Nivelamente Matemático [1]

Alexandre L. Madureira

Laboratório Nacional de Computação Científica—LNCC, Brasil
URL: `http://www.lncc.br/~alm`

Fundação Getúlio Vargas—FGV, Brasil

[1] 10 de maio de 2017

Resumo. Estas notas de aula são relativas ao curso de Análise I da Escola de Pós-Graduação em Economia da Fundação Getúlio Vargas (EPGE–FGV) e do Laboratório Nacional de Computação Científica (LNCC). Estas notas devem servir de apoio, e certamente não eliminam a necessidade de se usar os já clássicos, aprimorados e vários livros didáticos. Mencionamos alguns deles na biliografia.

Neste curso apresento alguns tópicos de análise que, espero, sejam úteis. Na verdade, o que eu espero mesmo é apresentar o rigor matemático aos alunos, e mostrar como este deve ser utilizado em conjunto com a intuição matemática. Minha experiência diz que os alunos do EPGE e do LNCC têm a intuição mais desenvolvida que o rigor.

Planejo discutir os seguintes tópicos:

- Os números reais e topologia em R^n
  Funções; Conjuntos finitos, infinitos, contáveis; Propriedades dos reais;
  Espaços Vetoriais; Conjuntos abertos e fechados; Vizinhanças; Teorema de Bolzano-Weierstrass;
  Conjuntos Compactos; Teorema de Heine–Borel;
- Sequências e Convergência;
  Sequências, Subsequências;
  Teorema de Bolzano-Weierstrass; Sequências de Cauchy
  Sequências Contráteis e pontos fixos de contrações; Caracterização de abertos e fechados;
  Sequências monótonas (em R); limsup, liminf;
- Funções Contínuas
  Propriedades Locais e Globais
  Preservação de Compacidade e Continuidade Uniforme
- Sequência de funções
  Convergência pontual e uniforme; Trocas de limites
  Equicontinuidade
- Diferenciabilidade
  Funções de uma variável; Derivadas parciais; Diferenciabilidade
  Regra da cadeia; Teorema de Taylor;
  Teorema da função implícita e da função inversa;
  Aplicações: Minização com restrições de igualdade e desigualdade

A referência básica é o livro *The elements of Real Analysis*, de Robert Bartle [**3**]. Outras referências importantes são os já clássicos [**10**, **18**], bem como o novo [**21**]. Para tópicos específicos em uma dimensão, pode-se ler [**4**, **9**, **20**]. Finalmente, idéias mais abstratas são apresentadas em [**11**, **19**].

Sumário

CAPíTULO 1

Uma introdução não tão formal aos fundamentos da matemática

[1]

A matemática se baseia na argumentação lógica. Outras áreas do conhecimento, talvez todas, podem também reclamar para si tal propriedade, Entretanto a matemática é o *próprio* desenvolvimento da argumentação formal, é a "lógica aplicada."

Este aspecto da matemática tem consequências interessantes; seus resultados independem da época, cultura e região em que foram gerados. O Teorema de Pitágoras, demonstrado por fanáticos matemáticos (os pitagóricos), cerca de 500 A.C., será válido em qualquer lugar e época (http://mathworld.wolfram.com/PythagoreanTheorem.html).

Outras áreas têm teorias "exatas" que são na verdade aproximações da realidade, com "validade" somente sob determinadas condições (por exemplo, teoria da relatividade versus física quântica). Mesmo certas definições podem mudar. Como exemplo, em 1997 a unidade de tempo *segundo* foi definida mais uma vez (http://en.wikipedia.org/wiki/Second). Quanto ao pobre quilograma, bem, este ainda busca uma definição adequada aos nossos tempos (http://en.wikipedia.org/wiki/Kilogram).

Parece-me desnecessário comentar sobre a volatilidade de várias teorias econômicas...

Nestes rápidos comentários que seguem, pretendo passear por alguns aspectos de como a matemática funciona. Uma ótima referência é o livro do Terence Tao [**20**].

1.1. Argumentação formal

1.1.1. Proposições. Como funciona a argumentação formal na prática? Objetos fundamentais são as *proposições* (ou expressões lógicas), que sempre são verdadeiras ou falsas, mas nunca verdadeiras *e* falsas simultaneamente. Por exemplo[2]

$$1+1=2, \tag{1.1.1}$$

$$1=2. \tag{1.1.2}$$

Vou me adiantar afirmando que (1.1.1) é verdadeira e (1.1.2) é falsa. Uma *conjectura* nada mais é que uma proposição que é ser verdadeira ou falsa (como toda proposição) mas que ainda não se tem a resposta. Por exemplo, dizer que

todo inteiro maior que 2 pode ser escrito como soma de dois números primos

é uma proposição, também conhecida como conjectura de Goldbach. Ela é verdadeira ou falsa, só que ninguém ainda sabe a resposta. Sabe-se que é verdadeira para todos os números menores que 4×10^{18}, mas não se sabe se é de fato verdadeira para *todos* os inteiros.

Exemplo 1.1. Os exemplos que não são afirmativas:

[1]Última Atualização: 23/11/2019

[2]Suponho, por enquanto, que as propriedades de conjuntos e dos números reais são conhecidas

X	Y	$X \wedge Y$
V	V	V
V	F	F
F	V	F
F	F	F

X	Y	$X \vee Y$
V	V	V
V	F	V
F	V	V
F	F	F

X	$\neg X$
V	F
F	V

TABELA 1. Tabelas verdade para operações lógicas $\wedge$, $\vee$ e $\neg$.

(1) frases sem sentido como $= 1 + 3-$ não são proposições.
(2) $1 - 4$ não é uma proposição pois não *afirma* nada, i.e., não há um verbo na frase (uma "regra" é que proposições têm verbos).
(3) $x > 4$ também não é uma proposição. De fato não há como determinar se ela é verdadeira ou falsa, pois não se sabe o valor de x. Entretanto, $x > 4$ é uma afirmação que chamamos de *predicado* e denotamos por $P(x)$. Aqui, x é uma *variável livre*, i.e., uma variável que temos quando definida torna $P(x)$ uma proposição. Uma questão importante é determinar quais os valores que x pode tomar. Neste exemplo, x poderia ser um número real, mas não um conjunto.

1.1.2. Conectivos lógicos. Proposições podem ser *negadas* ou combinadas com *ou* e *e*, gerando outras. Por exemplo, se a é um número real qualquer, então a afirmativa ($a > 0$ ou $a \leq 0$) é verdadeira, mas ($a > 0$ e $a \leq 0$) não o é.

Sejam X e Y duas proposições (ou predicados). A regra geral é que (X *e* Y) é também uma proposição denotada por $X \wedge Y$, e que só é verdadeira se X e Y forem *ambas* verdadeiras.

Similarmente, (X *ou* Y) é uma proposição denotada por $X \vee Y$ que só é falsa se X e Y forem *ambas* falsas. Note que se apenas uma das afirmativas for verdadeira, $X \vee Y$ é verdadeira. Note que esta noção pode diferir de um possível uso corriqueiro do *ou*, como na frase *ou eu, ou ele ficamos*. Neste caso quer-se dizer que ou eu fico, ou ele fica, mas não ambos — este é o chamado *ou exclusivo*[3]. Em matemática, dizer que a ou b é zero é verdade se $a = b = 0$.

Podemos também negar uma proposição X gerando a proposição "não X, denotada por $\neg X$, e onde $\neg X$ é verdadeira se X for falsa e $\neg X$ é falsa se X for verdadeira. Negar uma afirmativa pode ser útil pois para concluir que uma afirmativa Z é falsa, as vezes é mais fácil provar que $\neg Z$ é verdadeira. As regras acima são determinadas pela *tabela verdade* 1.

Considere também o exemplo a seguir.

EXEMPLO 1.2 ([**13**]). Considere as seguintes proposições
(1) $2 + 3 = 5$ and $\neg(1 + 1 = 2)$
A proposição acima é falsa pois $1+1 = 2$ ser verdadeiro torna $\neg(1+1 = 2)$ falsa.
(2) $2 + 3 = 5$ or $\neg(1 + 1 = 2)$
A proposição acima é verdadeira pois $2 + 3 = 5$ é verdadeira.

Operações lógicas podem ser combinadas. Por exemplo, se X, Y e Z são proposições, então, $\neg(X \vee Y)$ e $Z \vee \neg(X \wedge Y)$ também o são. O uso de parênteses é importante pois evita interpretações dúbias ou errôneas. Por exemplo como deve-se interpretar $X \wedge Y \vee Z$? As

[3]Outro termo matemático que pode ter sentido diferente do uso diário é *em geral*. Na matemática, em geral quer dizer *sempre*, enquanto no dia-a-dia quer dizer "quase sempre"

X	Y	$\neg X$	$\neg X$	$\neg(X \vee Y)$	$\neg X \wedge \neg Y$
V	V	F	F	F	F
F	V	V	F	F	F
V	F	F	V	F	F
F	F	V	V	V	V

TABELA 2. Tabelas verdade do Exemplo 1.3.

duas possibilidades

$$X \wedge (Y \vee Z), \qquad (X \wedge Y) \vee Z$$

parecem razoáveis e dão resultados diferentes. Entretanto $\neg X \vee Y$ deve ser interpretado como $(\neg X) \vee Y$ (e não como $\neg(X \vee Y)$. Similarmente, $\neg X \wedge Y$ significa $(\neg X) \wedge Y$.

Dizemos que duas proposições são *logicamente equivalentes* (ou simplesmente *equivalentes*) se têm a mesma tabela verdade, como ilustrado no exemplo abaixo.

EXEMPLO 1.3. As tabelas verdade de $\neg(X \vee Y)$, $\neg X \wedge \neg Y$ são dadas pela Tabela 2. Note que ambas proposições têm a mesma tabela vedade, e portanto são equivalentes.

As equivalências entre $\neg(X \vee Y)$ e $\neg X \wedge \neg Y$ como mostrado acima, e de $\neg(X \wedge Y)$ e $\neg X \vee \neg Y$ como no Exercício 1.1 são chamadas de *Regras de De Morgan*.

EXEMPLO 1.4 ([**13**]). Qual é a negação do predicado $1 \leq x < 5$? Note que esta afirmativa nada mais é que $(1 \leq x) \wedge (x < 5)$, e negá-la é portanto afirmar $\neg(1 \leq x) \vee \neg(x < 5)$, i.e., $(1 > x) \vee (x \geq 5)$. Vale observar que usamos a propriedade da *tricotomia* dos números reais.

Seguramente, este papo poderia ir bem mais longe com a álgebra de Boole ou booleana (http://en.wikipedia.org/wiki/Boolean_algebra).

1.1.3. Implicações. Os passos de uma argumentação matemática são dados via implicações, representadas pelo operador lógico $\Longrightarrow$. Se de um fato conhecido, por exemplo uma afirmativa verdadeira X, eu posso concluir uma afirmativa verdadeira Y, então eu escrevo

$$X \implies Y, \tag{1.1.3}$$

e leio X *implica* Y, ou ainda *se* X *então* Y. Dizemos que X é a *hipótese* e que Y é a conclusão.

Por exemplo

$$a > 0 \implies 2a > 0. \tag{1.1.4}$$

Abstraindo um pouco mais, note que (1.1.3) e (1.1.4) também são afirmativas. Outros exemplos de afirmativas:

$$0 = 0 \implies 0 = 0, \tag{1.1.5}$$

$$0 = 1 \implies 0 = 0, \tag{1.1.6}$$

$$0 = 1 \implies 0 = 1, \tag{1.1.7}$$

$$0 = 0 \implies 0 = 1. \tag{1.1.8}$$

As três primeiras afirmativas acima são verdadeiras. Somente a última é falsa. A primeira da lista é uma tautologia (redundância, do grego *tauto*, o mesmo), e é obviamente correta. Já a segunda é correta pois de hipóteses falsas pode-se concluir verdades (multiplique ambos os lados de (1.1.6) por zero). A terceira é verdade pois se a hipótese é verdadeira, a conclusão,

X	Y	$X \implies Y$
V	V	V
V	F	F
F	V	V
F	F	V

X	Y	$X \iff Y$
V	V	V
V	F	F
F	V	F
F	F	V

Tabela 3. Tabelas verdade para operações lógicas $\wedge$, $\vee$ e $\neg$.

sendo uma mera repetição da hipótese, também o é (este tipo de argumento é usado em demonstrações por contradição). Finalmente, (1.1.8) é falsa pois não se pode deduzir uma afirmativa falsa partindo-se de uma verdadeira.

A argumentação (e a demonstração) matemática baseia-se em supor que algumas hipóteses são verdadeiras e em concluir resultados através de implicações.

Note que a implicação não é "reversível", i.e., se $X \implies Y$, não podemos concluir que $Y \implies X$. Realmente, $1 = -1 \implies 1 = 1$ é verdadeiro, mas $1 = 1 \implies 1 = -1$ é falso.

As vezes, tanto a implicação como seu reverso valem. Se por exemplo $X \implies Y$ e $Y \implies X$ escrevemos simplesmente $X \iff Y$, e lemos X *se e somente se* Y. Confira as tabelas 3.

Em termos de linguagem, alguns cuidados têm que ser tomados, pois proposições podem ser descritas de forma "literária". Por exemplo, $X \implies Y$ pode ser descrito como

- Se X então Y
- X acontece somente se Y acontece
- X é suficiente para Y
- Y acontece se X acontece
- Y é necessária para X

De forma análoga, a proposição $X \iff Y$ pode ser dita como

- X se e somente se Y
- X é equivalente a Y
- X é necessária e suficiente a Y

Exemplo 1.5. Determine se as proposições abaixo são verdadeiras

(1) Se $1 + 1 = 3$ então $1 + 1 = 2$
 Como a hipótese é falsa, a implicação é verdadeira.
(2) n ser ímpar é necessário para n ser primo.
 A afirmativa acima pode ser reescrita como
 n primo implica em n ímpar.
 Se $n = 2$, a proposição é falsa. Ela é entretanto verdadeira para os demais inteiros positivos ($n = 3, 4, \dots$).

Finalmente, considere a implicação $X \implies Y$. Dizemos que $Y \implies X$ é sua *recíproca*, e que $\neg Y \implies \neg X$ é sua *contrapositiva*.

1.1.4. Quantificadores. Frases matemáticas $x > 3$ ou $x^2 = 1$ não são proposições mas sim predicados, como já foi discutido. Estão associados à *variàvel livre*, x, que quando fixado pode tornar o predicado uma proposição, sendo verdadeira ou falsa. Considere o predicato

$$P(x):\ x > 3,$$

onde o *conjunto universo* (ou simplesmente universo) $\mathcal{U}$ que x pode pertencer é, por exemplo, os números inteiros. Então $P(4)$ é a proposição verdadeira $4 > 3$, enquanto $P(1)$ é falsa.

Uma forma conveniente de se lidar com predicados e variáveis livres de forma é via *quantificadores*.

Definição 1.1.1. *Considere o predicado $P(x)$ indexado pela variável livre x pertencente ao conjunto universo $\mathcal{U}$. Então*

$$\text{para todo } x \in \mathcal{U},\ P(x) \tag{1.1.9}$$

é uma proposição que é verdadeira se $P(x)$ for verdade para todo $x \in \mathcal{U}$. Caso contrário, é falsa.

Da mesma forma,

$$\text{existe } x \in \mathcal{U} \text{ tal que } P(x) \tag{1.1.10}$$

é uma proposição que é verdadeira se existir ao menos um $x \in \mathcal{U}$ tal que $P(x)$ for verdade. Caso contrário, é falsa.

Na definição acima, a expressão *para todo*, também denotada pelo símbolo $\forall$, é chamada *quantificador universal*, enquanto a expressão *existe*, também denotada pelo símbolo $\exists$, é chamada *quantificador existencial*.

Note que para mostrar que (1.1.9) é falsa basta achar *um* $x \in \mathcal{U}$ tal que $P(x)$ seja falsa. Dizemos que este x é um *contra-exemplo*. Por outro lado, para motrar (1.1.10) falsa, tem que mostar que $P(x)$ falsa *para todo* $x \in \mathcal{U}$.

Exemplo 1.6. Dado o predicado

$P(n)$: n ser ímpar é necessário para n ser primo,

considere as proposições abaixo:

(1) Existe $n \in \mathbb{N}$ tal que $P(N)$.
(2) Para todo $n \in \mathbb{N}$, $P(N)$.

Bom, antes de analisar as proposições, note que o predicado pode ser escrito de forma mais direta como

$P(n)$: n primo $\implies$ n ímpar.

A proposição acima (1) é verdade pois $P(13)$ é verdade, e isto é suficiente (para mostrar existência, basta achar um exemplo). Por outro lado, (2) é falsa pois $P(2)$ é falsa (2 é primo sem ser ímpar). Logo existe um contra-exemplo: $n = 2$.

Note que o fato de (2) ser falsa depende do conjunto universo. A proposição

Para todo $n \in \mathbb{N}$ tal que $n \geq 3$, $P(N)$

é verdade.

1.1.5. Axiomas. E como começar a construção da matemática em si, i.e., quais são as hipóteses *básicas* que são necessariamente verdadeiras? Isso é importante pois, como vimos, partindo-se de hipóteses falsas pode-se chegar a conclusões falsas, *sem comprometer a lógica*. Aqui entram os *axiomas*, premissas verdadeiras consideradas "óbvias." É uma boa idéia que este conjunto de premissas seja o menor possível, i.e., um axioma do conjunto não pode ser demonstrada a partir dos outros.

A partir dos axiomas contrói-se via implicações toda uma matemática (mudando-se o conjunto de axiomas, muda-se a matemática).

Um exemplo de axioma vem a seguir.

AXIOMA 1.1.2 (do conjunto vazio). Existe um conjunto que não contém nenhum elemento.

Suponha que se possa definir o que é uma pessoa careca, e considere o seguinte axioma.

AXIOMA 1.1.3 (do fio extra). Um careca que ganhar um fio extra de cabelo continua careca.

Pode-se concluir então o seguinte resultado (tente demonstrá-lo).

Se o Axioma do fio extra vale, então todos os seres humanos são carecas.

O alerta que o resultado acima nos fornece é que devemos ter cuidado com os axiomas escolhidos. Resultados "patológicos" podem advir deles. E de fato, resultados "estranhos" permeiam a matemática...

1.1.6. Definições, lemas, teoremas. Uma das formas de se construir novos objetos matemáticos é através de *definições*. Por exemplo podemos definir o conjunto dos números naturais como $\mathbb{N} = \{1, 2, 3, \dots\}$[4]. Outro exemplo: seja

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{R} \\ x &\mapsto x^2. \end{aligned}$$

A expressão acima define uma função chamada "f" que associa a cada número inteiro o seu quadrado, levando-o nos reais.

E quanto a proposições dadas por lemas e teoremas[5]? Normalmente, lemas e teoremas são escritos à parte, sendo compostos por hipóteses, e conclusões explicitamente mencionadas.

Exemplos de lema e teorema vêm a seguir.

LEMA 1.1.4. Supondo que o Axioma do conjunto vazio vale, então existe somente um conjunto vazio.

[4] Alguns autores utilizam o símbolo := no lugar de = em definições. Esta é provavelmente uma boa idéia pouco utilizada, e eu não a seguirei.

[5] Uma dúvida comum: qual a diferença entre os três? Bom, normalmente *proposição* tem um caráter mais geral, sendo uma sentença lógica verdadeira (na matemática "usual"). Já um *lema* é proposição preliminar, que contribui na demonstração de um resultado principal, um *teorema*. Muitas vezes entretanto, o lema tem interesse próprio. Em geral, o gosto e o estilo do autor determinam o que é proposição, lema ou teorema.

TEOREMA 1.1.5 (de Fermat). [6] *Seja $n \in \mathbb{N}$, com $n > 2$. Então não existem inteiros positivos x, y, z tais que $x^n + y^n = z^n$.*

A hipótese do lema 1.1.4 é o axioma do conjunto vazio (Axioma 1.1.2), e a conclusão é de que só existe um conjunto vazio, isto é todos os conjuntos vazios são iguais. Este é um típico resultado de *unicidade*. Já no Teorema de Fermat 1.1.5, impondo-se hipóteses sobre a potência n (ser inteiro e maior que dois), obtem-se um resultado de *não existência*.

Normalmente lemas e teoremas descrevem resultados de interesse e não triviais, i.e., as conclusões não se seguem trivialmente das hipóteses. Algumas vezes entretanto casos importantes particulares são facilmente obtidos de resultados mais gerais. Estes casos particulares são chamados de *corolários*. O Teorema de Fermat por exemplo é um corolário de um outro resultado mais poderoso (chamado Teorema da Modularidade). É claro que "trivialidade" não é um conceito rigoroso e é certamente relativa.

1.1.7. Prova ou demonstração. Uma *prova* ou *demonstração* são os passos lógicos para se concluir uma proposição. Algumas demonstrações são simples, outras nem tanto. Por exemplo, a demonstração por Andrew Wiles do Teorema de Fermat fechou com chave de ouro a matemática do século XX. A prova é uma intricada sequência de resultados publicada num artigo de 109 páginas na mais conceituada revista de matemática, os Anais de Matemática de Princeton [**23**].

Antes da demonstração de Wiles, o agora "Teorema de Fermat" era "somente" uma conjectura, um resultado que acredita-se verdadeiro mas que ninguém demonstrou. Uma ainda conjectura famosa é a de Goldbach, que afirma que *todo inteiro par maior que dois pode ser escrito como a soma de dois números primos*. Para números menores que 10^{18}, o resultado foi checado computacionalmente, mas o caso geral ainda não está provado.

A demonstração por contradição segue os seguintes princípios lógicos: se queremos mostrar que uma afirmativa implica noutra, podemos simplesmente negar este fato e tentar chegar numa contradição.

Apesar de não termos ainda definido os conceitos abaixo, considere a afirmativa

$$\emptyset \subseteq A \quad \text{para qualquer conjunto } A. \tag{1.1.11}$$

Talvez uma demonstração "direta" não seja tão fácil. Mas suponha que (1.1.11) seja falso. Então existe algum conjunto A tal que $\emptyset \nsubseteq A$. Portanto existe algum elemento no conjunto vazio que não está em A. Mas isto é um absurdo, pois o vazio não contém nenhum elemento. O que se vemos é que negar (1.1.11) (afirmar que (1.1.11) é falso) nos leva a concluir um absurdo, e portanto (1.1.11) só pode ser verdade.

Outra forma de se olhar para esta demonstração [**13**] é ver que

$$x \in \emptyset \implies x \in A.$$

De fato, a afirmativa $x \in \emptyset$ é sempre falsa, e como falso implicar verdadeiro é verdadeiro, então $x \in A$ é verdade. Então, por definição, todo elemento de $\emptyset$ pertence a A.

[6] Enunciado de Fermat, na margem do livro *Arithmetica* de Diophantus: *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.* (É impossível separar um cubo em dois cubos, ou a quarta potência em quartas potências, ou em geral qualquer potência em duas potências iguais. Eu descobri uma demonstração realmente maravilhosa disto, para a qual esta margem é por demais exígua para caber.)

1.2. Exercícios

EXERCÍCIO 1.1. Sejam X e Y duas proposições. Mostre que $\neg(X \wedge Y)$ e $\neg X \vee \neg Y$ são equivalentes.

EXERCÍCIO 1.2. Mostre que

(1) $\neg(X \implies Y)$ é equivalente a $X \wedge (\neg Y)$.
(2) $X \implies Y$ é equivalente a $\neg Y \implies \neg X$.

CAPíTULO 2

Conjuntos e Funções

[1]

Esta parte do texto pretende apenas expor algumas dificuldades básicas, da parte talvez mais fundamental da matemática (excluindo-se a lógica). Duas referências também introdutórias, mas muito mais completas, são os livros do Terence Tao [**20**], e do Paul Halmos [**12**].

A primeira dificuldade encontrada é definir o que é um conjunto. Uma saída (questionável) é simplesmente dizer que um conjunto é uma "coleção" ou família de objetos (ou elementos ou membros). Se um objeto x faz parte de um conjunto A, dizemos que ele pertence à A e escrevemos $x \in A$ (o símbolo $\notin$ indica que quando um elemento não pertence a um conjunto).

Espera-se que o uso da palavra "coleção"acima não traga confusões. O termo coleção será a seguir utilizado para conjuntos cujos elementos são também conjuntos.

Considere agora dois conjuntos A e B.

- Dizemos que A está contido em B e escrevemos $A \subseteq B$ se todo elemento de A é elemento de B. Pode-se também escrever $B \supseteq A$ (lê-se B contém A) para indicar $A \subseteq B$.
- Se A não está contido em B escrevemos $A \not\subseteq B$.
- Dizemos que dois conjuntos A e B são iguais, e escrevemos $A = B$ se $A \subseteq B$ e $B \subseteq A$.
- Se não forem iguais, dizemos que são diferentes e escrevemos $A \neq B$.
- Também escrevemos $A \subsetneq B$ se $A \subseteq B$ mas $A \neq B$. Dizemos neste caso que A está *propriamente* contido em B.

O seguinte axioma é importante, nos garante que a "forma usual" de definir conjuntos é "segura," ou seja, quando definimos um conjunto obtemos um e apenas um conjunto (mesmo que seja vazio).

Axioma 2.0.1 (da especificação). Seja A um conjunto, e para cada $x \in A$, seja $P(x)$ uma afirmativa (verdadeira ou falsa). Então existe um único conjunto B composto de todos os elementos x de A tais que $P(x)$ é verdade.

O conjunto acima é denotado por $\{x \in A : P(x) \text{ é verdade}\}$. Quando o conjunto A é claro pelo contexto, podemos escrever simplesmente $\{x : P(x) \text{ é verdade}\}$. Este conjunto é formado por *todos os elementos* x que estejam em A e tais que a propiedade $P(x)$ seja verdadeira. Uma última forma de denotar os conjuntos é simplesmente descrever seus elementos entre as chaves.

[1]Última Atualização: 13/08/2019

Por exemplo, o conjunto dos números pares pode ser denotado por

$$\{x \in \mathbb{Z} : x \text{ é divisível por } 2\}.$$

Sendo um pouco menos formal, pode-se escrever este mesmo conjunto como $\{2x : x \in \mathbb{Z}\}$ ou ainda enumerar todos os elementos do conjunto: $\{\dots, -4, -2, 0, 2, 4, 6, \dots\}$.

Vale aqui descrever uma situação interessante dada pelo *Paradoxo de Russel*. É natural perguntar-se o quão grande podem ser conjuntos. Por exemplo, existe um conjunto U tal que todos os conjuntos existentes sejam *elementos* de U? Se U existe, então, pelo Axioma da especificação (Axioma 2.0.1) podemos formar

$$R = \{x \in U : x \text{ é conjunto e } x \notin x\}.$$

Então $R \notin U$. De fato, se $R \in U$, então $R \in R$ ou $R \notin R$. Vamos dividir em dois casos:

(1) Se $R \in R$, então $R \notin R$ pois por definição, R é formado pelos conjuntos que *não* se autocontém.
(2) Se $R \notin R$, então R não satisfaz as propriedades que definem R. No caso de *não* se autoconter. Logo $R \in R$.

Em ambas possibilidades (1) e (2) obtemos absurdos. Logo $R \notin U$. Mas U é exatamente o conjunto que contém *todos* os outros.... Somos levados a concluir que tal conjunto U não pode existir.

O próximo passo é definir as operações usuais. Por incrível que possa parecer, o mais difícil é definir a união entre dois conjuntos, e para isto é necessário um axioma.

Axioma 2.0.2 (da união). Para qualquer coleção de conjuntos, existe um conjunto que contém todos os elementos pertencentes a pelo menos um conjunto da coleção.

Podemos agora definir a união entre dois conjuntos A e B. Para tanto, note que pelo Axioma da união, existe um conjunto U que contém todos os elementos de A e de B. Definimos então $A \cup B = \{x \in U : x \in A \text{ ou } x \in B\}$.

Observe entretanto a seguinte armadilha. O Axioma da união não garante que o tal conjunto contendo A e de B é único, somente garante que existe. Podemos ter por exemplo um outro conjunto $\hat{U}$ contendo A e de B. Seja agora $C = \{x \in \hat{U} : x \in A \text{ ou } x \in B\}$. Para a união ser definida de forma única, temos que garantir que $C = A \cup B$. Isto é verdade, e para provar basta argumentar que $C \subseteq A \cup B$ e $C \supseteq A \cup B$.

Com o Axioma da especificação, podemos definir as seguintes operações.

- O conjunto interseção entre A e B é $A \cap B = \{x \in A : x \in B\}$.
- O conjunto diferença A menos B é $A \backslash B = \{x \in A : x \notin B\}$. O conjunto resultante também denotado por $A - B$ e chamado de complemento de B em relação à A.
- Quando é claro quem é o conjunto A, denotamos $A \backslash B$ por $\mathcal{C}(B)$, e o chamamos de complemento de B.

Observação. É fácil generalizar os conceitos acima para uniões e interseções arbitrárias de conjuntos. Por exemplo, dado $n \in \mathbb{N}$ e conjuntos $A_1, \dots, A_n$, definimos

$$\cup_{i=1}^n A_i = \{x : x \in A_i \text{ para algum } i \in \{1, \dots, n\}\}.$$

Outra forma é definir $I = \{1, \dots, n\}$ e escrever

$$\cup_{i=1}^{n} A_i = \cup_{i \in I} A_i = \{x : \text{ existe } i \in I \text{ tal que } x \in A_i\}.$$

É simples generalizar o conceito acima para conjuntos $A_1, A_2, \dots$, bastando para tal considerar $I = \mathbb{N}$:

$$\cup_{i=1}^{\infty} A_i = \cup_{i \in \mathbb{N}} A_i = \{x : \text{ existe } i \in \mathbb{N} \text{ tal que } x \in A_i\}.$$

Em termos de operações entre conjuntos, é útil a regra de *De Morgam*, que diz que para conjuntos E_n, onde $n \in \mathbb{N}$, temos que

$$\mathcal{C}(\cup_{i \in \mathbb{N}} E_n) = \cap_{i \in \mathbb{N}} \mathcal{C}(E_n), \qquad \mathcal{C}(\cap_{i \in \mathbb{N}} E_n) = \cup_{i \in \mathbb{N}} \mathcal{C}(E_n). \tag{2.0.1}$$

Outro conceito útil é o de *par ordenado*. Dados dois elementos, ou objetos a e b, formamos o par (a, b), e chamamos a e b de (primeiro e segundo) componentes de (a, b). Dizemos (definimos) que um par ordenado é *igual* a outro se os respectivos componentes forem iguais, i.e., $(a, b) = (a', b')$ se $a = a'$ e $b = b'$.

Do ponto de vista axiomático, não é claro que dados dois elementos, exista o par ordenado formado por eles. Viveremos por enquanto com esta dúvida. O importante é como pares ordenados são formados (por elementos de dois conjuntos) e quando são iguais (quando os componentes são iguais).

Definimos agora *produtos cartesianos*. Dados dois conjuntos A e B, definimos o conjunto $A \times B = \{(a, b) : \ a \in A, \ b \in B\}$ como sendo o composto pelos pares ordenados.

Observação. A extensão destes conceitos para *n-úplas* ordenadas e produtos cartesianos com n conjuntos é natural.

Chamamos R de *relação entre A e B* se R é subconjunto de $A \times B$. Similarmente, dizemos que $a \in A$ e $b \in B$ são *relacionados* se $(a, b) \in \mathrm{R}$. Uma *relação binária* num conjunto A é um subconjunto $\mathrm{R} \subseteq A \times A$. Dado $a, b \in A$, denotamos $(a, b) \in \mathrm{R}$ por $a \,\mathrm{R}\, b$, e $(a, b) \notin \mathrm{R}$ por $a \not\mathrm{R}\, b$.

Exemplo 2.1. Nos reais, $=$, $\geq$, $<$, etc definem relações binárias. Considere por exemplo $A = \{1, 2, 3\}$, e defina $< \subseteq A \times A$ por $< = \{(1, 2), (1, 3), (2, 3)\}$. Então $1 < 2$, $1 < 3$ e $2 < 3$.

Definição 2.0.3. *Dizemos que uma relação R em A é:*

i) completa: para todo a, $b \in A$ tem-se $a \,R\, b$ ou $b \,R\, a$
ii) transitiva: para todo a, b, $c \in A$ tais que $a \,R\, b$ e $b \,R\, c$ tem-se $a \,R\, c$
iii) reflexiva: para todo $a \in A$ tem-se $a \,R\, a$
iv) simétrica: para todo a, $b \in A$ tais que $a \,R\, b$ tem-se $b \,R\, a$
v) assimétrica: para todo a, $b \in A$ tais que $a \,R\, b$ tem-se $b \not R\, a$
vi) antissimétrica: para todo a, $b \in A$ tais que $a \,R\, b$ e $b \,R\, a$ tem-se $a = b$

Uma *relação de equivalência* $\sim$ num conjunto A é uma relação binária reflexiva, simétrica e transitiva. Um exemplo trivial de relação de equivalência é a relação de igualdade $=$.

Exemplo 2.2. Seja $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$. Então a relação

$$(a, b) \sim (c, d) \iff ad = bc$$

é de equivalência. De fato, note que $\sim$ é

(1) reflexiva: $(a, b) \sim (a, b)$ pois $ab = ba$.

(2) simétrica: seja $(a,b) \sim (c,d)$. Então, por definição, $ad = bc$. Então $(c,d) \sim (a,b)$ pois $bc = ad$.
(3) transitiva: seja $(a,b) \sim (c,d)$ e $(c,d) \sim (m,n)$. Segue-se por definição que $ad = bc$ e $cn = dm$. Quero mostrar que $an = bm$. Mas $adn = bcn = bdm$. Como $d \neq 0$, temos que $adn = bdm$. Portanto, $(a,b) \sim (m,n)$.

Seja agora um conjunto não vazio X e $\mathcal{P}(X)$ o *conjunto das partes de* X, i.e., é a coleção contendo todos os subconjuntos de X:

$$\mathcal{P}(X) = \{A : A \subseteq X\}.$$

Dada uma relação de equivalência em X e $x \in X$, podemos definir a classe de equivalência de x como sendo

$$[x] = \{\hat{x} \in X : \hat{x} \sim x\}.$$

Denotamos o conjunto de todas as classes de equivalência de X por $X/\sim \in \mathcal{P}(X)$, onde

$$X/\sim = \{[x] : x \in X\}.$$

Uma coleção $\mathcal{T} \subset \mathcal{P}(X)$ é uma *partição* de X se

(1) $\emptyset \notin \mathcal{T}$
(2) para todo A, $B \in \mathcal{T}$, temos $A = B$ ou $A \cap B = \emptyset$
(3) para todo $x \in X$ existe conjunto $A \in \mathcal{T}$ tal que $x \in A$

Por exemplo, $\{\mathbb{R}_{<0}, \{0\}, \mathbb{R}_{>0}\}$ define uma partição de $\mathbb{R}$.

2.1. Funções

Da definição de relação vem o importante conceito de função. Uma *função entre A e B* nada mais é que uma relação entre A e B, e sendo assim $f \subseteq A \times B$. Esta relação entretanto satisfaz a seguinte restrição: para todo $a \in A$ existe um único $b \in B$ tal que $(a,b) \in f$. Denotamos esta relação especial por $f : A \to B$. Dado $a \in A$, $b \in B$, dizemos que $f(a) = b$ se $(a,b) \in f$.

Comumente nos "esquecemos"desta definição e tratamos funções de forma mais informal e direta. Este pecadilho matemático não chega a atrapalhar nossos objetivos, mas é importante ter em mente a definição formal. Na "prática", uma função é uma regra que associa a cada elemento $x \in A$, um elemento $f(x) \in B$. Chamamos o conjunto A de *domínio* da função f e o denotamos por $D(f)$. Chamamos o conjunto B de *contradomínio* da função f. Escrevemos $f : A \to B$, ou ainda

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x). \end{aligned}$$

Se $E \subseteq A$, chamamos de *imagem de E* ao conjunto

$$f(E) = \{f(x) : x \in E\}.$$

Similarmente, dado um conjunto H, chamamos de *imagem inversa de H* o conjunto

$$f^{-1}(H) = \{x : f(x) \in H\}.$$

Se $f(A) = B$ dizemos que f é *sobrejetiva* (ou simplesmente *sobre*). Dizemos que f é *injetiva* (ou *biunívoca* ou *um a um* ou 1-1) quando, dados a, $a' \in D(f)$, se $f(a) = f(a')$ então $a = a'$. Numa forma mais compacta, escrevemos que para todo a, $a' \in D(f)$ temos

$$f(a) = f(a') \implies a = a'.$$

Se f é injetiva e sobre, a chamamos de *bijetiva* ou de uma *bijeção*.

Dado $f : A \to B$ e um subconjunto $A' \subseteq A$, podemos definir a *função restrição* $g = f|_{A'}$ onde $g : A' \to B$ é dada por $g(a') = f(a')$ para todo $a' \in A'$. Da forma análoga, dizemos que $h : A'' \to B$ é uma *extensão* de f se $A \subseteq A''$ e $h(a) = f(a)$ para todo $a \in A$.

Dados conjuntos A, B e C e funções $f : A \to B$ e $g : B \to C$, definimos a *função composta* $h : A \to C$ por $h(a) = g(f(a))$ para todo $a \in A$. Denotamos a função composta por $h = f \circ g$.

Dizemos que $g : B \to A$ é *função inversa* de f se

$$g(f(x)) = x \quad \text{para todo } x \in A, \qquad f(g(y)) = y \quad \text{para todo } y \in B.$$

Quando esta existir, denotamos a inversa de f por f^{-1}.

Observação. Note que a definição de *imagem inversa* independe de existir ou não a função inversa. Por exemplo, a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$ não tem inversa. Entretanto $f^{-1}(\mathbb{R}) = \mathbb{R}$.

Exemplo 2.3. Seja

$$\begin{aligned} f :&(0,4) \to \mathbb{R} \\ x &\mapsto \sqrt{x}. \end{aligned}$$

Então o domínio é $(0,4)$ e a imagem é $(0,2)$. Note que f não é invertível pois f não é sobrejetiva. Entretanto as imagens inversas

$$f^{-1}\big((1,2)\big) = (1,4), \qquad f^{-1}(\{2\}) = \{4\}, \qquad f^{-1}\big([-2,0)\big) = \emptyset, \qquad f^{-1}(\emptyset) = \emptyset.$$

são bem-definidas.

A seguir nos concentramos sobre a importante questão da *existência de uma função inversa*. Considerando $f : A \to B$, note que se f não for sobrejetiva, não existirá uma inversa f^{-1}. De fato, se existe $b \in B$ tal que $f(a) \neq b$ para todo $a \in A$, então $f(g(b)) \neq b$ para qualquer função $g : B \to A$. De forma análoga, se f não for injetiva, i.e., se existirem $a \neq a'$ em A tais que $f(a) = f(a') = b \in B$, entao não é possível definir $g(b)$ tal que $g(f(a)) = a$ e $g(f(a')) = a'$. Estes argumentos mostram que sobrejetividade e injetividade são condições emphnecessárias para a exitência de inversa. Na verdade, estas condições são também equivalentes, como mostra o lema abaixp.

Lema 2.1.1. Sejam A e B conjuntos e considere a função $f : A \to B$. Então f é invertível se e somente se é sobrejetiva e injetiva.

Demonstração. ($\Longrightarrow$) Suponha que f seja invertível, e denote $g = f^{-1} : B \to A$. Sejam $a, a' \in A$ tais que $f(a) = f(a')$. Então $a = g(f(a)) = g(f(a')) = a'$. Logo f é injetiva.

Seja agora $b \in B$, e seja $a = g(b)$. Enão $f(a) = f(g(b)) = b$, e portanto f é sobre.

($\Longleftarrow$) Suponha agora f uma bijeção, i.e., sobrejetiva e injetiva. Logo, dado $b \in B$, existe um único $a \in A$ tal que $f(a) = b$. Defina então $g(b) = a$. Note que $f(g(b)) = f(a) = b$ e $g(f(a)) = g(b) = a$. Como b é arbitrário, definimos a função $g : B \to A$. $\square$

2.2. Exercícios

Exercício 2.1. Mostre que
(1) $\{x \in \mathbb{R} : x^2 \geq 0\} = \mathbb{R}$.
(2) $\{x \in \mathbb{R} : x > 0\} \subsetneq \{x \in \mathbb{R} : x^2 \geq 0\}$.
(3) $\mathbb{R} \not\subseteq \{x \in \mathbb{R} : x^2 \geq 0\}$.

Exercício 2.2. Mostre a regra de *De Morgam* dada em (2.0.1).

Exercício 2.3. Mostre que $\{a, a\} = \{a\}$.

Exercício 2.4. Sejam A e B dois conjuntos disjuntos, i.e., $A \cap B = \emptyset$. Seja $X = A \cup B$. Mostre que $A = X \backslash B$ e $B = X \backslash A$.

Exercício 2.5. Sejam A e B dois conjuntos, e $C = (A \backslash B) \cup (B \backslash A)$. Mostre que $C = (A \cup B) \backslash (A \cap B)$ e que $C \cap A \cap B = \emptyset$.

Exercício 2.6. Sejam $X_1, X_2, \ldots,$ conjuntos tais que $X_i \subseteq X_{i+1}$ para todo $i \in \mathbb{N}$. Mostre que $\cap_{i \in \mathbb{N}} X_i = X_1$.

Exercício 2.7. Dado um conjunto A, mostre que $A \times \emptyset = \emptyset$.

Exercício 2.8. Sejam A, B e C conjuntos. Mostre que $A \times (B \cup C) = (A \times B) \cup (A \times C)$ e $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Exercício 2.9. Sejam A, B, C e D conjuntos. Mostre que $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$. Mostre que, em geral, a inclusão não é própria.

Exercício 2.10. Seja a relação $\sim$ em $\mathbb{R}^2$ dada por $(x_1, y_1) \sim (x_2, y_2)$ se $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Mostre que $\sim$ é uma relação de equivalência. Interprete geometricamente a relação $\sim$.

Exercício 2.11. Tentando generalizar a relação de equivalência do exercício 2.10, dada uma função $f : \mathbb{R}^2 \to \mathbb{R}$, defina a relação $(x_1, y_1) \sim (x_2, y_2)$ se $f(x_1, y_1) = f(x_2, y_2)$. Determine se é verdadeiro ou falso que $\sim$ seja de equivalência. Prove suas afirmativas.

Exercício 2.12. Interprete $\sim$ do exercício 2.11 considerando as curvas de nível $c(t) = \{(x, y) : f(x, y) = t\}$. Mostre que $\{c(t) : t \in \mathbb{R}\}$ determina uma partição de $\mathbb{R}^2$.

Exercício 2.13. Seja X conjunto não vazio e $\sim$ uma relação de equivalência em X. Mostre que $X/\sim$ define uma partição de X.

Exercício 2.14. Seja X um conjunto e $\succcurlyeq$ uma *preordenação* em X, i.e., é uma relação reflexiva e transitiva. Defina a relação $\sim$ tal que $a \sim b$ se $a \succcurlyeq b$ e $b \succcurlyeq a$. Mostre que $\sim$ é relação de equivalência.

Exercício 2.15. Sejam A, B conjuntos e $f : A \to B$ bijeção. Se $f^{-1} : B \to A$ for a função inversa de f, mostre que f^{-1} é bijeção.

Exercício 2.16. Sejam A, B e C conjuntos e $f : A \to B$, $g : B \to C$ bijeções. Mostre que a função composta $g \circ f : A \to C$ dada por $g \circ f(x) = g(f(x))$ é bijeção. Se f^{-1} e g^{-1} forem as funções inversas de f e g, quem é $(g \circ f)^{-1}$? Justifique suas conclusões.

Exercício 2.17. Seja A um conjunto e $f : A \to B$ injetiva. Mostre que a função $f : A \to f(A)$ é bijeção.

Exercício 2.18. Seja $g : X \to Y$ sobrejetiva. Mostre que existe $f : Y \to X$ tal que $g \circ f(y) = y$ para todo $y \in Y$.

CAPíTULO 3

Números Naturais, Conjuntos finitos e infinitos

[1] Neste capítulo introduzimos os n[umeros naturais e estabelecemos vários conceitos e resultados sobre conjuntos.

Para definir os chamados *números naturais*, introduzimos os *axiomas de Peano*. Estes axiomas garantem a existência de um conjunto $\mathbb{N}$ (os naturais) e de uma função s ($s(i)$ é chamado o *sucessor* de i) que satisfazem as seguintes propriedades:

(P1) $s : \mathbb{N} \to \mathbb{N}$ é injetiva
(P2) $s(\mathbb{N}) \backslash \mathbb{N}$ contém somente um elemento, que denotamos por 1
(P3) Se $X \subset \mathbb{N}$ é tal que $1 \in X$ e ($x \in X \implies s(x) \in X$) então $X = \mathbb{N}$

Denotamos o conjunto dos naturais da forma usual

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

A notação mais usual para o sucessor de $n \in \mathbb{N}$ é $s(n) = n + 1$. O ítem P3 acima é também chamado de *princípio da indução*, e serve para demonstrar resultados que valem para todos os naturais. Temos como exemplo o lema abaixo.

Lema 3.0.1. Para todo $n \in \mathbb{N}$ vale que $s(n) \neq n$.

Demonstração. Seja $X = \{n \in \mathbb{N} : s(n) \neq n\}$. Então $1 \in X$, por P2. Agora, se $n \in X$, então $s(n) \neq n$. Usando P1 concluímos que $s(s(n)) \neq s(n)$, logo $s(n) \in X$. Por P3 temos que $X = \mathbb{N}$. □

Outro exemplo de demonstração por indução vem a seguir. Considere a afirmativa

$$\sum_{i=1}^{n} i = \frac{n}{2}(n+1) \tag{3.0.1}$$

para todo $n \in \mathbb{N}$.

Para demonstrar que (3.0.1) vale para todos os inteiros positivos, começamos observando que para $n = 1$, a afirmativa é obviamente verdadeira. Suponha então que (3.0.1) seja verdade para $n = N^*$, i.e,

$$\sum_{i=1}^{N^*} i = \frac{N^*}{2}(N^*+1). \tag{3.0.2}$$

Para $n = N^* + 1$ temos

$$\sum_{i=1}^{N^*+1} i = N^* + 1 + \sum_{i=1}^{N^*} i.$$

[1]Última Atualização: 13/08/2019

Usamos a hipótese indutiva (3.0.2) obtemos

$$\sum_{i=1}^{N^*+1} i = N^* + 1 + \frac{N^*}{2}(N^* + 1) = \frac{N^* + 1}{2}(N^* + 2),$$

e podemos concluir que (3.0.1) vale para $n = N^* + 1$, e portanto vale para todos os inteiros positivos.

Um exemplo interessante de demonstração por indução mostra que todo número inteiro $n \geq 2$ é primo ou produto de primos [**1**]. De fato, considere a proposição para $n \geq 2$ inteiro:

$$P(n): \quad \text{todo inteiro } i, \text{ tal que } 2 \leq i \leq n, \text{ é primo ou produto de primos}$$

Então $P(2)$ é verdadeiro, pois 2 é primo. Suponha agora que $P(N^*)$ seja verdadeiro para algum inteiro dado N^*. Para $n = N^* + 1$, temos que se $N^* + 1$ for primo, então $P(N^* + 1)$ é verdadeiro. Se $N^* + 1$ não for primo, então ele é divisível por algum inteiro $p > 1$. Logo, existe $q \in \mathbb{N}$ tal que $N^* + 1 = pq$. Então tanto p como q são menores que $N^* + 1$, e então, pela hipótese indutiva $P(N^*)$, tanto p como q são primos ou produtos de primos. Portanto $N^* + 1$ é primo ou produto de primos. Logo $P(N^* + 1)$ vale.

Um dos passos fundamentais, e algumas vezes esquecido, da demonstração por indução é mostrar que o resultado vale para algum valor inicial (na demonstração acima, $n = 1$). De fato, sem isto, podemos erroneamente "provar" que

$$2n \text{ é sempre ímpar para todo } n \in \mathbb{N}, \tag{3.0.3}$$

com uma argumentação obviamente falsa. De fato supondo que $2N^*$ é ímpar, temos que $2(N^* + 1) = 2N^* + 2$ também é pois $2N^*$ é ímpar por hipótese, e somando 2 a um ímpar obtemos um ímpar. O problema desta demonstração é que não se mostrou (3.0.3) para nenhum número natural.

Usando o princípio da indução, podemos definir funções de forma *recursiva*. Seja, por exemplo, $f : A \to B$. Definimos então $f^n : A \to B$ para todo $n \in \mathbb{N}$ por

$$f^1 = f, \qquad f^{s(n)} = f \circ f^n \text{ para } n > 1.$$

Por exemplo, a função adição pode ser definida por $m + n = s^n(m)$. Algumas propriedades da adição são:

(1) $m + (n + p) = (m + n) + p$
(2) $m + n = n + m$
(3) $m + n = m + p \implies n = p$ (lei do corte)

Vale também a *tricotomia* que afirma que, para todo m, $n \in \mathbb{N}$, apenas uma das propriedades abaixo vale:

(1) m=n
(2) existe $p \in \mathbb{N}$ tal que $m = n + p$
(3) existe $q \in \mathbb{N}$ tal que $n = m + q$

Podemos então estabelecer em $\mathbb{N}$ a relação $\geq$. Dizemos que $m \geq n$ se $m = n$ ou se existir $p \in \mathbb{N}$ tal que $m = n+p$. Definimos $m > n$ se $m \geq n$ mas $n \neq n$. De forma análoga podemos também definir as relações $\leq$ e $<$.

Tendo formado o conceito de ordem nos naturais, podemos falar de menos elemento de um conjunto. Dado $A \subseteq \mathbb{N}$, dizemos que $a \in A$ é o *menor elemento* de A caso $a \leq p$ para todo $p \in A$. É claro que 1 é o menor elemento de $\mathbb{N}$ (pois ele não é sucessor de nenhum outro número), e portanto se $1 \in A$ então ele também será o menor elemento de A. O resultado abaixo garante que qualquer subconjunto dos naturais não vazia possui menor elemento.

Teorema 3.0.2 (Princípio da boa ordenação). *Seja $A \subseteq \mathbb{N}$ não vazio. Então A possui elemento mínimo.*

Demonstração. Se $1 \in A$, o resultado vale pois 1 será o elemento mínimo.

Suponha então $1 \notin A$. Dado $n \in \mathbb{N}$, seja $I_n = \{1, \dots, n\}$ e $X = \{n \in \mathbb{N} : I_n \cap A = \emptyset\}$. Note que $1 \in X$ (pois $I_1 = \{1\} \cap A = \emptyset$) e que $X \neq \mathbb{N}$ (pois $A \neq \emptyset$). Portanto tem que haver $k \in X$ tal que $k+1 \notin X$ (caso contrário teríamos $X = \mathbb{N}$ pelo princípio da indução). Então

$$I_k \cap A = \{1, \dots, k\} \cap A = \emptyset, \qquad I_{k+1} \cap A = \{1, \dots, k, k+1\} \cap A \neq \emptyset.$$

Logo $k+1 \in A$. Então $k+1$ é elemento mínimo de A, pois se $x < k+1$ então $x \in I_k$ e teríamos $x \notin A$. □

Do princípio da boa ordenação acima pode-se concluir o *segundo princípio da indução*

Teorema 3.0.3 (Segundo princípio da indução). *Seja $A \subseteq \mathbb{N}$ não vazio tal que dado $n \in \mathbb{N}$, se A contém todos os naturais tais que $m < n$, então $n \in X$. Então $X = \mathbb{N}$.*

Demonstração. Ver [**9**]. □

3.1. Conjuntos finitos e infinitos

Um conjunto B é *finito* se é vazio ou se existe uma bijeção entre B e $I_N = \{1, 2, \cdots, N\}$ para algum $N \in \mathbb{N}$. Caso B não seja finito, o dizemos *infinito*.

Exemplo 3.1. O conjunto $\{2, 3, 4, 5\}$ é finito pois a função $\phi : \{1, 2, 3, 4\} \to \{2, 3, 4, 5\}$ dada por $\phi(1) = 2$, $\phi(2) = 3$, $\phi(3) = 4$, $\phi(4) = 5$ é uma bijeção.

Exemplo 3.2. O conjunto I_n é finito para todo $n \in \mathbb{N}$.

Exemplo 3.3. Sejam X e Y conjuntos e $f : X \to Y$ bijeção entre eles. Então X é finito se e somente se Y o é.

Uma pergunta natural é se, dado um conjunto X finito, podemos definir o número de elementos de X. Em outras palavras, se $\phi : I_m \to X$ e $\psi : I_n \to X$ são bijeções pode-se concluir que $m = n$? A resposta é *sim*, e baseia-se no resultado abaixo.

Teorema 3.1.1. *Seja $n \in \mathbb{N}$ e $X \subseteq I_n$. Suponha que exista bijeção $\phi : I_n \to X$. Então $X = I_n$.*

Demonstração. Primeiro note que X é não-vazio pois existe bijeção $\phi : I_n \to X$. Argumentando por indução, suponha $n = 1$. Então, por hipótese, $X \subseteq \{1\}$ e portanto se $x \in X$ tem-se $x = 1$. Logo $X = \{1\} = I_1$.

Suponha agora o resultado verdadeiro para algum $n \in \mathbb{N}$.

Seja então $X \subset I_{n+1}$ e $\phi : I_{n+1} \to X$ bijeção. Seja $x = \phi(n+1)$. Então a restrição $\phi|_{I_n} \to X \backslash \{x\}$ é uma bijeção. Consideraremos a seguir as duas possibilidades, $x = n+1$ ou $x \neq n+1$.

Se $x = n+1$, então $X \backslash \{x\} \subseteq I_n$. Como $\phi|_{I_n} \to X \backslash \{x\}$ é bijeção, então, pela hipótese indutiva, $X \backslash \{x\} = I_n$. Logo $X = I_{n+1}$.

Se $x \neq n+1$ então $n+1 \in X\backslash\{x\}$ e existe $p \in I_{n+1}$ tal que $\phi(p) = n+1$. Seja a bijeção $g : I_{n+1} \to X$ dada por

$$g(i) = \begin{cases} \phi(i) & \text{se } i \neq p, i \neq n+1, \\ x & \text{se } i = p, \\ n+1 & \text{se } i = n+1. \end{cases}$$

Logo a restrição $g|_{I_n} \to X\backslash\{n+1\}$ é bijeção, e pela hipótese indutiva, $X\backslash\{n+1\} = I_n$. Logo $X = I_{n+1}$. □

Corolário 3.1.2. Sejam m, $n \in \mathbb{N}$. As seguintes afirmativas são verdadeiras:

(1) Se existe bijeção $\phi : I_m \to I_n$, então $m = n$.
(2) Se existem bijeções $\phi : I_m \to X$ e $\psi : I_n \to X$, então $m = n$.
(3) Seja X finito. Então não existe bijeção entre X e $Y \subsetneq X$ (i.e., para X finito, se existir bijeção entre X e $Y \subseteq X$ então $X = Y$).

Demonstração. (1) Suponha $n \leq m$ (caso contrário considere ϕ^{-1}). Então $I_n \subseteq I_m$ e pelo teorema anterior temos que $I_n = I_m$.
(2) Basta usar a bijeção $\psi^{-1} \circ \phi : I_m \to I_n$ e o resultado (1).
(3) Suponha $X \neq \emptyset$ finito. Então existe bijeção $\phi : I_n \to X$ para algum $n \in \mathbb{N}$. Então $\phi^{-1} : X \to I_n$ é também bijeção e seja

$$A = \phi^{-1}(Y) \subseteq \phi^{-1}(X) = I_n.$$

Note que $\phi|_A : A \to Y$ é bijeção. Argumentando por contridição, suponha agora que exista bijeção $f : X \to Y$ e $Y \subsetneq X$. Então $(\phi|_A)^{-1} \circ f \circ \phi : I_n \to A$ é bijeção. Como $A \subseteq I_n$, então $A = I_n$, e portanto

$$Y = \phi(A) = \phi(I_n) = X,$$

contradição com $Y \subsetneq X$.

□

Observação. Se X é finito não vazio, denotamos por $\#X$ ou $|X|$ a *cardinalidade* de X, i.e., se $n = \#X$ então existe bijeção $\phi : I_n \to X$. Se X for vazio definimos $\#X = 0$.

3.2. Conjuntos enumeráveis

Se um conjunto B é finito ou se existe uma bijeção entre B e $\mathbb{N}$, dizemos que B é *enumerável*.

Observação. Existe aqui uma diferença entre os termos usados em inglês no livro do Bartle [**3**], e suas traduções diretas em português. Seguindo Elon [**9**], usamos o termo *enumerável* para equivaler ao inglês *countable*. Já as expressões *enumerable* ou *denumerable* são usadas quando existe bijeção com $\mathbb{N}$, i.e., exclui os conjuntos finitos. Por sua vez, Rudin [**18**] define os termos de uma terceira forma.

Exemplo 3.4. $P = \{2, 4, 6, \cdots\}$ é enumerável pois $\phi : \mathbb{N} \to P$ definida por $\phi(n) = 2n$ é uma bijeção entre P e $\mathbb{N}$.

Exemplo 3.5. O conjunto $\mathbb{Z}$ é enumerável pois

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \cdots\},$$

e $\phi : \mathbb{N} \to \mathbb{Z}$ dada por $\phi(i) = (-1)^i[i/2]$ é uma bijeção entre $\mathbb{N}$ e $\mathbb{Z}$. A função $[\cdot] : \mathbb{R} \to \mathbb{Z}$ é tal que $[x]$ é a parte inteira de x, i.e., o maior inteiro menor ou igual a x.

Exemplo 3.6. $\mathbb{Q}$ é enumerável pela "contagem diagonal":

$$\begin{array}{lllllll}
0, & & & & & & \\
1, & -1, & 2, & -2, & 3, & -3, & \cdots \\
1/2, & -1/2, & 2/2, & -2/2, & 3/2, & -3/2, & \cdots \\
1/3, & -1/3, & 2/3, & -2/3, & 3/3, & -3/3, & \cdots \\
\vdots & & & & & &
\end{array}$$

e podemos contar pois

$$\mathbb{Q} = \left\{0, 1, -1, \frac{1}{2}, 2, -\frac{1}{2}, \frac{1}{3}, -2, -\frac{1}{3}, \cdots\right\}.$$

Exemplo 3.7. O conjunto de números reais $\mathbb{R}$ não é enumerável. Para mostrar isto, usaremos uma demonstração por contradição. Mostraremos na verdade que $I = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ não é enumerável.

Usando a base decimal, todo elemento $x \in I$ pode ser representado pelos dígitos $x = 0, a_1a_2a_3\cdots$, onde $a_i \in \{0, \dots, 9\}$. Note que esta representação não é única; por exemplo $1,0000\cdots = 0,9999\dots$. Os números da forma $\ell \times 10^{-k}$, para algum ℓ, $k \in \mathbb{N}$, possuem exatamente duas representações possíveis. Os demais números têm somente uma representação [**20**].

Suponha agora que I é enumerável. Então existe uma enumeração $x_1, x_2, \dots, x_n, \dots$ dos elementos de I tal que

$$\begin{aligned}
x_1 &= 0, a_{11}a_{12}a_{13}\dots, \\
x_2 &= 0, a_{21}a_{22}a_{23}\dots, \\
x_3 &= 0, a_{31}a_{32}a_{33}\dots, \\
&\dots,
\end{aligned}$$

onde $a_{ij} \in \{0, \dots, 9\}$. Seja agora $y = 0, b_1b_2b_3\cdots$ onde

$$b_i = \begin{cases} 1 & \text{se } a_{ii} \neq 1 \\ 2 & \text{se } a_{ii} = 1. \end{cases}$$

Logo, por construção, y não é da forma $\ell \times 10^{-k}$, onde ℓ, $k \in \mathbb{N}$, e portanto y possui representação única. Como $y \in I$ e $b_i \neq a_{ii}$ para todo $i \in \mathbb{N}$, então $y \neq x_n$ para todo $n \in \mathbb{N}$. Isto contradiz a afirmação que $x_1, x_2, \dots, x_n, \dots$ é uma enumeração dos elementos de I. Portanto, I não é enumerável.

3.3. Exercícios

Exercício 3.1. Mostre por indução que $n < 2^n$ para todo $n \in \mathbb{N}$.

EXERCÍCIO 3.2. Prove que, para todo inteiro $n > 1$ tem-se que

$$1 + \sum_{i=2}^{n} \frac{1}{\sqrt{i}} = 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}.$$

EXERCÍCIO 3.3. Mostre por indução a desigualdade de Bernoulli: se $x > -1$, então $(1 + x)^n \geq 1 + nx$ para todo $n \in \mathbb{N}$.

EXERCÍCIO 3.4. Mostre que $2^n + 1$ é divisível por 3 para todo número ímpar n.

EXERCÍCIO 3.5. Mostre usando contradição que $\sqrt{2}$ não é racional.

EXERCÍCIO 3.6. Mostre usando contradição que se $p_1, \ldots, p_n$ são todos os números primos menores ou iguais a p_n, então $p_1 \times \cdots \times p_n + 1$ não é divisível por p_i para nenhum $i \in \{1, \ldots, n\}$.

EXERCÍCIO 3.7. Mostre usando contradição que existem infinitos números primos.

EXERCÍCIO 3.8. Seja a função $x : \mathbb{N} \to \mathbb{R}$ definida da seguinte forma. Defina $x(1) = 1$ e $x(k) = x(k-1) \times k$, para todo inteiro $k > 1$. Mostre que $x(k) = k!$.

EXERCÍCIO 3.9. Usando indução, mostre que existe $J \in \mathbb{N}$ tal que $j^2 - 10j > 0$ para todo inteiro $j > J$.

EXERCÍCIO 3.10. Seja $\lambda < 1$ e $n \in \mathbb{N}$. Mostre que

$$\sum_{i=n}^{k} \lambda^i = \lambda^n \frac{1 - \lambda^{k-n+1}}{1 - \lambda}$$

para todo inteiro $k \geq n$.

EXERCÍCIO 3.11. Sejam os conjuntos A infinito e $B \neq \emptyset$ finito, e considere uma função $f : A \to B$. Mostre que existe $b \in B$ tal que $f^{-1}(\{b\})$ é infinito.

EXERCÍCIO 3.12. Mostre que a afirmativa do Exemplo 3.3 é verdadeira.

EXERCÍCIO 3.13. Sejam A e B finitos e disjuntos. Mostre que $A \cup B$ é finito. Generalize o resultado para um número finito de conjuntos.

EXERCÍCIO 3.14. Sejam A e B finitos. Construa uma bijeção entre $\{1, 2, \ldots, |A||B|\}$ e $A \times B$, onde $|A|$ denota o número de elementos de A (o mesmo para $|B|$ e B).

EXERCÍCIO 3.15. Mostre que todo conjunto infinito contém subconjunto infinito enumerável.

EXERCÍCIO 3.16. Mostre que $\mathbb{N} \times \mathbb{N}$ é enumerável da seguinte forma: mostre que $\phi : \mathbb{N} \times \mathbb{N} \to T = \{(m, n) : n \geq m\}$, onde $\phi(m, n) = (m, m + n - 1)$, é uma bijeção. A seguir mostre que a função definida de T em $\mathbb{N}$ por $(m, n) \to (1/2)n(n+1) - n + m$ é também uma bijeção. O esquema das bijeções é como abaixo:

$$\begin{array}{cccccc}
\phi(1,1) & \phi(1,2) & \phi(1,3) & \phi(1,4) & \phi(1,5) & \cdots \\
 & \phi(2,1) & \phi(2,2) & \phi(2,3) & \phi(2,4) & \cdots \\
 & & \phi(3,1) & \phi(3,2) & \phi(3,3) & \cdots \\
 & & & \phi(4,1) & \phi(4,2) & \cdots \\
 & & & & \vdots &
\end{array}$$

$$= \begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) & \cdots \\
 & (2,2) & (2,3) & (2,4) & (2,3) & \cdots \\
 & & (3,3) & (3,4) & (3,5) & \cdots \\
 & & & (4,4) & (4,5) & \cdots \\
 & & & & \vdots &
\end{array} = \begin{array}{cccccc}
1 & 2 & 4 & 7 & 11 & \cdots \\
 & 3 & 5 & 8 & 12 & \cdots \\
 & & 6 & 9 & 13 & \cdots \\
 & & & 10 & 14 & \cdots \\
 & & & & \vdots &
\end{array}$$

Exercício 3.17. Sejam A e B conjuntos enumeráveis. Mostre que o produto cartesiano $A \times B$ é enumerável. Conclua assim que $\mathbb{Z}$ enumerável implica em $\mathbb{Q}$ enumerável.

Exercício 3.18. Porque não se pode argumentar como no exemplo 3.7 e concluir erroneamente que os racionais *não* são enumeráveis.

Exercício 3.19. Para $i \in \mathbb{N}$, seja A_i conjunto infinito enumerável. Mostre que o produto cartesiano infinito $\prod_{i=1}^{\infty} A_i$ não é enumerável.

Exercício 3.20. Para $i \in \mathbb{N}$, seja $A_i = \{0, 1\}$. Mostre que o produto cartesiano infinito $\prod_{i=1}^{\infty} A_i$ não é enumerável.

Exercício 3.21. Considere o conjunto S em que cada elemento de S é uma sequência da forma $(a_1, a_2, a_3, \dots)$ com $a_i \in \{0, 1\}$, i.e.,

$$S = \{(a_1, a_2, a_3, \dots) : \, a_i \in \{0, 1\}, \, i \in \mathbb{N}\}.$$

Decida se S é ou não enumerável, e prove sua afirmativa.

Exercício 3.22. Mostre que, para todo $N \in \mathbb{N}$, se $A_1, \dots, A_N$ são enumeráveis, então $A_1 \times \cdots \times A_N$ é enumerável. (dica: usar o resultado do exercício 3.17).

Exercício 3.23. Seja A enumerável e suponha que exista uma função $f : A \to B$ sobrejetiva. Mostre que B é enumerável.

Exercício 3.24. Considere a base decimal, e mostre que os números da forma $\ell \times 10^{-k}$, para algum ℓ, $k \in \mathbb{N}$, possuem exatamente duas representações possíveis. Mostre também que os demais números têm somente uma representação.

Índice Remissivo

Referências Bibliográficas

[1] Tom M. Apostol, *Mathematical analysis*, 2nd ed., Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1974. MR0344384 (49 #9123)

[2] Mokhtar S. Bazaraa, Hanif D. Sherali, and C. M. Shetty, *Nonlinear programming*, 3rd ed., Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2006. Theory and algorithms. MR2218478 (2006k:90001)

[3] Robert G. Bartle, *The elements of real analysis*, 2nd ed., John Wiley & Sons, New York-London-Sydney, 1976. MR0393369 (52 #14179)

[4] Robert G. Bartle and Donald R. Sherbert, *Introduction to real analysis*, 2nd ed., John Wiley & Sons Inc., New York, 1992. MR1135107 (92i:26002)

[5] James Bisgard, *Mountain Passes and Saddle Points*, SIAM Rev. **57** (2015), no. 2, 275–292, DOI 10.1137/140963510. MR3345345

[6] Ward Cheney, *Analysis for applied mathematics*, Graduate Texts in Mathematics, vol. 208, Springer-Verlag, New York, 2001. MR1838468

[7] Roger A. Horn and Charles R. Johnson, *Matrix analysis*, Cambridge University Press, Cambridge, 1985. MR832183 (87e:15001)

[8] S. Kesavan, *Nonlinear functional analysis*, Texts and Readings in Mathematics, vol. 28, Hindustan Book Agency, New Delhi, 2004.

[9] Elon Lages Lima, *Curso de análise. Vol. 1*, Projeto Euclides [Euclid Project], vol. 1, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1976 (Portuguese). MR654861 (83h:26002a)

[10] ———, *Curso de análise. Vol. 2*, Projeto Euclides [Euclid Project], vol. 13, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1981 (Portuguese). MR654862 (83h:26002b)

[11] ———, *Espaços métricos*, Projeto Euclides [Euclid Project], vol. 4, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1977 (Portuguese). MR654506 (83d:54001)

[12] Paul R. Halmos, *Naive set theory*, Springer-Verlag, New York, 1974. Reprint of the 1960 edition; Undergraduate Texts in Mathematics. MR0453532 (56 #11794)

[13] Tamara J. Lakins, *The tools of mathematical reasoning*, Pure and Applied Undergraduate Texts, vol. 26, American Mathematical Society, Providence, RI, 2016. MR3525355

[14] David G. Luenberger, *Introduction to linear and nonlinear programming*, Addison-Wesley, Reading, MA, 1973.Zbl 0297.90044

[15] ———, *Optimization by vector space methods*, John Wiley & Sons Inc., New York, 1969. MR0238472 (38 #6748)

[16] Giuseppe De Marco, *For every ϵ there continuously exists a δ*, Amer. Math. Monthly **108** (2001), no. 5, 443–444, DOI 10.2307/2695800. MR1837868

[17] *Prova de Matemática Extramuros*, `http://www.provaextramuros.org.br/`.

[18] Walter Rudin, *Principles of mathematical analysis*, 3rd ed., McGraw-Hill Book Co., New York, 1976. International Series in Pure and Applied Mathematics. MR0385023 (52 #5893)

[19] I. M. Singer and J. A. Thorpe, *Lecture notes on elementary topology and geometry*, Springer-Verlag, New York, 1976. Reprint of the 1967 edition; Undergraduate Texts in Mathematics. MR0413152 (54 #1273)

[20] Terence Tao, *Analysis. I*, Texts and Readings in Mathematics, vol. 37, Hindustan Book Agency, New Delhi, 2006. MR2195040 (2006g:26002a)

[21] ———, *Analysis. II*, Texts and Readings in Mathematics, vol. 38, Hindustan Book Agency, New Delhi, 2006. MR2195041 (2006g:26002b)

[22] *Monkey saddle — Wikipedia, The Free Encyclopedia*, Wikipedia (2009).

[23] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035 (96d:11071)