2.1 não será provado por conter, em sua demonstração, conhecimentos relevantes à teoria dos números ordinais, conteúdo este que não faz parte do nosso trabalho.*

Teorema 3.2.1 ***(Hessemberg) ([5], teorema 3.13, p.94)*** $\aleph_\alpha + \aleph_\alpha = \aleph_\alpha$.

Observação 3.2.3 *O teorema 3.2.1 é mais geral do que o teorema 3.2.2. No entanto, podemos provar o teorema 3.2.2 utilizando os conceitos adquiridos nesse texto.*

Teorema 3.2.2 $\aleph_0 + \aleph_0 = \aleph_0$.

Prova. Sejam $\mathbb{N}_p$ e $\mathbb{N}_i$, respectivamente, os conjuntos dos números naturais pares e números naturais ímpares. Então, $\mathbb{N}_p$ e $\mathbb{N}_i$ são subconjuntos enumeráveis, disjuntos e a união deles é $\mathbb{N}$. Consequentemente, pela definição 3.1.1, $\aleph_0 + \aleph_0 = |\mathbb{N}_p| + |\mathbb{N}_i| = |\mathbb{N}_p \cup \mathbb{N}_i| = |\mathbb{N}| = \aleph_0$. ■

Proposição 3.2.6 $\aleph_\alpha + \aleph_\beta = \aleph_{max(\alpha,\beta)}$.

Prova. Assumamos, sem perda de generalidade, que $\alpha \geq \beta$. Então, temos que $\aleph_\alpha \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\alpha + \aleph_\alpha = \aleph_\alpha = \aleph_{max(\alpha,\beta)}$. ■

Lema 3.2.1 *Se A, B, C e D são conjuntos tais que $A \sim C, B \sim D$ então $A \times B \sim C \times D$.*

Prova. Como $A \sim C$, seja f uma função bijetiva tal que $f : A \to C$ e também sabendo que $B \sim D$, seja g uma função bijetiva tal que $g : B \to D$. Daí, definindo uma função $h : A \times B \to C \times D$ por $h(a, b) = (f(a), g(b))$, verifica-se que h é bijetiva. ■

3.2.2 Multiplicação de Cardinais

Definição 3.2.2 *Dados dois cardinais $\mathfrak{a}$ e $\mathfrak{b}$ tais que $|A| = \mathfrak{a}$ e $|B| = \mathfrak{b}$, temos que $|A \times B| = \mathfrak{a} \cdot \mathfrak{b}$ (ou $\mathfrak{ab}$). Esta multiplicação de cardinais é única.*

Suponhamos agora, que existam conjuntos C e D tais que $|C| = \mathfrak{a}, |D| = \mathfrak{b}$ e $|C \times D| = \mathfrak{c}'$. Temos que $A \sim C$ e $B \sim D$. Logo, por causa do lema 3.1.1, $C \times D \sim A \times B$ e $|C \times D| \sim |A \times B|$. Portanto, concluímos que $\mathfrak{c} = \mathfrak{c}'$.

Para ver que a definição acima é independente da escolha dos representantes A e B, sejam C e D conjuntos tais que $A \sim C$ e $B \sim D$. Então, temos que $A \times B \sim C \times D$ e, portanto, $|A \times B| = |C \times D|$. Esta definição dá a resposta que esperamos quando $\mathfrak{a}$ e $\mathfrak{b}$ são números cardinais finitos. Como a multiplicação dos números naturais é bastante familiar, nosso interesse principal aqui é o produto de números cardinais transfinitos, e o produto de um número cardinal finito por um número cardinal transfinito.

Proposição 3.2.7 ***(Propriedades Básicas da Multiplicação de Cardinais).***

(i) *Associativa.* $\mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c}) = (\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c}$.

(ii) *Comutativa.* $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a}$.

(iii) *Distributividade da multiplicação em relação à soma.* $\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}$.

(iv) *Monotonicidade da multiplicação.* $\mathfrak{a} \leq \mathfrak{b}$ *e* $\mathfrak{c} \leq \mathfrak{d} \Rightarrow \mathfrak{a} \cdot \mathfrak{c} \leq \mathfrak{b} \cdot \mathfrak{d}$.

Prova. (i) Sejam A, B e C conjuntos tais que $|A| = \mathfrak{a}, |B| = \mathfrak{b}$ e $|C| = \mathfrak{c}$. Como $(A \times B) \times C = A \times (B \times C)$, temos que $(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c})$. ■

Prova. (ii) Sejam A e B conjuntos tais que $|A| = \mathfrak{a}, |B| = \mathfrak{b}$. Como $A \times B \sim B \times A$, temos que $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a}$. ■

Prova. (iii) Sejam A, B e C conjuntos tais que $|A| = \mathfrak{a}, |B| = \mathfrak{b}$ e $|C| = \mathfrak{c}$. Como $A \times (B \cup C) = (A \times B) \cup (A \times C)$, temos que $\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}$. ■

Prova. (iv) Sejam A, B, C e D conjuntos tais que $|A| = \mathfrak{a}, |B| = \mathfrak{b}$, $|C| = \mathfrak{c}$ e $|D| = \mathfrak{d}$. Utilizaremos a mesma ideia da prova da proposição 3.1.2 (iv). Podemos assumir que $A \subseteq B$ e $C \subseteq D$. Consequentemente, teremos $A \times C \subseteq B \times D$, onde $|A \times C| \leq |B \times D|$. Isto posto, temos $|A \times C| = \mathfrak{a} \cdot \mathfrak{c}$ e $|B \times D| = \mathfrak{b} \cdot \mathfrak{d}$. Portanto, obtemos $\mathfrak{a} \cdot \mathfrak{c} \leq \mathfrak{b} \cdot \mathfrak{d}$. ■

Observação 3.2.4 *Se m e n são dois números cardinais finitos então mn é também um cardinal finito. Sobre os cardinais finitos a operação da multiplicação de cardinais é a multiplicação usual dos números naturais, uma vez que satisfaça a definição recursiva, isto é, $m \cdot 0 = 0$, e $m(n+1) = mn + m$.*

Observação 3.2.5 *O corolário 3.2.1 não será provado por conter, em sua demonstração, conhecimentos relevantes à teoria dos números ordinais, conteúdo este que não faz parte do nosso trabalho.*

Corolário 3.2.1 ***(Hessemberg) ([5], corolário 3.23, p.97)*** $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$.

Observação 3.2.6 *Temos que o corolário 3.2.1 é mais geral do que o corolário 3.2.2 porém, utilizando os resultados desse texto, este corolário pode ser perfeitamente provado.*

Corolário 3.2.2 $\aleph_0 \cdot \aleph_0 = \aleph_0$.

Prova. Como $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, pelo teorema 2.3.4, temos que $\aleph_0 \cdot \aleph_0 = \aleph_0$. ■

Corolário 3.2.3 $\aleph_\alpha \cdot \aleph_\beta = \aleph_{max(\alpha,\beta)}$

Prova. Assumamos, sem perda de generalidade, que $\alpha \leq \beta$. Temos que $\alpha_\beta = 1 \cdot \alpha_\beta \leq \aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta$, portanto, $\aleph_\alpha \cdot \aleph_\beta = \aleph_{max(\alpha,\beta)}$. ■

Proposição 3.2.8 *Se n é um cardinal finito e $n > 0$, então $n \cdot \aleph_\alpha = \aleph_\alpha$*

Prova. $\aleph_\alpha = 1 \cdot \aleph_\alpha \leq n \cdot \aleph_\alpha \leq \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$, portanto, $n \cdot \aleph_\alpha = \aleph_\alpha$. ■

3.2.3 Exponenciação de Números Cardinais

Definição 3.2.3 *Dados dois conjuntos A e B, definamos* $A^B = \{f; f : B \to A\}$.

Definição 3.2.4 *Dados dois cardinais $\mathfrak{a}$ e $\mathfrak{b}$ tais que $|A| = \mathfrak{a}$ e $|B| = \mathfrak{b}$, temos que $|A^B| = \mathfrak{a}^{\mathfrak{b}}$. Esta exponenciação de cardinais é única.*

Proposição 3.2.9 ***(Propriedades Básicas da Exponenciação de Cardinais)***

(i) $\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}} \cdot \mathfrak{a}^{\mathfrak{c}}$.

(ii) $\left(\mathfrak{a}^{\mathfrak{b}}\right)^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}\mathfrak{c}}$.

(iii) $(\mathfrak{a} \cdot \mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{c}}$.

(iv) $\mathfrak{a} \leq \mathfrak{b}$ *e* $\mathfrak{c} \leq \mathfrak{d} \Rightarrow \mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{d}}$.

Prova. (i) Sejam A, B e C conjuntos tais que $|A| = \mathfrak{a}, |B| = \mathfrak{b}$ e $|C| = \mathfrak{c}$ e $B \cap C = \emptyset$. Sabemos que $|B \cup C| = \mathfrak{b} + \mathfrak{c}$. É suficiente mostrar que os conjuntos $A^B \times A^C$ e $A^{B \cup C}$ são equipotentes. Com este propósito, associamos a cada par (f, g) de funções $f \in A^B$ e $g \in A^C$ a função $f \cup g \in A^{B \cup C}$ **(ver [5], p.28, proposição 6.17 e p.31, proposição 6.30)**. Esta associação estabelece uma equipotência entre os conjuntos $A^B \times A^C$ e $A^{B \cup C}$. Isto posto, $\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}} \cdot \mathfrak{a}^{\mathfrak{c}}$. ■

Prova. (ii) Sejam A, B e C conjuntos com cardinais $\mathfrak{a}, \mathfrak{b}$ e $\mathfrak{c}$, respectivamente. A proposição estará provada se estabelecermos que $A^{B \times C} \sim (A^B)^C$. Antes de mostrarmos a equipotência, necessitamos, primeiramente, de uma notação convencional: Para uma função dada $f : B \times C \to A$ e um elemento dado $a \in C$, existe uma função $f^a : B \to A$ definida por $f^a(b) = f(b, a)$ para todo $b \in B$. A função $g : A^{B \times C} \to (A^B)^C$, que associa a cada $f \in A^{B \times C}$ a função $h \in (A^B)^C$, dada por $h(a) = f^a$ para todo $a \in C$ é uma bijeção. ■

Prova. (iii) Sejam A, B e C conjuntos com números cardinais $\mathfrak{a}, \mathfrak{b}$ e $\mathfrak{c}$, respectivamente. A função $F : (A \times B)^C \to A^C \times B^C$, que emparelha cada função $f : C \to A \times B$ com a função $(f_A \circ f, f_B \circ f)$ em $A^C \times B^C$ é bijetiva. Isto posto, $(\mathfrak{a} \cdot \mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{c}}$. ■

Prova. (iv) Sejam A, B, C e D conjuntos com cardinalidade $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ e $\mathfrak{d}$, respectivamente, cujas potências são iguais as potências dos seus cardinais. Como $\mathfrak{a} \leq \mathfrak{b}$ e $\mathfrak{c} \leq \mathfrak{d}$, podemos assumir que $A \subseteq B$ e $C \subseteq D$. Pela definição 3.1.3, temos que $|A^C| = \mathfrak{a}^{\mathfrak{c}}$ e $|B^D| = \mathfrak{b}^{\mathfrak{c}}$. Como $A \subseteq B$, podemos afirmar que $A^C \subseteq B^C$, o que nos dá que $\mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{c}}$. Se $\mathfrak{c} = \mathfrak{d}$, é imediato que $\mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{d}}$. Se $\mathfrak{c} \neq \mathfrak{d}$, como $\mathfrak{a} \leq \mathfrak{b}$ e $\mathfrak{c} \leq \mathfrak{d}$, temos $\mathfrak{d} \geq \mathfrak{c}$ e, pela proposição 3.1.2 (iii), existe um número cardinal $\mathfrak{p}$ tal que $\mathfrak{d} = \mathfrak{c} + \mathfrak{p}$, onde podemos escrever que $\mathfrak{b}^{\mathfrak{d}} = \mathfrak{b}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{p}}$, em que $\mathfrak{b}^{\mathfrak{d}} \geq \mathfrak{b}^{\mathfrak{c}}$. Portanto, $\mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{c}}$ e $\mathfrak{b}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{d}} \Rightarrow \mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{d}}$. ■

Observação 3.2.7 *Se m e n são números cardinais finitos então m^n é um cardinal finito. Nos cardinais finitos a operação de exponenciação cardinal é a exponenciação usual dos números naturais, desde que satisfaça a definição recursiva, isto é, $m^0 = 1, m^{n+1} = m^n \cdot m$.*

Proposição 3.2.10 *Para todo cardinal finito $n > 0$, temos que $\aleph_\alpha \cdot \aleph_\alpha^n = \aleph_\alpha$.*

Prova. Por indução em n. Fazendo $n = 1$, pelo corolário 3.2.1 temos que

$$\aleph_1 \cdot \aleph_1 = \aleph_1.$$

Suponhamos agora que a igualdade seja verdadeira para $n = k$. Temos que

$$\aleph_\alpha \cdot \aleph_\alpha^k = \aleph_\alpha.$$

Para $n = k + 1$, obtemos

$$\aleph_\alpha \cdot \aleph_\alpha^{k+1} = \aleph_\alpha \cdot \aleph_\alpha^k \cdot \aleph_\alpha.$$

Como supomos que para $n = k$ a igualdade é verdadeira e, mais uma vez, pelo corolário 3.2.1, podemos escrever

$$\aleph_\alpha \cdot \aleph_\alpha^{k+1} = \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha,$$

o que conclui a nossa prova. ■

Corolário 3.2.4 *Para todo cardinal $\mathfrak{a}$, temos que $\mathfrak{a} < 2^{\mathfrak{a}}$.*

Prova. Selecionamos A tal que $|A| = \mathfrak{a}$. Então, $|\{\emptyset, \{\emptyset\}\}^A| = 2^{\mathfrak{a}}$. Além disso, $\wp(A) \sim \{\emptyset, \{\emptyset\}\}^A$ e, $A \prec \wp(A)$, de onde $A \prec \{\emptyset, \{\emptyset\}\}^A$. Portanto, $\mathfrak{a} < 2^{\mathfrak{a}}$. ■

Proposição 3.2.11 *Se $n \geq 2 \Rightarrow n^{\aleph_\alpha} = 2^{\aleph_\alpha}$ tal que $\beta \leq \alpha \Rightarrow {\aleph_\beta}^{\aleph_\alpha} = 2^{\aleph_\alpha}$.*

Prova. Se $n \geq 2$ e $\beta \leq \alpha$ então $2^{\aleph_\alpha} \leq n^{\aleph_\alpha} \leq \aleph_\beta^{\aleph_\alpha}$, pela monotonicidade da exponenciação, temos que $2^{\aleph_\alpha} \leq (2^{\aleph_\alpha})^{\aleph_\alpha}$, desde que $\aleph_\beta \leq \aleph_\alpha \leq 2^{\aleph_\alpha}$. Isto posto, temos que $2^{\aleph_\alpha} \leq 2^{\aleph_\alpha \cdot \aleph_\alpha} = 2^{\aleph_\alpha}$. Portanto, todas estas desigualdades são igualdades, e nossa proposição se verifica. ■

3.3 Outros Resultados Envolvendo Aritmética Cardinal

Teorema 3.3.1 $2^{\aleph_0} = \aleph_1$.

Prova. Usando o Teorema de Cantor-Schroder-Bernstein, visto no capítulo 2 deste trabalho, é suficiente mostrarmos que $2^{\aleph_0} \leq \aleph_1$ e $2^{\aleph_0} \geq \aleph_1$. Note que $\aleph_0 = |\mathbb{Q}|$, o que implica dizer que $2^{\aleph_0} = |\wp(\mathbb{Q})|$. Considere $f : \mathbb{R} \to \wp(\mathbb{Q})$, definida por $f(a) = \{x \in \mathbb{Q}; x < a\} \subset \mathbb{Q}$, para cada $a \in \mathbb{R}$. Se a e b são números reais distintos, podemos supor que $a < b$. Logo, existe $r \in \mathbb{Q}$, tal que $a < r < b$, o que implica que $r \in f(b)$ e $r \notin f(a)$, o que mostra que $f(a) \neq f(b)$, Consequentemente, f é uma função injetiva. Isto posto, $\aleph_1 = |\mathbb{R}| \leq |\wp(\mathbb{Q})| = 2^{\aleph_0}$. Por outro lado, a função $g : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$, definida por $g(h) = 0, h(0)h(1)h(2)... \in \mathbb{R}$ é injetiva, o que mostra que $2^{\aleph_0} \leq \aleph_1$, como queríamos. ■

Corolário 3.3.1 $\aleph_0 < \aleph_1$.

Prova. Pelo Teorema de Cantor, temos que $\aleph_0 < |\wp(\mathbb{N})| = 2^{|\mathbb{N}|} = 2^{\aleph_0} = \aleph_1$. ■

Corolário 3.3.2 *Considere os conjuntos $\mathbb{R}$ e $X = \{x_1, x_2, ..., x_n\}$. Se $Y = \mathbb{R} - X$, então $|Y| = |\mathbb{R}|$.*

Prova. Seja $|Y| = a$. Como $\mathbb{R} = Y \cup X$ e $Y \cap X = \emptyset$ segue que $\aleph_1 = |\mathbb{R}| = |Y \cup X| = a + n = a$ **(ver proposição 3.2.4, p. 32)**. ■

Proposição 3.3.1 *A cardinalidade do conjunto dos números irracionais é maior do que $\aleph_0$, ou seja $|\mathbb{I}| > \aleph_0$.*

Prova. Escrevemos $\mathbb{I} = \mathbb{R} - \mathbb{Q}$. Por absurdo, suponhamos que $|\mathbb{R} - \mathbb{Q}| = \aleph_0$. Como $\mathbb{R} = (\mathbb{R} - \mathbb{Q}) \cup \mathbb{Q}$ é uma união disjunta, temos que $|\mathbb{R}| = |\mathbb{R} - \mathbb{Q}| + |\mathbb{Q}| \leq \aleph_0 + \aleph_0 = \aleph_0$, ou seja, teríamos que $|\mathbb{R}| \leq \aleph_0$, o que gera um absurdo. Portanto, concluímos que $|\mathbb{I}| > \aleph_0$. ■

Proposição 3.3.2 *Se A é um subconjunto enumerável de B e $|B| = \aleph_1$ então, $|B - A| = \aleph_1$.*

Prova. Podemos assumir, sem perda de generalidade, que $B = \mathbb{R} \times \mathbb{R}$. Seja $P = \{x \in \mathbb{R}; (x, y) \in A\}$ para algum $y \in \mathbb{R}$. Temos que $|P| \leq |A|$. Como A é enumerável, então $|A| = \aleph_0$ e temos que $|P| \leq \aleph_0$. Assim, existe $x_0 \in \mathbb{R}$ tal que $x_0 \notin P$. Logo $X = \{x_0\} \times \mathbb{R}$ é disjunto de A, ou seja, está contido em $(\mathbb{R} \times \mathbb{R}) - A$. Além disso temos que $|X| = |\mathbb{R}|$, de onde concluímos que $\aleph_1 \leq |(\mathbb{R} \times \mathbb{R}) - A|$. Isto posto, $|B - A| = \aleph_1$. ■

Cantor provou que podem existir infinitos cardinais transfinitos, muito maiores que a cardinalidade do conjunto dos números reais. Para qualquer conjunto não vazio A, $|A| < |\wp(A)|$, o que nos permite afirmar que $\aleph_1 < |\wp(\mathbb{R})| = \aleph_2$, onde $\aleph_2 = 2^{\aleph_1}$. Obtemos, assim um novo cardinal transfinito estritamente superior aos anteriores.

$\aleph_2$ é o cardinal de, por exemplo, o conjunto de todas as funções reais de variável real. Pelo que foi apresentado, podemos construir uma sucessão de cardinais transfinitos $\aleph_1 < \aleph_2 < \aleph_3 < ....$

A partir do Teorema de Cantor, concluímos que $\aleph_0 < 2^{\aleph_0}$. Assim, o conjunto $\wp(\mathbb{N})$, cuja cardinalidade é $2^{\aleph_0}$ não é enumerável. Isso significa que enquanto $\mathbb{N}$ é infinito e enumerável, o conjunto $\wp(\mathbb{N})$ tem uma quantidade muito maior de elementos, ele é infinito e não enumerável.

O teorema também indica que $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < 2^{2^{2^{\aleph_0}}} < ...$, ou seja, existem infinitos cardinais transfinitos. Mais formalmente, pode-se definir a sequência (c_n) tal que $c_1 = \aleph_0$ e para cada n natural, $c_{n+1} = 2^{cn} > c_n$.

Apêndice A

Um Breve Comentário Sobre a Hipótese do Contínuo

Este apêndice foi elaborado a partir das seguintes referências bibliográficas: [2], [10].

A matemática é hoje um domínio do conhecimento altamente sofisticado onde se descrevem estruturas extremamente complexas. O conjunto dos números reais não é um representante dessa extrema complexidade. Seria pois de esperar que uma teoria como a teoria dos conjuntos, que é suficientemente poderosa para formalizar a matemática, pudesse decidir a questão $\mathfrak{c} = \aleph_1$.

Já vimos que $|\mathbb{R}| > \aleph_0 = |\mathbb{N}|$. Cantor acreditou que se poderia demonstrar que não existem cardinalidades intermediárias entre $\mathfrak{c}$ e $\aleph_0$, o que corresponde a afirmar que $\mathfrak{c} = \aleph_1$. É claro que $2^{\aleph_0}$ que é o cardinal do conjunto das funções $f : \mathbb{N} \to 2 = \{0, 1\}$ (que pode ser visto como o conjunto das representações biádicas dos reais no intervalo $(0, 1)$) coincide com $\mathfrak{c}$. Mas isto não resolve a questão original, apenas permite escrevê-la de outra forma, ou seja: $2^{\aleph_0} = \aleph_1$.

A convicção de Cantor alimenta a denominada *hipótese do contínuo* ou seja, $2^{\aleph_0} = \aleph_1$, ou seja, não existe nenhum conjunto A com a propriedade $\aleph_0 < |A| < \aleph_1$. Ele dedicou enormes esforços tentando provar ou refutar esta conjectura. Por várias vezes chegou a anunciar tê-la provado, mas, invariavelmente, descobria algum erro nas suas deduções. Em 1884, numa carta enviada a **Mittag Leffler** (1846-1927), ele refere ter encontrado uma *demonstração rigorosa* de que o contínuo não tem a cardinalidade $\aleph_1$ (ou seja a hipótese do contínuo seria falsa). Contudo, passado um dia depois desta declaração, Cantor voltou a escrever a Mittag Leffler dando conta da descoberta de um erro na sua *prova* e de sua intenção de voltar a estabelecer a veracidade da hipótese do contínuo.

A ideia de Cantor consistia em provar que, dado um subconjunto $X \subset \mathbb{R}$, se tem $|X| \leq |\mathbb{N}|$ ou $|X| = |\mathbb{R}|$, ou seja, que não existem cardinalidades intermediárias entre

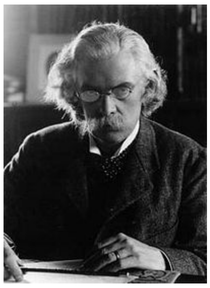

Figura A.1: Mittag Leffler

$|\mathbb{N}|$ e $|\mathbb{R}|$. Deste modo, $|\mathbb{R}|$ teria que ser o primeiro cardinal maior que $\aleph_0$. Cantor foi assim conduzido a uma tentativa de caracterizar a estrutura dos conjuntos dos reais. A sua abordagem levou-o a considerar caracterizações topológicas.

Uma noção básica, neste contexto é a de *conjunto aberto*. Um subconjunto $X \subset \mathbb{R}$ é *aberto* se, dado um elemento $a \in X$, podemos considerar um real $\epsilon > 0$ tal que $(a - \epsilon, a + \epsilon) \subset X$. O intervalo aberto $(a - \epsilon, a + \epsilon)$ é chamado de *vizinhança aberta* de a com raio ϵ e denota-se por $V_\epsilon(a)$. Um subconjunto $X \subset \mathbb{R}$ se diz *fechado* se o seu complementar em $\mathbb{R}$ for aberto.

Por outro lado, um *ponto de acumulação* de um conjunto $X \subset \mathbb{R}$ é um real a tal que, para qualquer $\epsilon > 0$, a vizinhança $V_\epsilon(a)$ contém pontos de X diferentes de a. Se $a \in X$ não for um ponto de acumulação de X, diz-se que é um *ponto isolado* de X.

Definição A.0.1 *Um subconjunto $P \subset \mathbb{R}$ é chamado perfeito se é fechado e não tem pontos isolados.*

Nem todo conjunto fechado é perfeito (por exemplo, $\{0\}$ é fechado e não é perfeito, uma vez que 0 é um ponto isolado). Mas, todo o conjunto fechado de cardinalidade superior a $\aleph_0$ é da forma $P \cup S$ onde P é perfeito e $|S| \leq \aleph_0$ (Teorema de Cantor-Bendixon).

Teorema A.0.2 *Se P é um conjunto perfeito, então $|P| = |\mathbb{R}|$.*

Estas considerações nos permitem explicar por que razão a hipótese do contínuo se impôs tão fortemente a Cantor. Não é difícil observar que a maior parte dos conjuntos considerados na prática da análise matemática ou são *enumeráveis*, isto é, possuem cardinalidade não superior à dos naturais ou são intervalos, ou se obtém de um destes dois tipos usando as operações comuns na teoria dos conjuntos, como são as uniões, as interseções ou o complementar.

Assim, se procurarmos conjuntos de algum modo *relevantes* na prática dessa análise, temos que procurar conjuntos que fazem parte de um certo *universo* de subconjuntos de $\mathbb{R}$ que é fechado para a realização daquelas operações e contém os objetos básicos mencionados. Em termos abstratos, esse *universo* possui a estrutura daquilo que se designa por *σ-álgebra de conjuntos.*

Definição A.0.2 *Uma família $\mathcal{A}$ de subconjuntos de $\mathbb{R}$ diz-se uma σ-álgebra, se $\mathcal{A} \neq 0$ e:*

(1) se $A, B \in \mathcal{A}$ então, $A \cap B = \mathcal{A}$;

(2) se $A, B \in \mathcal{A}$ então, $A \cup B = \mathcal{A}$;

(3) se $A \in \mathcal{A}$ então, $\mathbb{R} - A \in \mathcal{A}$;

(4) se $\{A_n; n \in \mathbb{N}\} \subset \mathcal{A}$ então

$$\bigcap_{n\in\mathbb{N}} A_n \in \mathcal{A} \text{ e } \bigcup_{n\in\mathbb{N}} A_n \in \mathcal{A}$$

Recorrendo a esta noção podemos caracterizar mais precisamente o *universo* a que anteriormente citamos: trata-se da menor σ-álgebra de subconjuntos de $\mathbb{R}$ que contém os conjuntos abertos. Essa σ-álgebra é conhecida como *álgebra dos conjuntos borelianos.* Podemos também agora ter uma noção mais exata da razão que levou Cantor a considerar a hipótese do contínuo como um teorema que poderia ser demonstrado. A razão é que entre os borelianos não se pode encontrar nenhum contra-exemplo para a hipótese do contínuo, por que qualquer destes conjuntos é enumerável ou contém um subconjunto perfeito. Isso mostra que um eventual contra-exemplo escaparia à prática matemática corrente e seria, de certa forma, *pouco natural.*

Os borelianos são conjuntos *simples*, no sentido em que cada um possui uma espécie de história, que é neste caso uma sequência de operações que descreve como cada boreliano se obtém a partir de conjuntos abertos.

Uma questão intimamente relacionada ao problema do contínuo, citado habitualmente como problema do contínuo generalizado, é o seguinte: Existe algum número cardinal que está estritamente entre um número cardinal transfinito $\mathfrak{a}$ e $2^{\mathfrak{a}}$? Esta questão também não foi respondida. A conjetura de que não existe um tal número cardinal é chamada *hipótese do contínuo generalizada.*

Hipótese do Contínuo Generalizada. Para qualquer número transfinito $\mathfrak{a}$, não há nenhum cardinal $\mathfrak{x}$ tal que $\mathfrak{a} < \mathfrak{x} < 2^{\mathfrak{a}}$.

Logo em 1900, no Congresso Internacional de Matemáticos, em Paris, o grande matemático alemão **David Hilbert** (1862-1943) apresentou uma lista de 23 problemas matemáticos não resolvidos, sendo o primeiro deles o problema do contínuo.

Figura A.2: David Hilbert

Nenhum progresso foi feito em solucionar este problema até o ano de 1938, pois em 1939, **Kurt Gödel** (1906-1978) demonstrou que a hipótese do contínuo é consistente relativamente aos axiomas da teoria dos conjuntos. Este resultado é do mesmo tipo daqueles que estabelecem a consistência da negação do axioma das paralelas através da exibição de geometrias não euclidianas. Como é que sabemos que o axioma das paralelas não se pode provar a partir dos restantes axiomas da geometria euclidiana?

Figura A.3: Kurt Gödel

Paralelamente, podemos associar a conjuntos de axiomas estruturas que o interpretam, ou seja, no qual os axiomas são verdadeiros. Tais estruturas são denominadas *modelos* da axiomática. (Os axiomas da geometria euclidiana plana são verdadeiros se interpretarmos *ponto* como um par ordenado (x, y) de números reais e a *reta* como um conjunto de tais pares que satisfazem equações da forma $ax + by + c = 0$ (onde a e b não são simultaneamente nulos). Por outro lado, os números naturais, com a ordem usual e as operações de adição e multiplicação usuais, constituem um modelo de axiomas (de Peano) para a aritmética.

A relação entre provas e modelos é a seguinte: se θ se demonstra a partir de um conjunto de axiomas $\sigma_1, \sigma_2, ..., \sigma_n$, então θ é verdadeira em qualquer modelo de

$\sigma_1, \sigma_2, ..., \sigma_n$. Reciprocamente, graças ao Metateorema da Completude Semântica, demonstrado por Gödel, sabemos também que se uma sentença é verdadeira em todos os modelos de uma dada axiomática, então é demonstrável nessa axiomática.

Se Γ é um conjunto de sentenças (uma axiomática) e se θ é uma sentença, escrevemos $\Gamma \vdash \theta$ para indicar que existe uma prova de θ com hipóteses em Γ (isto é, usando os axiomas de Γ). Se, por outro lado, M é uma estrutura onde, uma vez interpretada, a sentença θ se mostra verdadeira, escrevemos $M \models \theta$ para indicar este fato. (Se, para qualquer sentença θ em Γ se tem $M \models \theta$, escrevemos $M \models \Gamma$). Finalmente, se σ é uma sentença e Γ é uma axiomática e se para qualquer estrutura M se tiver que $M \models \Gamma$ implica $M \models \sigma$, então escrevemos $\Gamma \models \sigma$ e dizemos que σ é consequência semântica de Γ.

Metateorema da Completude Semântica (Gödel). Se Γ é uma axiomática e σ é uma sentença, tem-se $\Gamma \vdash \sigma$ se, e somente se,

$$\Gamma \models \sigma.$$

Antes de Gödel, Cantor já havia estabelecido que os cardinais constituíam uma ordem linear e que a cardinalidade do contínuo $\mathfrak{c}$, era estritamente superior à cardinalidade dos números naturais, que era $\aleph_0$.

Cantor conjecturou que $\mathfrak{c} = \aleph_1$, ou seja, que os reais tinham a cardinalidade do segundo cardinal infinito. Por outro lado, devido ao trabalho de **von Neumann** (1903-1957), já se possuía uma boa imagem do *universo de conjuntos.*

Figura A.4: von Neumann

De fato, depois do trabalho de von Neumann ficou claro que os conjuntos se dispõem numa hierarquia cumulativa, que pode ser descrita recursivamente (nos ordinais), iterando a operação que a cada conjunto X faz corresponder o conjunto de suas partes $\wp(X) = \{A; A \subset X\}$.

Os *números ordinais* são uma extensão dos números naturais diferentes dos inteiros e dos cardinais. Como outros tipos de números, ordinais podem ser somados, multiplicados e exponenciados. Os números ordinais podem ser de dois tipos: aqueles que sucedem a outros ordinais e que, por isso, são chamados de *ordinais* *sucessores*, e que os não sucedendo a nenhum ordinal são chamados de *ordinais limite*. (Por exemplo, 4 é um ordinal sucessor. O ordinal ω é um ordinal limite). O *universo* de conjuntos usualmente denotado por V encontra-se estratificado em níveis V_α indexados nos ordinais α. Esses níveis se definem por recursão transfinita nos ordinais de acordo com o seguinte:

$$V_0 = \emptyset;\ V_{S(\alpha)} = \wp(V_\alpha);\ V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha \text{ (se } \lambda \text{ é um ordinal limite).}$$

Pode-se provar que qualquer conjunto ocorre num destes níveis, pelo que o aspecto geral de um *universo* de conjuntos se traduz no acima citado.

Acontece que a operação $\wp$ é demasiado geral e abstrata. $\wp(X)$ pode conter subconjuntos de X de tal modo abstratos e gerais que não podem ser caracterizados, nem sequer isolar um princípio formador. Esta situação configura uma operação $\wp$ que vai muito além daquilo que é exigido pela prática matemática, onde os conjuntos que utilizamos são, em geral, descritos fazendo envolver algum tipo de princípio formador, ou alguma característica de seus elementos.

Gödel decidiu então descrever uma espécie de *sub-universo* de conjuntos ao reproduzir a hierarquia vista anteriormente, mas utilizando dessa vez uma operação mais fraca da operação $\wp$ que iremos denotar por $\mathcal{D}$. Vamos considerar, que $\mathcal{D}(X)$ é formado pelos subconjuntos de X cujos elementos são *descritíveis* usando a operação X. A definição do *novo universo* (que se denota por L) é então a seguinte:

$$L_0 = \emptyset;\ L_{S(\alpha)} = \mathcal{D}(L_\alpha);\ L_\lambda = \bigcup_{\alpha<\lambda} L_\alpha \text{ (se } \lambda \text{ é um ordinal limite)}$$

Os conjuntos que surgem em algum L_α são chamados *construtíveis* e formam L, que se designa *universo construtível de Gödel*. Usando o fato de existir um controle muito maior sobre a estrutura de $\wp(X)$, quando interpretamos $\wp$ em L, Gödel conseguiu provar que naquele universo existe uma bijeção entre o conjunto dos reais construtíveis, ou seja, entre o conjunto que, do ponto de vista de L, é $\mathbb{R}$, e o ordinal que, do ponto de vista de L, é $\aleph_1$. Assim, em L, a hipótese do contínuo é verdadeira.

Apesar de notável, o resultado de Gödel apenas revela que os axiomas da teoria dos conjuntos não refutam a hipótese do contínuo. A questão de saber se aquele princípio se pode provar a partir dos axiomas permaneceu intocada. Poder-se-ia efetivamente demonstrar a hipótese do contínuo na teoria dos conjuntos? Ou, como na situação do axioma das paralelas, seria a teoria dos conjuntos incapaz de decidir aquela questão?

A resposta a estas questões teria que esperar pela década de 60 do século XX, altura em que **Paul Cohen** (1934-2007), da Stanford University, mostrou finalmente que a teoria dos conjuntos não pode provar a hipótese do contínuo. Ele obteve esta conclusão, tendo sido bem sucedido na descrição de um universo de conjuntos onde $|\mathbb{R}| \geq \aleph_2$. A técnica de Cohen, conhecida como *Forcing*, foi completamente inovadora e surpreendeu toda a comunidade matemática. Ao contrário de Gödel que procedeu à prova do seu resultado de consistência descrevendo aquilo que se designa modelo interno, ou seja, um *universo* menor com os mesmos ordinais, a técnica de Cohen lhe permitiu descrever *super-universos*, ou seja, expansões do universo original, contendo os mesmos ordinais.

Figura A.5: Paul Cohen

Basicamente, ele descreveu um processo que, dados um *universo* de conjuntos V e um conjunto G (contendo informação não disponível em V), permite obter um novo universo $V[G]$, verificando:

(1) $V \subset V[G]$;

(2) $G \in V[G]$;

(3) $V[G]$ tem os mesmos ordinais que V.

Cohen provou que a hipótese do contínuo não é verdadeira em $V[G]$. Deste modo, também a negação da hipótese do contínuo é consistente com a teoria dos conjuntos.

Referências Bibliográficas

[1] Alfonso, A. B., Nascimento, M. C., Feitosa, H. A. *Teoria dos Conjuntos: Sobre a Fundamentação Matemática e a Construção de Conjuntos Numéricos*, Rio de Janeiro: Ed. Ciência Moderna Ltda. (2011)

[2] Ávila, G. *Várias Faces da Matemática*, Segunda Edição, São Paulo: Blucher. (2010)

[3] Hefez, A. *Curso de Álgebra, volume 1*, Quarta Edição, Rio de Janeiro: IMPA. (2011)

[4] Halmos, P. *Teoria Ingênua dos Conjuntos*, São Paulo: Polígono/EDUSP. (1970)

[5] Levy, A. *Basic Set Theory*, Dover Publications. (2002)

[6] Suppes, P. *Axiomatic Set Theory*, New York: Dover Publications. (1977)

[7] Hein, N., Dadam, F. *Teoria Unificada dos Conjuntos*, Rio de Janeiro: Editora Ciência Moderna. (2009)

[8] Cantor, G. *Contributions to the Founding of the Theory of Transfinite Numbers*, Dover Publications. (1955)

[9] Figueiredo, D. G. *Números Irracionais e Transcedentes*, Rio de Janeiro: SBM. (2011)

[10] Rocha, J. *Treze Viagens pelo Mundo da Matemática*, Rio de Janeiro: SBM. (2012)

[11] Lima, E. L. *Curso de Análise; vol 1. 14. ed*, Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada. (2012)

[12] Neto, A. C. M. *Tópicos de Matemática Elementar: introdução à análise*, Rio de Janeiro: SBM. (2012)