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] 22 de setembro de 2020

Resumo. Estas notas de aula são relativas ao curso de Introdução à Análise da Escola de Pós-Graduação em Economia da Fundação Getúlio Vargas (EPGE–FGV). Elas devem servir de apoio para estudos nos tópicos cobertos, mas 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 têm a intuição mais desenvolvida que o rigor.

Planejo discutir os seguintes tópicos:

- Conjuntos e funções
  - Fundamentos de lógica e o método axiomático
  - Conjuntos: definições, operações e propriedades
  - Relações: equivalência, funções, ordenações
- Conjuntos finitos, infinitos, (não-)enumeráveis.
  - O conjunto dos naturais
  - Indução
  - Conjuntos (in)finitos, (não-)enumeráveis
- Números reais
  - Cotas, supremos e ínfimos
  - Propriedades

A referência básica é o livro *The elements of Real Analysis*, de Robert Bartle [**3**]. Outras referências importantes são os já clássicos [**10**, **19**], bem como o novo [**22**]. Para tópicos específicos em uma dimensão, pode-se ler [**4**, **9**, **21**]. Finalmente, idéias mais abstratas são apresentadas em [**11**, **20**].

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 [**21**].

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 pode 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} (pelo método conhecido como *Força Bruta e Ignorância* (BFI em inglês), mas não se sabe se é de fato verdadeira para *todos* os inteiros.

[1] Última Atualização: 26/08/2020

[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 $\neg$.

EXEMPLO 1.1. Os exemplos que não são proposições:

(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 proposição ($a > 0$ 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 mesmo que somente uma das proposições seja 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].

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 proposição pode ser útil pois para concluir que uma proposição 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

[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.

interpretações dúbias ou errôneas. Por exemplo como deve-se interpretar $X \wedge Y \vee Z$? As 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 proposição 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.

Uma *tautologia* (redundância, do grego *tauto*, o mesmo) é uma proposição sempre verdadeira, como por exemplo $X \vee \neg X$, ou ainda $Y \implies Y$ (ver seção a seguir). Em ambos os casos, as proposições são verdadeiras não importando de X, Y são verdadeiro ou falso. Uma *contradição* é uma proposição que é sempre falsa, como por exemplo $X \wedge \neg X$, que independe do valor lógico de X.

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 $\implies$. Se de um fato conhecido, uma proposição verdadeira X, eu posso concluir uma outra proposição 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

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

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 $\neg$.

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

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

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

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

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

As três primeiras proposições acima são verdadeiras. Somente a última é falsa. A primeira da lista é uma tautologia do tipo $X \implies X$, 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, 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 proposição 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 uma 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 a Tabela 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.

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

TABELA 4. Tabelas verdade para operações lógicas $X \implies Y$ e sua contrapositiva $\neg Y \implies \neg X$.

(2) n ser ímpar é necessário para n ser primo.
A proposição 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*. Veja pela Tabela 4 que uma implicação e sua contrapositiva são equivalentes.

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 *variável 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) que x pode pertencer é, por exemplo, formado pelos 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*

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

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

Da mesma forma,

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

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:

(i) Existe $n \in \mathbb{N}$ tal que $P(n)$.
(ii) 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 (i) é verdade pois $P(13)$ é verdade, e isto é suficiente (para mostrar existência, basta achar um exemplo). Por outro lado, (ii) 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 (ii) 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 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

$$f : \mathbb{Z} \to \mathbb{R}$$
$$x \mapsto x^2.$$

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

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.

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), obtém-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 **[24]**.

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, descrita na página 1.

A demonstração por contradição segue os seguintes princípios: se queremos mostrar que uma afirmativa implica noutra, podemos simplesmente negar este fato e tentar chegar numa contradição. Suponha que queiramos mostrar que $X \implies Y$ seja verdade. Temos então que mostrar que sempre que $X = V$ tem-se $Y = V$. Se se consegue mostrar que

$$X \wedge \neg Y \implies \neg X, \tag{1.1.11}$$

[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.

[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.)

X	Y	$X \implies Y$	$X \wedge \neg Y \implies \neg X$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

TABELA 5. Equivalência lógica entre $X \implies Y$ e $X \wedge \neg Y \implies \neg X$.

então conclui-se que $X = V$ implica em $Y = V$. Veja que (1.1.11) é na verdade equivalente a $X \implies Y$, como mostra a Tabela 5. A argumentação acima chama-se por contradição porque se supusermos que $X = V$ e $Y = F$ obtém-se $X = F$, uma contradição.

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

$$\emptyset \subseteq A \quad \text{para qualquer conjunto } A. \tag{1.1.12}$$

Talvez uma demonstração "direta" não seja tão fácil. Mas suponha que (1.1.12) 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 (1.1.12) (afirmar que (1.1.12) é falso) nos leva a concluir um absurdo, e portanto (1.1.12) 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.

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 [**21**], 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.

2.1. Definições básicas

Repetimos aqui o Axioma 1.1.2, que garante a existência do conjunto vazio.

AXIOMA 2.1.1 (do conjunto vazio). Existe um conjunto que não contém nenhum elemento, i.e,

$$(\forall x)(x \notin \emptyset).$$

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 $A \nsubseteq B$.
- 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 2.1.2 (da especificação). Seja A um conjunto, e para cada $x \in A$, seja $P(x)$ uma proposição. Então existe um único conjunto B composto de todos os elementos x de A tais que $P(x)$ seja verdade.

[1] Última Atualização: 15/09/2020

O conjunto acima é denotado por $\{x \in A : P(x)\}$. Quando o conjunto A é claro pelo contexto, podemos escrever simplesmente $\{x : P(x)\}$. 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.

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

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

Pode-se ainda usar a *definição construtiva* $\{2x : x \in \mathbb{Z}\}$, ou, sendo um pouco menos formal, enumerar todos os elementos do conjunto: $\{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$.

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 2.1.2) 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, a 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. Para evitar absurdos como acima, impomos o seguinte axioma [**21**].

Axioma 2.1.3 (Regularidade). Se A é conjunto não vazio, então A tem que possuir ao menos um elemento que não seja um conjunto, ou que seja disjunto de A.

Note que o axioma acima impede que, dado um conjunto A, tenhamos $A \in A$. De fato, considere $B = \{A\}$. Segundo o Axioma da Regularidade, temos que ter A disjunto de B. Mas se $A \in A$, então $A \in A \cap B$, uma contradição.

De forma análoga, pode-se mostrar que dados dois conjuntos X e Y, não se pode ter $X \in Y$ e $Y \in X$. Basta aplicar o Axioma da Regularidade ao conjunto $\{X, Y\}$.

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 2.1.4 (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 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 $A \cap B = \{x \in A : x \in B\}$. Dizemos que dois conjuntos A e B são *disjuntos* se $A \cap B = \emptyset$.
- 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 $A_1, \ldots, A_n$, definimos

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

Outra forma é definir $I = \{1, \ldots, n\}$ 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 $A_1, A_2, \ldots$, 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

$$\mathcal{C}(\cup_{i \in \mathbb{N}} E_n) = \cap_{i \in \mathbb{N}} \mathcal{C}(E_n), \qquad \mathcal{C}(\cap_{i \in \mathbb{N}} E_n) = \cup_{i \in \mathbb{N}} \mathcal{C}(E_n). \tag{2.1.1}$$

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. Uma forma de se definir o par ordenado (a, b) é por $\{\{a\}, \{a, b\}\}$ (na verdade, basta usar $\{\{a\}, \{a, b\}\}$ e o Axioma da Regularidade 2.1.3).

LEMA 2.1.5. **[17]** Dados elementos a, b, defina o par ordenado (a, b) como o conjunto $\{\{a\}, \{a, b\}\}$. Mostre então que $(w, x) = (y, z)$ se e somente se $w = y$ e $y = z$.

DEMONSTRAÇÃO. Suponha que $\{\{w\}, \{w, x\}\} = \{\{y\}, \{y, z\}\}$. Queremos mostrar que $w = y$ e $x = z$. Como $\{\{w\}, \{w, x\}\} \subseteq \{\{y\}, \{y, z\}\}$, então $\{w\} = \{y\}$ ou $\{w\} = \{y, z\}$. No primeiro caso, $w = y$, e no último caso, $w = y = z$. Temos então que $w = y$ em ambas situações.

De $\{w, x\} \in \{\{y\}, \{y, z\}\}$ temos que ou $\{w, x\} = \{y\} = \{w\}$, e então $w = x$, ou $\{w, x\} = \{y, z\} = \{w, z\}$ e então $x = z$.

Se $w = x$ então

$$\{\{x\}\} = \{\{x\}, \{x, x\}\} = \{\{w\}, \{w, x\}\} = \{\{w\}, \{w, z\}\}.$$

Mas então $\{w, z\} \in \{\{x\}\}$ e $z = x$. □

O mais importante na verdade, 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.

2.2. Relações e partições

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 2.2.1. *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 $a = b$

Dada uma relação reflexiva R num conjunto X, definimos sua *parte assimétrica* como sendo a relação $P_R \subseteq X^2$ tal que

$$P_R = \{(x, y) \in X^2 : xRy, y \not R\, x\}.$$

A relação $I_R = R \backslash P_R$ é a *parte simétrica* de R.

Por exemplo, dada a relação $\leq$ em $\mathbb{R}$, sua parte assimétrica é dada por $<$, e sua parte simétrica por $=$.

Uma *relação de equivalência* $\sim$ num conjunto A é, por definição, uma relação binária que seja 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, $(a, b) \sim (m, n)$.

A relação de equivalência acima nos permite escrever

$$\frac{a}{b} = \frac{c}{d}$$

nos racionais $\mathbb{Q}$.

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:

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

Outra notação para o cnojunto das partes é 2^X.

Por exemplo, se $X = \{1, 2, 3\}$, então

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, X\}.$$

Outros exemplos são

$$\mathcal{P}(\emptyset) = \{\emptyset\}, \quad \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}, \quad \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$

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

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

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

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

Exemplo 2.3. A "menor" relação de equivalência dum conjunto X é a *relação diagonal* $D_X = \{(x, x) : x \in X\}$. Note que neste caso, $[x] = \{x\}$ para todo $x \in X$. Esta relação é a menor possível no sentido de que qualquer outra relação a conterá. Analogamente, a "maior" relação de equivalência é dada por $X^2 = X \times X$.

Teorema 2.2.2 ([**13**]). *Seja $\sim$ uma relação de equivalência definida num conjunto não-vazio X. Então*

(1) para todo $x \in X$, $x \in [x]$
(2) para todo x, $y \in X$, $x \sim y$ se e somente se $[x] = [y]$
(3) para todo x, $y \in X$, $x \not\sim y$ se e somente se $[x] \cap [y] = \emptyset$

O teorema acima nos diz que as classes de equivalência "dividem" ou "particionam" um conjunto X. Considere a seguinte definição formal. 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 $\mathbb{R}$.

Corolário 2.2.3 (do Teorema 2.2.2). Seja $\sim$ uma relação de equivalência definida num conjunto não-vazio X. Então $X/\sim$ é uma partição de X.

A volta do corolário acima também vale, ou seja, uma partição define uma relação de equivalência, como nos mostra o teorema a seguir.

TEOREMA 2.2.4 ([**13**]). *Seja X conjunto não vazio, e $\mathcal{T}$ uma partição de X. Seja a relação de equivalência $\sim$ dada por*

$$x \sim y \iff (\exists A \in \mathcal{T})(x \in A \wedge y \in A),$$

para quaisquer x, $y \in X$. Além disto, as classes de equivalência definidas por $\sim$ são exatamente os elementos de $\mathcal{T}$, i.e., $X/\sim = \mathcal{T}$.

DEMONSTRAÇÃO. Temos que mostrar que a relação $\sim$ acima definida satisfaz as propriedades de uma relação de equivalência. Note que de fato é reflexiva pois para $x \in X$, tem-se que existe $A \in \mathcal{T}$ tal que $x \in A$, e portanto $x \sim x$. Para ver que é simétrica, note que se $x \sim y$, então, por definição, existe $A \in \mathcal{T}$ tal que $x \in A$ e $y \in A$. Logo $y \sim x$. Finalmente, para provar a transitividade, suponha que $x \sim y$ e $y \sim x$. Então existe $A \in \mathcal{T}$ tal que $x \in A$ e $y \in A$, e existe $B \in \mathcal{T}$ tal que $y \in B$ e $z \in B$. Mas como $y \in A \cap B$, então $A = B$, pois $\mathcal{T}$ é uma partição. Portanto $x \in A$ e $z \in A$ implica em $x \sim z$. Concluímos então que $\sim$ é de fato uma relação de equivalência.

Para ver que $X/\sim = \mathcal{T}$, mostraremos que $X/\sim \subseteq \mathcal{T}$ e $\mathcal{T} \subseteq X/\sim$.

Seja $[a] \in X/\sim$. Então $a \in X$ e existe $A \in \mathcal{T}$ tal que $a \in A$ Mas então $[a] = A$ pois

$$x \in [a] \iff x \sim a \iff x \in A. \tag{2.2.1}$$

Logo $[a] = A \in \mathcal{T}$. Como $[a]$ é arbitrário, então $X/\sim \subseteq \mathcal{T}$.

Seja agora $A \in \mathcal{T}$. Então $A \neq \emptyset$. Seja então $a \in A$. Novamente (2.2.1) implica que $A = [a]$, logo $A \in \mathcal{T}/\sim$, como queríamos demonstrar. □

2.2.1. Relações de ordem. Outro tipos de relação são as que definem *ordenações*, que são sempre transitivas. Definimos uma *preordem* $\precsim$ em X como sendo uma relação transitiva e reflexiva ($x \precsim x$ para todo $x \in X$). Dizemos que uma preordem $\precsim$ é uma *ordenação parcial* de um conjunto X se for antissimétrica, i.e.,

- $a \precsim a$ para todo $a \in A$ (reflexiva)
- $a \precsim a'$ e $a' \precsim a'' \implies a \precsim a''$ (transitiva)
- $a \precsim a'$ e $a' \precsim a \implies a = a'$ (antisimétrica)

Uma ordenação parcial é dita *linear* ou *total* se for completa ($a \precsim a'$ ou $a' \precsim a$).

Usamos a notação de que, dada uma preordem $\precsim$, denotamos sua parte assimétrica por $\prec$, e sua parte simétrica por $\sim$.

EXEMPLO 2.4. Os conjuntos $\mathbb{N}$, $\mathbb{Q}$ e $\mathbb{R}$ são totalmente ordenados usando-se a relação $\leq$ usual. Em se tratando de conjuntos, a relação definida por $\subseteq$ define uma relação parcial (ver exercício 2.17), mas não total. De fato, considere por exemplo $\mathcal{F} = \big\{\{1,2\}, \{2\}, \{3\}\big\}$. Então $\{2\} \subseteq \{1,2\}$, mas $\{2\} \subsetneq \{3\}$ e $\{3\} \subsetneq \{2\}$, e portanto $\{2\}$ e $\{3\}$ não são comparáveis.

EXEMPLO 2.5. Considere em $\mathbb{R}^2$ a seguinte preferência *alfabética* ou *lexicográfica*, onde $(x_1, x_2) \succcurlyeq (y_1, y_2)$ se

$$\begin{cases} x_1 > y_1 \text{ ou} \\ x_1 = y_1 \text{ e } x_2 \geq y_2. \end{cases}$$

Esta ordenação é total. De fato, ela é:

(i) reflexiva: $(x_1, x_2) \succcurlyeq (x_1, x_2)$ pois $x_1 = x_1$ e $x_2 \geq x_2$

(ii) transitiva: suponha $(x_1, x_2) \succcurlyeq (y_1, y_2)$ e $(y_1, y_2) \succcurlyeq (z_1, z_2)$. Se $x_1 > y_1$ segue-se que $x_1 > z_1$ pois $y_1 \geq z_1$, e então $(x_1, x_2) \succcurlyeq (z_1, z_2)$. Se $x_1 = y_1$ então $x_1 \geq z_1$, e duas possibilidades se nos apresentam. Se $x_1 > z_1$ então $(x_1, x_2) \succcurlyeq (z_1, z_2)$. Se $x_1 = z_1$, então $x_2 \geq z_2$ pois $x_2 \geq y_2$ e $y_2 \geq z_2$.

(iii) antisimétrica: suponha agora $(x_1, x_2) \succcurlyeq (y_1, y_2)$ e $(y_1, y_2) \succcurlyeq (x_1, x_2)$. Note que não podemos ter $x_1 > y_1$ nem $y_1 > x_1$, e portanto $x_1 = y_1$. Analogamente, não podemos ter $x_2 > y_2$ nem $y_2 > x_2$ e então $x_2 = y_2$. Logo, $(x_1, x_2) = (y_1, y_2)$.

Em $\mathbb{R}^n$, a ordenação seria $(x_1, \ldots, x_n) \succcurlyeq (y_1, \ldots, y_n)$ se uma das seguintes situações ocorrer:

(i) $x_1 > y_1$
(ii) $x_1 = y_1, \ldots, x_{k-1} = y_{k-1}$ e $x_k > y_k$ para algum $k \in \{2, \ldots, n\}$
(iii) $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$

Esta ordenação também é total; ver Exercício 2.22.

2.3. 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 $(a, b) \in f$. Definimos o conjunto de todas as funções de A em B por B^A.

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 2.6. Seja

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

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 *necessárias* para a existência de inversa. Na verdade, estas condições são também equivalentes, como mostra o lema abaixo.

Lema 2.3.1. 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 $g : B \to A$. □

Note que duas funções são *iguais* se seus domínios e contradomínios são iguais, e se além disto elas "assumem" os mesmos valores, i.e. seus gráficos são iguais. O gráfico de uma função $f : X \to Y$ é definido por

$$\mathrm{Gr}(f) = \{(x, f(x)) : x \in X\} \subset X \times Y.$$

Dados dois conjuntos X e Y, podemos definir a função *projeção* $\pi_X : X \times Y \to X$ por $\pi_X\big((x, y)\big) = x$ (é mais comum simplificar a notação para $\pi_X(x, y)$). A projeção $\pi_Y : X \times Y \to Y$ é definida analogamente. Note que projeções são necessariamente sobrejetivas, mas nem sempre injetivas (quando elas seriam injetivas?).

2.4. 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 (2.1.1).

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 ([**17**]). Dado o conjunto $X \neq \emptyset$ e uma relação R em X, defina a relação inversa $R^{-1} = \{(y, x) \in X^2 : xRy\}$. Mostre que R é simétrica se e somente se $R = R^{-1}$.

Exercício 2.11 ([**17**]). Se R_1 e R_2 são duas relações num conjunto $X \neq \emptyset$, definimos a composição $R_2 \circ R_1 = \{(y, x) \in X^2 : xRyz,\ zRy \text{ para algum } z \in X\}$. Mostre que R é transitiva se e somente se $R \circ R$.

Exercício 2.12 ([**17**]). Mostre que a parte simétrica de uma relação reflexiva é reflexiva e simétrica, e que a parte assimétrica não é nem reflexiva nem simétrica.

Exercício 2.13. 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 2.14. Tentando generalizar a relação de equivalência do exercício 2.13, 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 2.15. Interprete $\sim$ do exercício 2.14 supondo $f : \mathbb{R}^2 \to \mathbb{R}$ sobrejetiva e considerando as curvas de nível $c(t) = \{(x, y) \in \mathbb{R}^2 : f(x, y) = t\}$. Mostre que $\{c(t) : t \in \mathbb{R}\}$ determina uma partição de $\mathbb{R}^2$.

Exercício 2.16. Mostre que se um conjunto A é totalmente ordenado, então todos seus subconjuntos também o são.

Exercício 2.17. Seja $\mathcal{F}$ uma coleção de conjuntos. Mostre que $\subseteq$ define uma ordenação parcial, mas não total.

Exercício 2.18. Prove o Teorema 2.2.2.

Exercício 2.19. Prove o Corolário 2.2.3.

Exercício 2.20. Seja X um conjunto e $\succcurlyeq$ uma *preordenação* em X. 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 2.21. Seja a relação no $\mathbb{R}^n$ dada por $\mathbf{x} \geq \mathbf{y}$ se $x_i \geq y_i$ para todo $i = 1, \ldots, n$. Mostre que é uma ordenação parcial.

Exercício 2.22. Mostre que a ordenação lexicográfica no $\mathbb{R}^n$, definida no Exemplo 2.5, é total.

Exercício 2.23. Mostre que a única relação parcial que é também uma relação de equivalência é dada pela relação diagonal (ver Exemplo 2.3).

Exercício 2.24. 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 2.25. 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 2.26. Seja A um conjunto e $f : A \to B$ injetiva. Mostre que a função $f : A \to f(A)$ é bijeção.

Exercício 2.27. Seja A um conjunto e $f : A \to B$ sobrejetiva. Mostre que existe $g : B \to A$ injetiva.

Exercício 2.28. 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 números 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 $X \subseteq \mathbb{N}$ 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 definindo o conjunto

$$X = \{n \in \mathbb{N} : \ \text{(3.0.1) é verdade}\}.$$

Observe que para $n = 1$, a afirmativa é obviamente verdadeira, e então $1 \in X$. Suponha então que $N^* \in X$, i.e., (3.0.1) seja verdade para $n = N^*$:

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

[1] Última Atualização: 22/09/2020

Para $n = N^* + 1$ temos

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

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 $N^* + 1 \in X$. Por (P3) concluímos que $X = \mathbb{N}$, e então (3.0.1) 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:

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

Seja $X = \{n \in \mathbb{N} : P(n) \text{ é verdade}\}$. Note que $P(1)$ é verdadeiro, pois todo inteiro i tal que $2 \leq i \leq 1$ é primo. Então $1 \in X$. Suponha agora que $n \in X$, i.e., suponha que $P(n)$ seja verdadeiro para algum inteiro dado n. Queremos mostrar que $n + 1 \in X$. Se $n + 1$ for primo, então $P(n + 1)$ é verdadeiro, e portanto $n + 1 \in X$. 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 de ordem $\geq$. 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 $<$.

A relação $<$ tem as seguintes propriedades:

(i) Transitividade: se $m < n$ e $n < p$ então $m < p$. De fato, se $m < n$ e $n < p$ então existem l, $q \in \mathbb{N}$ tais que $m + l = n$ e $n + q = p$. Logo $m + (l + q) = n + q = p$, e portanto $m < p$.

(ii) Tricotomia: Dados m, $n \in \mathbb{N}$ uma, e somente uma, situação ocorre: ou $m = n$ ou $m < n$ ou $n < m$. Esta propriedade segue diretamente da propriedade de tricotomia dos naturais.

(iii) Monotonicadade da adição: se $m < n$ então $m + p < n + p$ para todo $p \in \mathbb{N}$. De fato, se $m < n$ então existe $q \in \mathbb{N}$ tal que $m + q = n$, e portanto $(m + p) + q = n + p$, i.e., $m + p < n + p$.

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 $I_n = \{1, \ldots, n\}$ 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

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

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 $X \subseteq \mathbb{N}$ não vazio tal que dado $n \in \mathbb{N}$, se X contém todos os naturais tais que $m < n$, então $n \in X$. Então $X = \mathbb{N}$.*

Demonstração. (Por contradição) Seja $Y = \mathbb{N} \backslash X$. Quero mostrar que $Y = \emptyset$. De fato, suponha $Y \neq \emptyset$. Então Y possui elemento mínimo $p \in Y$, e $\{1, \ldots, p - 1\} \cap Y = \emptyset$. Logo, $\{1, \ldots, p - 1\} \subset X$. Por hipótese em X, $p \in X$, uma contradição com $p \in Y$. □

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*. Consideraremos a seguir propriedade de conjuntos finitos, e depois de conjuntos infinitos.

3.1.1. Conjuntos finitos. Por definição, para mostrar que um conjunto é finito, é necessário achar uma bijeção com I_n, para algum $n \in \mathbb{N}$.

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 $X \subset I_{n+1}$, com $n+1 \in X$ (caso contrário, $X \subseteq I_n$ e o resultado segue por indução) 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 contradição, 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 $|X| = 0$.

O resultado a seguir garante que não podemos ter conjuntos infinitos contidos em conjuntos finitos.

TEOREMA 3.1.3. *Suponha X conjunto finito e $Y \subseteq X$. Temos então que*

(i) Y é finito
(ii) $|Y| \leq |X|$
(iii) se $|Y| = |X|$, então $Y = X$

DEMONSTRAÇÃO. Sem perda de generalidade, suponha $X = I_n$ (faça o caso geral como exercício). Por indução, suponha $n = 1$. Então (i), (ii) e (iii) são triviais.

Suponha agora que (i), (ii) e (iii) valham quando $X = I_n$ para algum n fixo. No caso de $Y \subseteq X = I_{n+1}$ temos então que, se $Y \subseteq I_n$, temos pela hipótese indutiva que Y é finito e $|Y| \leq n < n + 1 = |I_{n+1}| = |X|$.

Suponha agora que $\{n+1\} \in Y$ e que $Y \neq \{n+1\}$ (caso trivial). Pela hipótese indutiva, existe bijeção

$$\psi : I_p \to Y \backslash \{n + 1\}$$

para algum $p \leq n$. Note que

$$p = n \implies Y \backslash \{n + 1\} = I_n \tag{3.1.1}$$

pois $Y \backslash \{n + 1\} \subseteq I_n$.

Seja $\phi : I_{p+1} \to Y$ tal que

$$\phi(x) = \begin{cases} \psi(x) & \text{se } x \in I_p, \\ n + 1 & \text{se } x = p + 1. \end{cases}$$

Então ϕ é bijeção. Logo, Y é finito e $|Y| = p + 1 \leq n + 1 = |X|$. Finalmente, se $|Y| = |X|$, então $p = n$ pois $p + 1 = |Y| = |X| = n + 1$. Por (3.1.1), temos que $Y \backslash \{n + 1\} = I_n$, i.e., $Y = I_{n+1}$ pois $n + 1 \in Y$. □

COROLÁRIO 3.1.4. Seja Y conjunto finito e $f : X \to Y$ injetiva. Então X é finito e $|X| \leq |Y|$.

DEMONSTRAÇÃO. Como $f(X) \subseteq Y$, então $f(X)$ é finito. Como $f : X \to f(X)$ é bijeção, então X é finito. Finalmente, $|X| = |f(X)| \leq |Y|$. □

COROLÁRIO 3.1.5. Seja X conjunto finito e $g : X \to Y$ sobrejetiva. Então Y é finito e $|Y| \leq |X|$.

DEMONSTRAÇÃO. Como $g : X \to Y$ é sobrejetiva, então existe $f : Y \to X$ injetiva tal que $g \circ f : Y \to Y$ e $g(f(y)) = y$ para todo $y \in Y$. Pelo corolário acima, X finito implica em Y finito e $|Y| \leq |X|$. □

Outro conceito importante é o da limitação. Dizemos que $X \subset \mathbb{N}$ é *limitado* se existir $k \in \mathbb{N}$ tal que $x \leq k$ para todo $x \in X$ (chamamos k de *cota superior* de X). Os conjuntos não limitados são chamados de *ilimitados*.

TEOREMA 3.1.6. *Seja $X \neq \emptyset$. As afirmativas abaixo são equivalentes:*

(i) X é finito
(ii) X é limitado
(iii) X possui um maior elemento (i.e., existe uma cota superior de X que pertence a X)

DEMONSTRAÇÃO. Para mostrar que $(i) \implies (ii)$, suponha $X = \{x_1, \ldots, x_n\}$. Então $k = x_1 + \cdots + x_n$ é tal que $x \leq k$ para todo $x \in X$. Portanto X é limitado.

Para ver que $(ii) \implies (iii)$, considere o conjunto

$$A = \{p \in \mathbb{N} : \ p \text{ é cota superior de } X\}.$$

Seja p_0 o menor elemento de A. Então $p_0 \in X$. (Para mostrar isto, suponha que $p_0 \notin X$. Então $p_0 > x$ para todo $x \in X$. Como $X \neq \emptyset$, então $p_0 > 1$. Logo $p_0 = p_1 + 1$ para algum $p_1 \in \mathbb{N}$. Então $p_1 \notin A$ pois $p_1 < p_0$ e p_0 é menor elemento de A. Logo p_1 não é cota superior de X e então existe $n \in X$ tal que $n > p_1$. Logo $n \geq p_1 + 1 = p_0$. Como $p_0 \geq n$, então $p_0 n$, contradição com $p_0 \notin X$.) Temos então que $p_0 \in X$ e $p_0 \geq x$ para todo $x \in X$. Logo X possui um maior elemento.

Para mostrar $(iii) \implies (i)$, considere $k \in \mathbb{N}$ cota superior de X. Então $X \subset I_k$, e portanto é finito. □

3.1.1.1. *União e produto cartesiano de conjuntos finitos.* A seguir disutimos resultados a respeito da união e produtos cartesianos de conjuntos finitos. Começamos por discutir uniões finitas de conjuntos finitos. A seguir consideramos propriedades de produtos cartesianos finitos de conjuntos finitos.

TEOREMA 3.1.7. *Seja X e Y conjuntos finitos disjuntos. Então $X \cup Y$ é finito e $|X \cup Y| = |X| + |Y|$.*

DEMONSTRAÇÃO. Seja $m = |X|$ e $n = |Y|$, e bijeções $\phi : I_m \to X$ e $\psi : I_m \to Y$. Seja $\xi : I_{m+n} \to X \cup Y$ dada por

$$\xi(i) = \begin{cases} \phi(i) & \text{se } i \in \{1, \ldots, m\}, \\ \psi(i - m) & \text{se } i \in \{m + 1, \ldots, m + n\}. \end{cases}$$

Então ξ é um bijeção (prove esta afirmativa). □

COROLÁRIO 3.1.8. Sejam $X_1, \ldots, X_k$ conjuntos finitos tais que $X_i \cap X_j = \emptyset$ para todos $i, i = 1, \ldots, k$. Então $X_1 \cup \cdots \cup X_k$ é finito e $|X_1 \cup \cdots \cup X_k| = |X_1| + \ldots |X_k|$.

DEMONSTRAÇÃO. Por indução. □

COROLÁRIO 3.1.9. Se $Y_1, \ldots, Y_k$ são finitos (não necessariamente disjuntos), então $Y_1 \cup \cdots \cup Y_k$ é finito e $|Y_1 \cup \cdots \cup Y_k| \leq |Y_1| + \ldots |Y_k|$.

DEMONSTRAÇÃO. Para $k = 2$, temos que $Y_1 \cup Y_2 = y_1 \cup A$, onde definimos $A = Y_2 \backslash Y_1$. Então $y_1 \cap A = \emptyset$, e pelo Teorema 3.1.7,

$$|Y_1 \cup Y_2| = |Y_1 \cup A| = |Y_1| + |A| = |Y_1| + |Y_2 \backslash Y_1| \leq |Y_1| + |Y_2|.$$

Para $k > 2$, fazer por indução. □

COROLÁRIO 3.1.10. Se $X_1, \ldots, X_k$ são conjuntos finitos, então $X_1 \times \cdots \times X_k$ é finito e $|X_1 \times \cdots \times X_k| = |X_1| \ldots |X_k|$.

DEMONSTRAÇÃO. Suponha $k = 2$. Se $X = \{x_1, \ldots, x_m\}$ e $Y = \{y_1, \ldots, y_n\}$, então

$$X \times Y = A_1 \cup \cdots \cup A_m,$$

onde

$$A_1 = \{(x_1, y_1), \ldots, (x_1, y_n)\}, \ \ldots, A_m = \{(x_m, y_1), \ldots, (x_m, y_n)\}.$$

Portanto $X \times Y$ é união finita de conjuntos disjuntos. Logo é finito e

$$|X \times Y| = |A_1| \ldots |A_m| = mn = |X||Y|.$$

O caso para $k > 2$ pode ser feito por indução. □

Finalmente, temos o importante resultado que nos di quantas funções existem entre conjuntos finitos.

COROLÁRIO 3.1.11. Sejam X e Y conjuntos finitos com $|X| = m$ e $|Y| = n$. Considere o conjunto

$$\mathcal{F}(X, Y) = \{f : X \to Y : \ f \text{ é função}\}.$$

Então $\mathcal{F}(X, Y)$ é finito e $|\mathcal{F}(X, Y)| = n^m$.

DEMONSTRAÇÃO. Se $X = I_m$, então $f \in \mathcal{F}(X, Y)$ pode ser escrita como

$$\big(f(1), \ldots, f(m)\big) = (y_{i_1}, \ldots, y_{i_m}) \in Y^m.$$

Logo $|\mathcal{F}(X, Y)| = |Y^m| = n^m$. No caso geral, seja $\phi : I_m \to X$. Então

$$\psi : \mathcal{F}(X, Y) \to \mathcal{F}(I_m, Y), \qquad \psi(f) = f \circ \phi$$

é bijeção. Logo $|\mathcal{F}(X, Y)| = \mathcal{F}(I_m, Y) = n^m$. □

3.1.2. Conjuntos infinitos. Para mostrar que um conjunto é infinito, é preciso provar que não existe bijeção com I_n, qualquer que seja $n \in \mathbb{N}$.

EXEMPLO 3.4. Para mostrar que $\mathbb{N}$ é infinito, considere, por contradição, que exista bijeção $\phi : I_n \to \mathbb{N}$ para algum $n \in \mathbb{N}$. Seja então

$$p = \phi(1) + \cdots + \phi(n).$$

Logo, $p > \phi(j)$ para todo $j \in I_n$ e portanto $p \notin \phi(I_n)$. Mas como $p \in \mathbb{N}$ e $\phi(I_n) = \mathbb{N}$, obtemos uma contradição.

EXEMPLO 3.5. Seja $P = \{2j : \ j \in \mathbb{N}\}$. Então P é infinito, pois $\psi : P \to \mathbb{N}$ dada por $\psi(j) = j/2$ é bijeção. Se houvesse bijeção ϕ entre I_n e P, para algum $n \in \mathbb{N}$, então $\phi \circ \psi$ seria bijeção entre I_n e $\mathbb{N}$, um absurdo.

Note que, por exclusão, temos os seguintes resultados:

(i) X infinito e $f : X \to Y$ injetiva implica em Y infinito

(ii) Y infinito e $f : X \to Y$ sobre implica em X infinito
(iii) Se $X \subsetneq Y$ e $f : X \to Y$ é bijeção, então X e Y são infinitos

EXEMPLO 3.6. Os conjuntos $\mathbb{Z}$ e $\mathbb{Q}$ são infinitos, pois as funções $f : \mathbb{N} \to \mathbb{Z}$ definida por $f(i) = i$ e $g : \mathbb{N} \to \mathbb{Q}$ dada por $g(i) = i$ são injetivas. As funções f e g são chamadas de *inclusões*.

3.2. Conjuntos enumeráveis e não enumeráveis

Se um conjunto B é finito ou se existe uma bijeção entre B e $\mathbb{N}$, dizemos que B é *enumerável*. Caso um conjunto não seja enumerável, o chamamos de não 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 [**19**] define os termos de uma terceira forma.

3.2.1. Conjuntos enumeráveis. Uma forma de mostrar que um conjunto é enumerável é usar a definição, i.e., mostrar que ou ele é finito ou mostra uma bijeção com $\mathbb{N}$.

EXEMPLO 3.7. $P = \{2, 4, 6, \cdots\}$ é enumerável pois $\phi : \mathbb{N} \to P$ definida por $\phi(n) = 2n$ é uma bijeção entre P e $\mathbb{N}$.

EXEMPLO 3.8. 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.

TEOREMA 3.2.1. *Todo conjunto infinito contém $Y \subseteq X$ infinito enumerável.*

DEMONSTRAÇÃO. A ideia da demonstração é baseada na construção de uma função $\phi : \mathbb{N} \to X$ injetiva. Por indução:

(i) escolha $x_1 \in X$ e defina $\phi(1) = x_1$
(ii) suponha que $\phi(1) = x_1, \ldots \phi(n) = x_n$ estejam definidos
(iii) escolha $x_{n+1} \in X \backslash \{x_1, \ldots, x_n\}$ e defina $\phi(n + 1) = x_{n+1}$

Então ϕ é injetiva, pois dados $m < n$, então $\phi(m) \in \{x_1, \ldots, x_{n-1}\}$ mas

$$\phi(n) \in X \backslash \{x_1, \ldots, x_{n-1}\}.$$

Logo $\phi(m) \neq \phi(n)$. Então ϕ é bijeção entre $\mathbb{N}$ e $\phi(\mathbb{N}) \subseteq X$, e então $\phi(\mathbb{N})$ é infinito enumerável. □

COROLÁRIO 3.2.2. Um conjunto X é infinito se e somente se existe bijeção entre X e uma parte própria de X.

DEMONSTRAÇÃO. ($\Longleftarrow$) Nenhum conjunto finito pode ser bijetivo a um subconunto próprio.

($\Longrightarrow$) Seja $A \subset X$ subconjunto infinito enumerável, dado por $A = \{a_1, a_2, a_3, a_4, \dots\}$. Então $Y = X \backslash \{a_1, a_3, a_5, \dots\}$ é tal que $Y \subsetneq X$. Seja $\phi : X \to Y$ dada por

$$\phi(x) = \begin{cases} x & \text{se } x \in Y = X \backslash A, \\ a_{2n} & \text{se } x = a_n \in A. \end{cases}$$

Então ϕ é uma bijeção (mostre). □

É razoável pensar que todo subconjunto de conjuntos enumeráveis é também enumerável. Este resultado é verdadeiro, e é consequência do caso particular, nos naturais.

TEOREMA 3.2.3. *Seja $X \subseteq \mathbb{N}$. Então X é enumerável.*

DEMONSTRAÇÃO. Se $X \subseteq \mathbb{N}$ for finito, então é enumerável. Suponha agora X infinito, e seja $f : \mathbb{N} \to X$ definida indutivamente como abaixo:

(i) $f(1) =$ menor elemento de X.
(ii) dado $n \in \mathbb{N}$ suponha $f(1), \dots, f(n)$ dadas tal que $f(1) < \cdots < f(n)$, e que $f(n) < x$ para todo $x \in B_n = X \backslash \{f(1), \dots, f(n)\}$. Note que $B_n \neq \emptyset$ pois X é infinito.
(iii) $f(n+1) =$ menor elemento de B_n.

Então f é uma bijeção. Para provar, note que se $m < n$ então $f(m) < f(n)$ e portanto f é injetiva. Para provar sobrejetividade, se existisse $x \in X \backslash f(\mathbb{N})$, então $x \in B_n$ para todo $n \in \mathbb{N}$. Logo $x > f(n)$ para todo $n \in \mathbb{N}$, e $f(\mathbb{N})$ teria que ser limitado. Uma contradição com $f(\mathbb{N})$ ser infinito.

Como f é bijeção entre $\mathbb{N}$ e X, então X é enumerável. □

COROLÁRIO 3.2.4. Sejam X e Y conjunto. Valem os seguintes resultados:

(i) Seja $X \subseteq Y$ onde Y é enumerável. Então X é enumerável.
(ii) Se $f : X \to Y$ é injetiva e Y é enumerável, então X é enumerável.

Sejam $X, Y \subseteq \mathbb{N}$. Dizemos que $f : X \to Y$ é crescente se $m < n$ implica em $f(m) < f(n)$. Note que a função f definida no Teorema 3.2.3 satisfaz tal propriedade. Temos portanto que o corolário a seguir vale.

COROLÁRIO 3.2.5. Dado $X \subseteq \mathbb{N}$ infinito, existe bijeção crescente $f : \mathbb{N} \to X$.

DEMONSTRAÇÃO. Ver função construida no Teorema 3.2.3. □

Finalmente, temos o seguinte resultado.

TEOREMA 3.2.6. *Seja X enumerável e $f : X \to Y$ sobrejetiva. Então Y é enumerável.*

DEMONSTRAÇÃO. Como f é sobrejetiva, existe $g : Y \to X$ tal que $f(g(y)) = y$ para todo $y \in Y$. Então g é injetiva, e segue-se do Corolário 3.2.4 que Y é enumerável. □

Consideramos a seguir produtos cartesianos e uniões de conjuntos enumeráveis.

TEOREMA 3.2.7. *Sejam A e B enumeráveis. Então $A \times B$ é enumerável.*

DEMONSTRAÇÃO. Sejam $\phi : A \to \mathbb{N}$ e $\psi : B \to \mathbb{N}$ injetivas (mostre a existência destas funções). Então $g : A \times B \to \mathbb{N} \times \mathbb{N}$ tal que $g(a, b) = (\phi(a), \psi(b))$ é injetiva. Pelo Corolário 3.2.4, basta mostrar que $\mathbb{N} \times \mathbb{N}$ é enumerável.

Para mostrar que $\mathbb{N} \times \mathbb{N}$ é enumerável, considere a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $f(m, n) = 2^m 3^n$. Então f é injetiva (mostre), e portanto $\mathbb{N} \times \mathbb{N}$ é enumerável. □

OBSERVAÇÃO. Por indução, mostra-se que $A_1, \dots A_k, \dots$ enumeráveis implica em

$$\Pi_{i=1}^{k} A_i = A_1 \times A_2 \times \cdots \times A_k$$

enumerável. Entretanto, não é verdade que $\Pi_{i=1}^{\infty} A_i$ seja enumerável em geral. Basta para isto que $|A_i| > 1$ para uma infinidade de índices, como mostraremos no Teorema 3.2.10.

COROLÁRIO 3.2.8. $\mathbb{Q}$ é enumerável.

DEMONSTRAÇÃO. Como $\mathbb{Z}$ e $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$ são enumeráveis, então $\mathbb{Z} \times \mathbb{Z}^*$ é enumerável. Como $\phi : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}$ dada por $\phi(p, q) = p/q$ é sobrejetiva, então $\mathbb{Q}$ é enumerável. □

Apesar do Corolário 3.2.8 provar que os racionais são enumeráveis, não fica claro como poderíamos de fato "contar" os racionais. O exemplo abaixo mostra uma possibilidade.

EXEMPLO 3.9. $\mathbb{Q}$ é enumerável pela "contagem diagonal":

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

e podemos contar pois

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

COROLÁRIO 3.2.9. Para todo $i \in \mathbb{N}$, seja X_i enumerável. Então $\cup_{i\in\mathbb{N}} X_i$ é enumerável.

DEMONSTRAÇÃO. Seja $X = \cup_{i\in\mathbb{N}} X_i$, e para cada $i \in \mathbb{N}$, seja $f_i : \mathbb{N} \to X_i$ sobrejetiva. Seja $f : \mathbb{N} \times \mathbb{N} \to X$ tal que $f(m, n) = f_m(n)$. Então f é sobrejetiva (mostre). Como $\mathbb{N} \times \mathbb{N}$ é enumerável, então X também o é. □

3.2.2. Conjuntos não enumeráveis. Dizemos que conjuntos A e B têm a mesma cardinalidade (e escrevemos $|A| = |B|$) e existir bijeção $f : A \to B$. Dizemos que $|A| < |B|$ se houver injeção $\phi\, A \to B$ mas não existir sobrejeção $A \to B$.

TEOREMA 3.2.10. *Sejam $X_1, X_2, \dots$ tais que $|X_i| > 1$ para todo $i \in \mathbb{N}$. Então $\Pi_{i\in\mathbb{N}} X_i$ não é enumerável.*

DEMONSTRAÇÃO. Claramente, temos que $\Pi_{i\in\mathbb{N}} X_i$ nao é finito. Por contradição, suponha que $\phi : \mathbb{N} \to \Pi_{i\in\mathbb{N}} X_i$ seja sobrejeção. Então podemos escrever

$$\begin{aligned} \phi(1) &= (x_{1,1}, x_{1,2}, x_{1,3}, \dots), \\ \phi(2) &= (x_{2,1}, x_{2,2}, x_{2,3}, \dots), \\ &\vdots \end{aligned}$$

onde $x_{i,j} \in X_j$. Seja agora $\bar{x} = (\bar{x}_1, \bar{x}_2, \dots)$ tal que $\bar{x}_i \in X_i$ e $\bar{y}_i \neq x_{i,i}$. Logo $\bar{y} \in \Pi_{i\in\mathbb{N}} X_i$ mas $\bar{y} \neq \phi(i)$ para todo $i \in \mathbb{N}$. Então ϕ não pode ser sobrejetiva, uma contradiação. □

EXEMPLO 3.10. 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 $a_i \in \{0, \ldots, 9\}$. Note que esta representação não é única; por exemplo $1,0000\cdots = 0,9999\ldots$. 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 [**21**].

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

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

onde $a_{ij} \in \{0, \ldots, 9\}$. 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 $x_1, x_2, \ldots, x_n, \ldots$ 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. Mostre que a afirmativa do Exemplo 3.3 é verdadeira.

EXERCÍCIO 3.12. Seja X conjunto finito. Mostre que $f : X \to X$ é injetiva se e somente se é sobrejeção.

EXERCÍCIO 3.13. Mostre que a função ξ definida na demonstração do Teorema 3.1.7 é uma bijeção.

EXERCÍCIO 3.14. Faça os detalhes da demonstração do Corolário 3.1.8.

EXERCÍCIO 3.15. Sejam A e B finitos. Construa uma bijeção entre $\{1, 2, \ldots, |A||B|\}$ e $A \times B$.

EXERCÍCIO 3.16. 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 3.17. Mostre que a função construida no Corolário 3.2.2 é de fato bijeção.

EXERCÍCIO 3.18. Prove o Corolário 3.2.4.

EXERCÍCIO 3.19. 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:

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

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

EXERCÍCIO 3.20. 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 3.21. Porque não se pode argumentar como no exemplo 3.10 e concluir erroneamente que os racionais *não* são enumeráveis.

EXERCÍCIO 3.22. 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 3.23. 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 3.24. 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 3.25. 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 3.20).

EXERCÍCIO 3.26. Seja A enumerável e suponha que exista uma função $f : A \to B$ sobrejetiva. Mostre que B é enumerável.

EXERCÍCIO 3.27. 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.

CAPíTULO 4

Corpos Ordenados

[1] Estudaremos o números reais como sendo um corpo ordenado completo, e somente estas propriedades são necessárias.

4.1. Corpos

Um corpo $\{K, +, \cdot\}$ é formado por um conjunto K sobre o qual existem duas operações $+$ e $\cdot$ tais que

(1) A adição $+$ tem as seguintes propriedades:
  (i) associativa: $(x + y) + z = x + (y + z)$
  (ii) comutativa: $x + y = y + x$
  (iii) existe elemento neutro 0 tal que $x + 0 = x$
  (iv) todo elemento $x \in K$ possui elemento simétrico $-x$ tal que $x + (-x) = 0$

(2) A multiplicação $\cdot$ é tal que
  (i) associativa: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
  (ii) comutativa: $x \cdot y = y \cdot x$
  (iii) existe elemento neutro: $1 \cdot x = x$
  (iv) todo elemento $x \in K$, $x \neq 0$ possui elemento inverso x^{-1} tal que $x \cdot x^{-1} = 1$

(3) distributividade: $x \cdot (y + z) = x \cdot y + x \cdot z$

Note que num corpo $(-1) \cdot (-1) = 1$, pois

$$(-1) \cdot (-1) + (-1) \cdot 1 = (-1) \cdot (-1 + 1) = (-1) \cdot 0 = 0.$$

Logo $(-1) \cdot (-1) = -(-1) = 1$.

Os seguintes conjuntos e suas operações formam um corpo.

EXEMPLO 4.1. O conjunto $\mathbb{Q}$ com as operações

$$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'}, \qquad \frac{p}{q} \cdot \frac{p'}{q'} = \frac{p'q'}{qq'}.$$

EXEMPLO 4.2. O conjunto $\mathbb{Q}(t)$ das funções racionais da forma $p(t)/q(t)$, onde $p(t)$ e $q(t)$ são polinômios com $p(t)$ polinômio não nulo. Então $\mathbb{Q}(t)$ é corpo com as operações usuais de somas e multiplicação de funções racionais.

EXEMPLO 4.3. O conjunto $Z_2 = \{0, 1\}$ forma um corpo com as seguintes operações:

$$0 + 1 = 1 + 0 = 1, \qquad 0 + 0 = 1 + 1 = 0, \qquad 0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0, \qquad 1 \cdot 1 = 1.$$

Note neste caso que "$-1 = 1$".

[1] Última Atualização: 29/09/2020

EXEMPLO 4.4. Generalizando o exemplo anterior, definimos o conjunto $Z_p = \{1, 2, \ldots, p-1\}$ com a operação *módulo* p, i.e. dois número m, $n \in \mathbb{Z}$ são iguais se m/p e n/p têm o mesmo resto. Então Z_p é um corpo se p for primo.

OBSERVAÇÃO. Num corpo, se $x^2 = y^2$, então $(x+y)(x-y) = x^2 - y^2 = 0$ e portanto $x = y$ ou $x = -y$.

4.1.1. Corpos Ordenados. Começamos por definir o que é um corpo ordenado.

DEFINIÇÃO 4.1.1. *Dizemos que um corpo K é ordenado se existir conjunto $P \subseteq K$ tal que*

(i) $x, y \in P \implies x \cdot y \in P$ *e* $x + y \in P$
(ii) se $x \in K$ *então uma e apenas uma possibilidade ocorre:*

$$x \in P, \qquad -x \in P, \qquad x = 0.$$

Neste caso, dizemos K é ordenado com ordem P.

Chamamos os elementos de P de *positivos* e os elementos de $-P = \{-x : x \in P\}$ de *negativos*. Note que $K = P \cup -P \cup \{0\}$ e que $P \cap -P = P \cap \{0\} = -P \cap \{0\} = \emptyset$.

4.1.1.1. *Propriedades básicas.* Temos então as seguintes propriedades num corpo ordenado.

LEMA 4.1.2. Seja K corpo ordenado com ordem P. Então valem as seguintes propriedades:

(i) $a \in K$, $a \neq 0 \implies a^2 \in P$
(ii) $1 \in P$
(iii) não existe $a \in K$ tal que $a^2 = -1$

DEMONSTRAÇÃO. Para mostrar (i), note que como $a \neq 0$ então $a \in P$ ou $a \in -P$. Se $a \in P$ então $a^2 = a \cdot a \in P$. Se $a \in -P$ então $-a \in P$. Logo $a^2 = (-a) \cdot (-a) \in P$.

Para ver que $1 \in P$, basta notar que $1 = 1 \cdot 1 = 1^2 \in P$ por (i).

Finalmente, (iii) segue pois $-1 \in -P$ por (ii) e $a^2 \in P$ por (i). Logo não pode ocorrer $a^2 = -1$. □

COROLÁRIO 4.1.3. O corpo dos números complexos $\mathbb{C}$ não é ordenado pois $i^2 = -1$.

EXEMPLO 4.5. Em $\mathbb{Q}$ temos $P = \{p/q : p \cdot q \in \mathbb{N}\}$.

EXEMPLO 4.6. Em $\mathbb{Q}(t)$ temos

$P = \{p(t)/q(t) \in \mathbb{Q}(t) :$ o coeficiente do termo de maior grau de $p(t)q(t)$ é positivo$\}$.

Por exemplo, $3t^5 - 10/(t^3 - 2)$ é positivo, enquanto $-2t^3 - t + 20/(t+2)$ é negativo.

EXEMPLO 4.7. O corpo Z_2 não é ordenado pois $1+1 = 0 \notin P$. De forma análoga, Z_3 não é ordenado pois se o fosse teríamos $1 + 2 = 0$ implica que $2 = -1 \in -P$. Mas $2 + 2 = 1 \in P$

Uma importante propriedade de qualquer corpo ordenado K é que pode-se "inserir" em K os naturais, inteiros e racionais de forma que $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq K$. Seguindo a argumentação de **[9]**, seja $1' \in K$ o elemento neutro da multiplicação. $f : \mathbb{N} \to K$ tal que $f(1) = 1'$, e, por indução, $f(m+1) = f(m) + 1'$. Resulta que $f(2) = 1' + 1'$, $f(3) = 1' + 1' + 1'$, etc. Por construção, $f(m+n) = f(m) + f(n)$ (prova por indução) e como $f(n)$ é positivo, então

$m < n$ implica em $f(m) < f(n)$. Logo f é injetiva e portanto define uma bijeção entre N e sua imagem $\mathbb{N}' = f(\mathbb{N}) \subseteq K$. É prática comum identificar $\mathbb{N}'$ com $\mathbb{N}$ (é o que faremos), obtendo $\mathbb{N} \subseteq K$. Definimos então $\mathbb{Z} \subseteq K$ por

$$\mathbb{Z} = \{-n \in K : n \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}.$$

Finalmente, definimos $\mathbb{Q} \subseteq K$ por

$$\mathbb{Q} = \{p \cdot q^{-1} : p \in \mathbb{Z},\, q \in \mathbb{Z}^*\}.$$

DEFINIÇÃO 4.1.4. *Se K é um corpo ordenado com ordem P, então dizemos que $x < y$ se $y - x \in P$. Analogamente, escrevemos $x > y$ se $x - y \in P$.*

Segue-se da definição que

$$x > 0 \iff x \in P, \qquad x < 0 \iff x \in -P$$

pois $x = x - 0 \in P$ e $-x = 0 - x \in P$. Note ainda que

(i) transitividade: $x < y$ e $y < z \implies x < z$. De fato, como $y - x \in P$ e $z - y \in P$, então $(y - x) + (z - y) \in P$. Logo $z - x \in P$, i.e., $x < z$.
(ii) tricotomia: há uma e somente um possibilidade dentre $x < y$, $x = y$, $x > y$. Para provar isto, basta considerar $y - x$ e usar a propriedade (ii) da Definição 4.1.1.
(iii) monotonicidade da adição: se $x < y$ então $x + z < y + z$ para todo $z \in K$. De fato, se $y - x \in P$ então $(y + z) - (x + z) \in P$.
(iv) monotonicidade da multiplicação: se $x < y$ então $x \cdot z < y \cdot z$ para todo $z \in P$. Basta ver que $y - x \in P$ e $z \in P$ implica em $(y - x) \cdot z \in P$. Logo $y \cdot z - x \cdot z \in P$.

Definições e propriedade semelhantes valem para $\leq$, $\geq$, $>$.

OBSERVAÇÃO. Note que num corpo ordenado K, como $1 > 0$, então

$$0 < 1 < 1 + 1 < 1 + 1 + 1 < 1 + 1 + 1 + 1 < \cdots .$$

Portanto K contém infinitos elementos, i.e., não existe corpo ordenado finito.

4.1.2. Intervalos e módulos. Dado um corpo ordenado K, e a, $b \in K$, com $a < b$, definimos os seguintes *intervalos*:

(1) $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
(2) $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
(3) $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
(4) $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$
(5) $[a, +\infty) = \{x \in \mathbb{R} : a \leq x\}$
(6) $(a, +\infty) = \{x \in \mathbb{R} : a < x\}$
(7) $(-\infty, b] = \{x \in \mathbb{R} : x \leq b\}$
(8) $(-\infty, b) = \{x \in \mathbb{R} : x < b\}$
(9) $(-\infty, +\infty) = K$

Os quatro primeiros intervalos acima são limitados. O primeiro é fechado, o segundo aberto, o terceiro fechado à esquerda e aberto à direita, o quarto aberto à direita e fechado à esquerda. Os intervalos (5-10) são semi-retas, onde (5) é fechada à esquerda, etc. Para $a = b$ definimos $[a, b] = \{a\}$, um intervalo dito *degenerado* (os demais são chamados de não-degenerados).

Observação. Alguns autores chamam alguns intervalos particulares de segmentos. A notação] e [é por vezes utilizada no lugar de (e); por exemplo $]a, b[= (a, b)$, etc **[3, 9, 19]**.

A seguir apresentamos uma propriedade importante a respeito de intervalos.

Lema 4.1.5. Todo intervalo não degenerado é infinito.

Demonstração. Sem perda de generalidade, seja $a < b$ e (a, b) intervalo. Seja $x_1 = (a + b)/2$. Então $a < x_1$ e $x_1 < b$. De forma indutiva, defina $x_{n+1} = (a + x_n)/2$, e portanto $a < x_{n+1}$ e $x_{n+1} < x_n$. Obtemos desta forma

$$a < \cdots < x_{n+1} < x_n < \cdots < x_3 < x_2 < x_1 < b.$$

Então o conjunto infinito $\{x_1, x_2, x_3, \ldots, x_n, x_{n+1}, \ldots\} \subseteq (a, b)$. Logo (a, b) é infinito. □

Definimos a seguir a função *módulo* (ou valor absoluto) $|\cdot| : K \to P \cup \{0\}$ dada por

$$|x| = \begin{cases} x & \text{se } x \in P, \\ 0 & \text{se } x = 0, \\ -x & \text{se } x \in -P. \end{cases}$$

Outra forma de escrever a função módulo é $|x| = \max\{-x, x\}$, onde

$$\max\{-x, x\} = \begin{cases} -x & \text{se } x \in -P, \\ x & \text{se } x \in P. \end{cases}$$

Algumas propriedades desta função são, para todo a, $b \in K$:

(i) $|-a| = |a|$: se $a = 0$, então $|0| = 0 = |-0|$. Se $a > 0$, então $-a < 0$ e logo $|-a| = -(-a) = a = |a|$. Se $a < 0$, então $-a > 0$ e $|-a| = -a = |a|$.

(ii) $|ab| = |a||b|$: note que $x^2 = |x|^2$ e então

$$|xy|^2 = (xy)^2 = x^2y^2 = |x|^2|y|^2 = (|x||y|)^2.$$

Portanto $|xy| = |x||y|$ ou $|xy| = -|x||y|$. Como $|xy|$ e $|x||y|$ são positivos, então $|xy| = |x||y|$.

(iii) Dados a, $k \in K$ são equivalentes:
(a) $-k \leq a \leq k$
(b) $a \leq k$ e $-a \leq k$
(c) $|a| \leq k$
Para provar $(a) \implies (b)$ basta notar que se $-k \leq a \leq k$, então $-k \leq a$ e $a \leq k$. Logo $k \geq -a$. Para provar $(b) \implies (c)$, note que $\max\{a, -a\} \leq k$ e então $|a| \leq k$. Finalmente $(c) \implies (a)$ segue pois $|a| = \max\{a, -a\} \leq k$ implica em $a \leq k$ e $-a \leq k$. Logo $a \geq -k$.

(iv) $-|a| \leq a \leq |a|$: tome $k = |a|$ no ítem (iii) acima. Então $|a| \leq |a| \implies -|a| \leq a \leq |a|$.

Outra propriedade que segue das acima citados é a equivalência

$$|x - a| < b \iff a - b \leq x \leq a + b.$$

De fato,

$$|x - a| < b \iff -b \leq x - a \leq b \iff a - b \leq x \leq a + b.$$

Lema 4.1.6 (Desigualdade Triangular). Para todo a, $b \in K$ temos

$$|a + b| \leq |a| + |b|.$$

DEMONSTRAÇÃO. Sabemos que $-|a| \leq a \leq |a|$ e $-|b| \leq b \leq |b|$. Logo,

$$-|a| - |b| \leq a + b \leq |a| + |b|,$$

que é equivalente a $|a + b| \leq |a| + |b|$, como queríamos demonstrar. □

Finalmente valem as desigualdades

$$|x| - |y| \leq$$

A definição de alguns intervalos particulares é imediata usando-se o módulo:

$$(a - d, a + d) = \{x \in \mathbb{R} : |x - a| < d\}, \qquad [a - d, a + d] = \{x \in \mathbb{R} : |x - a| \leq d\},$$

4.1.3. Cotas, supremo, ínfimo. Relembramos aqui os conceitos de *conjuntos limitados* e de *cota superior e cota inferior*.

DEFINIÇÃO 4.1.7. *Considere um conjunto $A \subseteq K$. Dizemos que $c^* \in K$ é* cota superior *de A se $a \leq c^*$ para todo $a \in A$. Analogamente, dizemos que $c_* \in K$ é* cota inferior *de A se $c_* \leq a$ para todo $a \in A$. Se um conjunto tem cota superior dizemos que ele é* limitado por cima ou superiormente. *Se um conjunto tem cota inferior dizemos que ele é* limitado por baixo ou inferiormente. *Se um conjunto tem cota superior e inferior, dizemos que ele é limitado.*

Segue-se da definição que se um conjunto possui cota superior, então ele possui infinitas cotas superiores:

$$c^* \text{ cota superior de } A \implies c^* + 1 \text{ cota superior de } A.$$

Observação análoga vale para as cotas inferiores.

EXEMPLO 4.8. Por exemplo $A \subseteq \mathbb{N} \subseteq K$ possui cota inferior, pois possui elemento mínimo pelo Princípio da boa ordenação. Para $a < b$ elementos de K, intervalos da forma $(a, b]$ por exemplo tem a como cota inferior e b como cota superior.

EXEMPLO 4.9. Note que qualquer número é cota inferior e superior do conjunto vazio.

Uma propriedade importante que alguns corpos possuem é $\mathbb{N}$ ser ilimitado. Corpos ordenados com esta propriedade são chamados de *corpos arquimedianos*.

Note que nem todo corpo ordenado é arquimediano. Por exemplo, $Q(t)$ com a ordenação definida no Exemplo 4.6 é tal que $n < t$ para todo $n \in \mathbb{N}$. Logo $\mathbb{N}$ é limitado superiormente, com t sendo uma cota superior.

Um corpo ordenado é arquimediano se possuir uma das propriedades descritas no teorema a seguir.

TEOREMA 4.1.8. *Seja K corpo ordenado e $\mathbb{N} \subset K$. Então são equivalentes:*

(1) $\mathbb{N}$ não é limitado superiormente
(2) para todo a, $b \in K$ e $a > 0$ existe $n \in \mathbb{N}$ tal que $na > b$
(3) para todo $a > 0$ existe $n \in \mathbb{N}$ tal que $0 < 1/n < a$

DEMONSTRAÇÃO. $(i) \implies (ii)$: seja $a, b \in K$, com $a > 0$. Então b/a não é cota superior de $\mathbb{N}$, e portanto existe $n \in \mathbb{N}$ tal que $n > b/a$.

$(ii) \implies (iii)$: por hipótese, existe $n \in \mathbb{N}$ tal que $na > 1$. Logo $1/ > 0$ e $1/n < a$.

$(iii) \implies (i)$: Para todo $b \in K$ existe $n \in \mathbb{N}$ tal que $1/n < 1/b$, i.e., $b < n$. Então b não é cota superior de $\mathbb{N}$. □

Da definição de cotas, derivamos o conceito de supremos e ínfimos.

DEFINIÇÃO 4.1.9. *Se um conjunto $A \subset K$ é não vazio e limitado superiormente, chamamos de* supremo de A *ou simplesmente* $\sup A$ *a menor de suas cotas superiores, se existir. Analogamente, se um conjunto A é não vazio e limitado por baixo, chamamos de* ínfimo de A *ou simplesmente* $\inf A$ *a maior de suas cotas inferiores, se existir.*

Logo, se $s^* = \sup A$, então

(1) $a \leq s^*$ para todo $a \in A$.
(2) Se existe $v \in K$ tal que $a \leq v$ para todo $a \in A$, então $s^* \leq v$.

OBSERVAÇÃO. Segue-se da definição a unicidade do supremo e do ínfimo, se estes existirem, ver Exercício 4.7.

EXEMPLO 4.10. Considere os seguintes exemplos:

(i) Note que $\emptyset \subset K$ não possui nem sup nem inf, pois todo elemento de K é cota superior e inferior de $\emptyset$.
(ii) Se $X \subset K$ possuir elemento máximo, então este será o supremo de X. Em particular, todo conjunto finito possui ínfimo e supremo.
(iii) Seja $a < b \in K$. Se $Y = [a, b)$ então $b > y$ para todo $y \in X$ e portanto b é cota superior de Y. Para mostrar que b é supremo, vamos mostrar que $\bar{y}$, tal que $a < \bar{y} < b$, não pode ser cota superior de X. De fato seja $y' = (\bar{y} + b)/2$. Então $y' \in [a, b)$ com $y' > \bar{y}$. Logo $\bar{y}$ não é cota superior, e b é a menor das cotas superiores. Logo $b = \sup[a, b)$.
(iv) Se $X = [a, b]$ então $\inf X = a$ e $\sup X = b$, por argumentos análogos aos acima apresentados.

Observe pelos exemplos (iii) e (iv) acima que os supremos e ínfimos podem ou não pertencer ao conjunto.

O resultado a seguir nos dá uma forma equivalente para determinar o supremo de um conjunto.

LEMA 4.1.10. Seja A não vazio e s^* cota superior de A. Então $s^* = \sup A$ se e somente se para todo $\epsilon > 0$ existir $a_\epsilon \in A$ tal que $s^* - \epsilon < a_\epsilon$.

DEMONSTRAÇÃO. ($\Rightarrow$) Seja $s^* = \sup A$ e $\epsilon > 0$. Como $s^* - \epsilon < s^*$, então $s^* - \epsilon$ não é cota superior de A. Logo, existe um elemento $a_\epsilon \in A$ tal que $a_\epsilon > s^* - \epsilon$.

($\Leftarrow$) Seja s^* cota superior de A. Suponha que para todo ϵ exista $a_\epsilon \in A$ tal que $s^* - \epsilon < a_\epsilon$. Vamos então mostrar que $s^* = \sup A$.

Seja c^* cota superior de A com $c^* \neq s^*$. Se $c^* < s^*$, definimos $\epsilon = s^* - c^*$ e então $\epsilon > 0$ e existe $a_\epsilon \in A$ tal que $a_\epsilon > s^* - \epsilon = c^*$. Isto é uma contradição com o fato de c^* ser cota superior. Logo temos obrigatoriamente $c^* > s^*$, e s^* é a menor das cotas superiores, i.e., $s^* = \sup A$. □

4.2. Exercícios

EXERCÍCIO 4.1. Mostre que num corpo, o 0 não possui inversa multiplitiva.

EXERCÍCIO 4.2. Prove que num corpo existe um único elemento neutro da adição, um único elemento neutro da multiplicação, todo $x \neq 0$ possui um único inverso aditivo e um um único inverso multiplicativo.

EXERCÍCIO 4.3. Mostre que num corpo K com ordem P,

(1) se a, $b \in -P$ então $a + b \in -P$
(2) se $a \in -P$ e $c \in P$, então $a \cdot c \in -P$
(3) se $c \in P$, então $c^{-1} \in P$

EXERCÍCIO 4.4. Mostre que se $x > y > 0$ num corpo K, então $x^{-1} < y^{-1}$. E que se $x^2 + y^2 = 0$, então $x = y = 0$.

EXERCÍCIO 4.5. Mostre que o conjunto P definido no Exemplo 4.6 define de fato uma ordem.

EXERCÍCIO 4.6. Seja K corpo ordenado, $A \subseteq K$ e as funções $f : A \to K$ e $g : A \to K$ sejam tais que os conjuntos $f(A)$ e $g(A)$ sejam limitados superiormente e que tenham supremo. Defina a função $f + g : A \to K$ por $(f + g)(x) = f(x) + g(x)$ e suponha que $\sup(f + g)(A)$ exista. Mostre que $\sup(f + g)(A) \leq \sup f(A) + \sup g(A)$. Dê um exemplo em que a desigualdade é estrita.

EXERCÍCIO 4.7. Seja $A \subseteq K$ conjunto limitado. Mostre que $\inf A$ e $\sup A$, quando estes existem, são únicos.

EXERCÍCIO 4.8. Mostre que nenhum corpo é limitado superiormente ou inferiormente.

CAPíTULO 5

Os números reais

[1] Neste capítulo, falaremos sobre números reais. Suporemos aqui que os números reais e as operações neles definidas são bem definidos e "existem", sem entrar em detalhes sobre a construção deste corpo. A idéia é apenas apresentar propriedades que os reais satisfazem.

5.1. Introdução

Vamos ver primeiro que nem sempre um conjunto limitado num corpo ordenado possui supremo ou ínfimo. Considere primeiro os seguintes resultados.

LEMA 5.1.1 (Pitágoras). Não existe $x \in \mathbb{Q}$ tal que $x^2 = 2$

DEMONSTRAÇÃO. Por contradição suponha que $p \in \mathbb{Z}$ e $q \in \mathbb{Z}^*$ sejam primos entre si e que $(p/q)^2 = 2$. Então $p^2 = 2q^2$ e portanto p é par. Seja $p = 2\bar{p}$. Então $4\bar{p}^2 = 2q^2$, i.e., $2\bar{p}^2 = q^2$ e q é par. Uma contradição com p e q serem primos entre si. □

Considere os conjuntos

$$X = \{x \in \mathbb{Q} : x \geq 0 \text{ e } x^2 < 2\}, \qquad Y = \{x \in \mathbb{Q} : x > 0 \text{ e } x^2 > 2\}. \tag{5.1.1}$$

Temos então os seguintes resultados

LEMA 5.1.2. Sejam X e Y como em (5.1.1). Então

(i) X não possui elemento máximo.
(ii) Y não possui elemento mínimo.
(iii) Todo elemento de Y é cota superior de X.

DEMONSTRAÇÃO. Ver [**9**]. □

O resultado a seguir garante a existência de conjuntos sem supremo.

LEMA 5.1.3. Seja X definido em (5.1.1). Então não existe supremo de X em $\mathbb{Q}$.

DEMONSTRAÇÃO. Suponha que exista $a \in X$ com $a = \sup X$. Então $a > 0$ pois $1/2 \in X$. Note que $a \notin X$, pois se fosse, a seria elemento máximo de X, e este não existe, segundo o ítem (i) do Lema 5.1.2. Logo $a^2 \geq 2$.

Suponha agora que $a^2 > 2$. Então $a \in Y$, onde Y é definido em (5.1.1). Entretanto, todo elemento de Y é cota superior de X (ítem (iii) do Lema 5.1.2), então temos que ter a elemento mínimo de Y (pois a é sup de X). Como não existe elemento de mínimo de Y (ítem (ii) do Lema 5.1.2), então $a \notin Y$. Logo $a^2 \leq 2$.

De $a^2 \geq 2$ e $a^2 \leq 2$ concluímos que $a^2 = 2$, um absurdo pois $a \in \mathbb{Q}$ contradiz o Lema 5.1.1. □

[1] Última Atualização: 29/09/2020

Da discussão acima, vemos que há corpos onde conjuntos limitados superiormente não possuem supremo. O mesmo vale para conjuntos limitados inferiormente e sem ínfimo.

5.2. Os números Reais

Dizemos que um corpo ordenado K é *completo* se para todo subconjunto de K não vazio limitado superiormente existe supremo.

AXIOMA 5.2.1 (Existência dos reais). Existe um corpo ordenado completo $\mathbb{R}$ chamado *corpo dos reais*.

Por ser completo, o conjunto dos reais possuem então uma propriedade *fundamental*, que o distingue por exemplo dos racionais, o fato de ser completo. Chamamos esta propriedade de *propriedade do supremo em* $\mathbb{R}$

5.2.1. Propriedades dos Reais. Sendo um corpo ordenado, $\mathbb{R}$ não é limitado nem superiormente nem inferiormente. Além disto, temos as inclusões $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Uma surpreendente consequência do $\mathbb{R}$ ser completo é que é torna-se também *arquimediano*, como mostra o resultado abaixo.

LEMA 5.2.2 (Propriedade arquimediana). Para todo $x \in \mathbb{R}$, existe $n \in \mathbb{N}$ tal que $n > x$.

DEMONSTRAÇÃO. (Por contradição.) Seja $x \in \mathbb{R}$ e suponha que não exista n tal que $n > x$. Portanto, x é cota superior de $\mathbb{N} \subseteq \mathbb{R}$. Pela Propriedade do supremo de $\mathbb{R}$, então $\mathbb{N}$ tem um supremo s. Logo existe $m \in \mathbb{N}$ tal que $s - 1 < m$. Mas então, $s < m + 1$, uma contradição, pois $m + 1 \in \mathbb{N}$ e s deveria ser cota superior de $\mathbb{N}$. □

OBSERVAÇÃO. Densidade de $\mathbb{Q}$ em $\mathbb{R}$: Se x, $y \in \mathbb{R}$ e $x < y$, então existe $r \in \mathbb{Q}$ tal que $x < r < y$. Da mesma forma, existe $r \in \mathbb{R}\backslash\mathbb{Q}$ tal que $x < r < y$.

5.2.2. Intervalos Encaixantes. Uma importante propriedade dos números reais, intrinsicamente ligada à sua própria definição, é dada por interseções de intervalos encaixantes, noção que discutimos a seguir.

DEFINIÇÃO 5.2.3. *Dizemos que uma sequência de intervalos I_n é encaixante se*

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots \supseteq I_n \supseteq \ldots$$

Nos dois exemplos abaixo, ilustramos o fato de que interseções de intervalos encaixantes podem ser vazias ou não. Entretanto, quando os intervalos forem fechados e limitados, o Teorema dos intervalos encaixantes abaixo garante que estas interseções são sempre não vazias.

EXEMPLO 5.1. Se $I_n = [0, 1/n]$ então $\cap_{n=1}^{\infty} I_n = \{0\}$. De fato, $0 \in I_N$ para todo $n \in \mathbb{N}$ e portanto $0 \in \cap_{n=1}^{\infty} I_n$. Por outro lado, para $x \in \mathbb{R}$ não nulo a Propriedade arquimediana (Lema 5.2.2) garante a existência de $n \in \mathbb{N}$ tal que $x \notin I_n$. Logo $x \notin \cap_{n=1}^{\infty} I_n$.

EXEMPLO 5.2. Usando novamente a Propriedade arquimediana (Lema 5.2.2) temos que se $I_n = (0, 1/n)$ então $\cap_{n=1}^{\infty} I_n = \emptyset$.

TEOREMA 5.2.4 (Teorema dos intervalos encaixantes). *Sejam $I_n = [a_n, b_n]$ intervalos fechados, limitados, não vazios e encaixantes. Então existe $\xi \in \mathbb{R}$ tal que $\xi \in \cap_{n=1}^{\infty} I_n$. Além disto, se $\inf\{b_n - a_n : n \in \mathbb{N}\} = 0$, então ξ é o único elemento da interseção.*

DEMONSTRAÇÃO. Segue-se das hipóteses que para todo $n \in \mathbb{N}$ temos

$$a_{n+1} \geq a_n, \qquad b_{n+1} \leq b_n, \qquad a_n \leq b_n. \tag{5.2.1}$$

Temos $b_1 \geq a_n$ para todo n pois $I_n \subseteq I_1$. Seja $\xi = \sup\{a_n : n \in \mathbb{N}\}$. Logo $\xi \geq a_n$ para todo n. Queremos mostrar agora que $\xi \leq b_n$ para todo n. Suponha o contrário, i.e., que exista $b_k < \xi$ para algum k. Logo $b_k < a_m$ para algum m. Seja $p = \max\{k, m\}$. Então $a_p \geq a_m > b_k \geq b_p$, uma contradição com (5.2.1). Logo $a_n \leq \xi \leq b_n$ para todo $n \in \mathbb{N}$ e portanto $\xi \in I_n$ para todo $n \in \mathbb{N}$.

Supondo agora que $\inf\{b_n - a_n : n \in \mathbb{N}\} = 0$, definimos $\eta = \inf\{b_n : n \in \mathbb{N}\}$. Então $\eta \geq a_n$ para todo $n \in \mathbb{N}$ e $\eta \geq \xi$. Como $0 \leq \eta - \xi \leq b_n - a_n$ para todo $n \in \mathbb{N}$, temos $\eta = \xi$ pois $\inf\{b_n - a_n : n \in \mathbb{N}\} = 0$ (ver exercício 5.11). Finalmente, seja $x \in \cap_{n=1}^{\infty} I_n$. Como $x \geq \xi = \eta$ e $x \leq \eta = \xi$, então $x = \xi = \eta$ é o único ponto em $\cap_{n=1}^{\infty} I_n$. □

5.3. Exercícios

EXERCÍCIO 5.1. Mostre que todo intervalo da reta não degenerado contém infinitos elementos.

EXERCÍCIO 5.2. Prove a afirmativa do exemplo 4.9.

EXERCÍCIO 5.3. Se $A \subseteq \mathbb{R}$ é um conjunto não vazio e limitado, então $A \subseteq [\inf A, \sup A]$.

EXERCÍCIO 5.4. Enuncie e demonstre o resultado análogo ao Lema 4.1.10 no caso do ínfimo.

EXERCÍCIO 5.5. Suponha que A e B sejam dois conjuntos de números reais limitados superiormente, e que toda cota superior de A seja cota superior de B. Mostre que $\sup A \geq \sup B$.

EXERCÍCIO 5.6. Sejam A e B dois conjuntos não vazios de $\mathbb{R}$ limitados superiormente, e seja o conjunto $C = \{a + b : a \in A,\, b \in B\}$ formado pela soma dos elementos de A com os elementos de B. Mostre que $\sup C = \sup A + \sup B$.

EXERCÍCIO 5.7. Seja $A \subset \mathbb{R}^n$ não vazio, e $f : \mathbb{R}^n \to \mathbb{R}$ dada por

$$f(\mathbf{x}) = \inf\{\|\mathbf{x} - \mathbf{y}\| : \mathbf{y} \in A\}.$$

Mostre que f está bem definida. Construa entretanto um exemplo onde não exista $\mathbf{y} \in A$ tal que $f(\mathbf{x}) = \|\mathbf{x} - \mathbf{y}\|$, para algum $\mathbf{x} \in \mathbb{R}^n$.

EXERCÍCIO 5.8 (Densidade dos racionais nos reais). Mostre que dados x, $y \in \mathbb{R}$ com $x < y$, existe $r \in \mathbb{Q}$ tal que $x < r < y$.

EXERCÍCIO 5.9. Faça os detalhes do exemplo 5.2.

EXERCÍCIO 5.10. Mostre que intervalos encaixantes não limitados podem ter interseção vazia.

EXERCÍCIO 5.11. Usando a notação do Teorema 5.2.4, mostre que $\inf\{b_n - a_n : n \in \mathbb{N}\} = 0$ se e somente se $\inf\{b_n : n \in \mathbb{N}\} = \sup\{a_n : n \in \mathbb{N}\}$.

EXERCÍCIO 5.12. Aponte na demonstração do Teorema 5.2.4 quais o(s) argumento(s) que não é (são) válido(s) se considerarmos uma sequência encaixante de intervalos abertos.

EXERCÍCIO 5.13. Usando o teorema dos intervalos encaixantes, mostre que $\mathbb{R}$ não é enumerável. (Sugestão: considere $E = \{x_1, x_2, \dots\} \subseteq [0,1]$, e construa um intervalo do tipo $I_1 = [a_1, b_1]$ tal que $x_1 \notin I_1$. Indutivamente, construa intervalo $I_j = [a_j, b_j] \subset I_{j-1}$ tal que $x_j \notin I_j$. Conclua então que $[0,1]$ não é enumerável).

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] Efe A. Ok, *Real analysis with economic applications*, Princeton University Press, Princeton, NJ, 2007. MR2275400

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

[19] 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)

[20] 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)

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

[22] ———, *Analysis. II*, Texts and Readings in Mathematics, vol. 38, Hindustan Book Agency, New Delhi, 2006. MR2195041 (2006g:26002b)
[23] *Monkey saddle — Wikipedia, The Free Encyclopedia*, Wikipedia (2009).
[24] 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)