Universidade Federal de Sergipe
Centro de Ciencias Exatas e Tecnologia
Departamento de Matemática

Material Didático para a disciplina

Fundamentos de Matemática

Paulo de Souza Rabelo

Aracaju - SE
2013

Sumário

CAPÍTULO 1

Introdução

O que é Lógica? Lógica é a ciência que estuda pricípios e métodos de inferência, tendo o objetivo principal de determinar em que condições certas coisas se seguem (são consequências), ou não, de outras. Obviamente, como definição, isso deixa bastante a desejar: precisamos explicitar o que é "inferência", por exemplo, e o que se quer dizer com "se seguem"ou "consequência".

Vamos começar com o problema apresentado no seguinte mini-conto de fadas:

> Há não muito tempo atrás, num país distante, havia um velho rei que tinha três filhas, inteligentíssimas e de indescritível beleza, chamadas Guilhermina, Genoveva e Griselda. Sentindo-se perto de partir desta para melhor, e sem saber qual das filhas designar como sua sucessora, o velho rei resolveu submetê-las a um teste. A vencedora não apenas seria a nova soberana, como ainda receberia a senha da conta secreta do rei (num banco suíço), além de um fim de semana, com despesas pagas, na Disneylândia. Chamando as filhas à sua presença, o rei mostrou-lhes cinco pares de brincos, idênticos em tudo com exceção das pedras neles engastadas: três eram de esmeralda, e dois de rubi. O rei vendou então os olhos das moças e, escolhendo ao acaso, colocou em cada uma delas um par de brincos. O teste consistia no seguinte: aquela que pudesse dizer, sem sombra de dúvida, qual o tipo de pedra que havia em seus brincos herdaria o reino (e a conta na Suíça, etc.).
>
> A primeira que desejou tentar foi Guilhermina, de quem foi removida a venda dos olhos. Guilhermina examinou os brincos de suas irmãs, mas não foi capaz de dizer que tipo de pedra estava nos seus (e retirou-se, furiosa). A segunda que desejou tentar foi Genoveva. Contudo, após examinar os brincos de Griselda, Genoveva se deu conta de que também não sabia determinar se seus brincos eram de esmeralda ou rubi e, da mesma forma que sua irmã, saiu batendo a porta. Quanto a Griselda, antes mesmo que o rei lhe tirasse a venda dos olhos, anunciou corretamente, alto e bom som, o tipo de pedra de seus brincos, dizendo ainda o porquê de sua afirmação. Assim, ela herdou o reino, a conta na Suíça e, na viagem à Disneylândia, conheceu um jovem cirurgião plástico, com quem se casou e foi feliz para sempre.

Agora, um probleminha para você resolver: que brincos tinha Griselda, de esmeralda ou de rubi? Pense e responda! Já de volta? Bem, espero que voce tenha feito o esforço e descoberto que os brincos de Griselda eram de esmeralda. Contudo, responder ao exercício dizendo apenas

que os brincos eram de esmeralda não é suficiente: voce poderia ter tido um palpite feliz, acertando simplesmente por sorte. Para me convencer de que você sabe mesmo a resposta, voce tem de expor as **razões** que o/a levaram a concluir que os brincos eram de esmeralda; voce tem de **justificar** essa sua afirmação. Note que as princesas também estavam obrigadas a fazer isto: o velho rei não estava interessado em que uma delas acertasse a resposta por acaso.

Ora, enquanto tentava resolver o problema, você deve ter tomado vários pontos de partida e pode ter seguido por vários caminhos à busca de solução. A esse processo de busca vamos chamá-lo de **raciocínio**, ou de processo de inferência. Basicamente, raciocinar, ou fazer inferências, consite em "manipular"a informação disponível - aquilo que sabemos ou supomos ser verdadeiro - e extrair consequências disso, obtendo informação nova. O resultado de um processo (bem sucedido) de inferência é que você fica sabendo algo que não sabia antes: que os brincos de Griselda são de esmeralda; que o assassino foi o mordomo; que o melhor time do país é o Vasco. É claro que este processo também pode terminar num fracasso!

Porém, a Lógica não procura dizer como as pessoas raciocinam, mas se interessa primeiramente pela questão de se aquelas coisas que sabemos (o ponto de partida do processo), de fato constituem uma boa razão para aceitar a conclusão alcançada, isto é, se a conclusão é uma consequência daquilo que sabemos (nossas hipóteses). A importância de uma boa justificativa vem do fato de que muitas vezes cometemos erros de raciocínio, chegando a uma conclusão que simplesmente não decorre da informação disponível. E, claro, há contextos nos quais uma afirmação só pode ser aceita como verdadeira se muito bem justificada: na ciência de um modo geral, por exemplo, ou em um tribunal (onde alguém só pode ser condenado se não houver dúvida quanto a sua culpa).

Com relação ao problema dos brincos das princesas, uma justificação de que os brincos de Griselda são de esmeralda pode ser algo como o que se segue:

> Existem apenas dois pares de brincos de rubi; logo, se tanto Genoveva quanto Griselda estivessem com brincos de rubi, Guilhermina, a primeira, saberia que os seus são de esmeralda. Guilhermina, contudo, não soube dizer qual o tipo de pedra em seus brincos. Logo, ou Genoveva e Griselda tinham ambas brincos de esmeralda, ou uma tinha brincos de rubi e a outra, de esmeralda. Mas disso se segue agora que, se Griselda tivesse brincos de rubi, Genoveva, a segunda, teria visto isso, e saberia que os seus são de esmeralda. Genoveva, contudo, também não soube dizer qual o tipo de pedra em seus brincos. Logo, Griselda não tinha brincos de rubi, ou seja, seus brincos eram de esmeralda.

Essa listagem de razões mostrando como deduzir, ou como demonstrar, a partir dos dados do problema, a conclusão a respeito de qual pedra estava nos brincos de Griselda, é o que chamamos de **argumento**.

O objetivo nessa disciplina é mostrar que existem argumentos, considerados válidos, de uso frequente em matemática, seja para resolvermos problemas ou provarmos determinadas afirmações (teoremas). A veracidade desses argumentos estará baseada em princípios lógicos (primeira parte do curso) e será verificada através de tabelas-verdade, regras de inferencia e árvores de refutação. Veremos as vantagens e desvantagens da cada um desses métodos. Na

sequência, estudaremos alguns argumentos de prova/resolução, exemplificando-os com matemática elementar: noções de divisibilidade, do que é ser um número par, ímpar, racional, irracional, primo, etc.

Por fim, estudaremos tópicos que permearão a vida acadêmica do aluno e são fundamentais em matemática: conjuntos, relações, funções e cardinalidade.

Quase nada do escrito nessas notas é de minha autoria: ela é uma colagem de diversas partes dos livros citados nas referências. Muito conteúdo veio do livro do Bloch [1]. O interesse é proporcionar aos alunos uma fonte de leitura em português, já que há poucos livros nesse idioma que contemple satisfatoriamente a ementa da disciplina - em geral, livros de matemática discreta. Por outro lado, há uma extensa literatura em inglês.

CAPÍTULO 2

Noções de Lógica

Lógica Matemática encontra aplicações em muitas áreas de computação. As leis da lógica são empregadas no design de circuitos digitais, inteligência artificial, programação de computadores e de linguagens, banco de dados relacionais, etc.

Para entender matemática, devemos entender o que faz um argumento correto, isto é, uma prova. Uma vez provado que uma afirmação matemática é verdadeira, chamamos ela um teorema. Uma coleção de teoremas sobre um tópico organiza o que sabemos sobre esse tópico. Provas jogam um papel essencial quando verificamos que programas computacionais produzem uma saída correta para todos os valores de entrada, quando estabelecemos a segurança de um sistema e quando criamos inteligência artificial. Sistemas autômatos têm sido construídos permitindo que computadores produzam suas próprias provas.

Nesta primeira parte estudaremos o que faz um argumento correto e introduzimos ferramentas para construir esses argumentos. Desenvolveremos um arsenal de métodos de provas diferentes que nos capacitarão a provar diversos resultados ou resolver problemas. Será suficiente para nossos propósitos apresentar os conceitos de modo informal.

2.1 Cálculo Proposicional

Uma característica especial que distingue matemática de outras ciências é o tipo de raciocínio utilizado. Cientistas fazem observações de casos particulares ou fenômenos e buscam uma teoria geral que descreve ou explica as observações. Esta visão é chamada **raciocínio indutivo**, e é testada por fazer outras observações. Se os resultados são incompatíveis com as expectativas teóricas, o cientista usualmente rejeita ou modifica a teoria.

Matemáticos também usam, com frequência, o raciocínio indutivo para descrever modelos e relações entre quantidades e estruturas. Mas o que caracteriza o pensamento do matemático é o **raciocínio dedutivo**, no qual usamos lógica para retirar conclusões baseadas em afirmações aceitas como verdadeiras. Se os resultados de alguma teoria matemática são incompatíveis com a realidade, a falha não está na teoria, mas nas hipóteses tomadas. Assim, o matemático não está restrito ao campo do fenômeno observável.

Os objetos fundamentais em lógica são as proposições.

Definição 2.1.1. *Uma proposição é uma afirmação que é verdadeira ou falsa, mas não ambas.*

Exemplo 2.1.2. *(1)* $\sqrt{2}$ *é um número irracional;*

(2) Todo triângulo é isósceles;

(3) Que horas são?

(4) $x+1=2$*;*

(5) Existem infinitos números primos;

(6) Vixe Maria!

(7) Esta afirmação é falsa.

Questões imperativas e exclamativas não são proposições. A afirmação (4) pode ser verdadeira ou falsa, dependendo do valor de x associado. Ela é um **predicado** (uma afirmação contendo uma ou mais variáveis). A afirmação (7) faz uma referência a si mesma, tornando impossível atribuir-lhe um valor: se assumirmos sua veracidade, então a sentença afirma que é falsa, e da mesma forma, ao assumirmos ela como falsa, encontramos que ela é verdadeira. Isto é um exemplo de um **paradoxo**. O estudo de paradoxos exerce um papel chave no desenvolvimento da lógica moderna. As demais afirmações são proposições.

No estudo de lógica, usamos letras para representar proposições simples (ou atômicas), tais como P, Q, R e S; e atribuímos o valor V ou F a uma proposição se ela for verdadeira ou falsa, respectivamente. O que faz a lógica interessante é que existem vários modos úteis de formar novas proposições a partir das antigas. Para isso usamos os chamados **conectivos lógicos**. Com

CONECTIVO	SÍMBOLO
e (conjunção)	$\wedge$
ou (disjunção)	$\vee$
não (negação)	$\sim$ ou $\neg$
se, $\cdots$ então (condicional ou implicacão)	$\rightarrow$ ou $\Rightarrow$
se, e somente se (bicondicional)	$\leftrightarrow$ ou $\Leftrightarrow$

Tabela 2.1 Conectivos lógicos

exceção do "não"$(\sim)$, os símbolos para esses conectivos são escritos entre duas proposições. A veracidade de uma proposição composta depende da verdade de suas componentes. Estudemos cada um desses conectivos.

2.1.1 Conjunção

Se um aluno chegasse para o professor e dissesse: "Não tenho tempo para lazer, pois trabalho e estudo". Em que situação o professor diria: "Voce está mentindo!"? E em qual situação o aluno estaria dizendo a verdade?

> **Numa conjunção, se P e Q são proposições, então $P \wedge Q$ é uma afirmação verdadeira quando ambos, P e Q, são verdadeiros, e falsa caso contrário.**

Esta afirmação é usualmente apresentada na forma de uma **tabela-verdade**, na qual são exibidas todas as possibilidades para os valores de P e Q (ver Tabela 2.2).

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Tabela 2.2 Tabela-verdade para a conjunção

Exemplo 2.1.3. *(1) Trabalho como professor de matemática no Estado e no município.*

(2) O número 2 é um número primo e um número par.

(3) Três é maior que 1 e menor que 5.

Observação 2.1.4. *Notemos que o número de possibilidades para uma proposição composta por n proposições é* 2^n.

2.1.2 Disjunção

Consideremos as seguintes afirmações:

(1) Atlético ou Fluminense vencerá a libertadores.

(2) Eu vou comer um hambúrguer ou uma pizza.

Em que sentido elas são válidas? A afirmação (1) é dita está na forma **exclusiva**, significando que "ou um ou outro, mas não ambos". Em matemática, usamos a disjunção na forma **inclusiva**, como em (2), significando que ambas as possibilidades também pode ocorrer.

> **Assim, numa disjunção, se P e Q são proposições, então $P \vee Q$ é uma afirmação verdadeira quando pelo menos uma das componentes for verdadeira, e falso quando ambas, P e Q, forem falsas.**

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Tabela 2.3 Tabela-verdade para a disjunção

Exemplo 2.1.5. *(1)* $7 > 3$ *ou* $1 + 1 = 5$.

(2) O Vasco será o campeão brasileiro deste ano ou o Flamengo será rebaixado para a segunda divisão.

2.1.3 Negação

Seja P uma proposição. A negação de P, denotada por $\sim P$ (ou $\neg P$, ou ainda $no(P)$), é verdadeira quando a proposição P é falsa, e é falsa quando P é verdade.

P	$\sim P$
V	F
F	V

Tabela 2.4 Tabela-verdade para a negação

Exemplo 2.1.6. *(1) Se P representa a afirmação "este é um curso fácil", $\sim P$ significa que "este curso é difícil". A quem atribuirmos o valor verdadeiro? A P ou a $\sim P$?*

(2) Se P significa "quatro é um número par", então $\sim P$ afirma que "quatro é ímpar".

Observação 2.1.7. *Verifique que $\sim(\sim P) = P$. Na linguagem comum, uma dupla negação é usada para enfatizar uma afirmação e não para tornar ela positiva. Por exemplo, ao dizer "não quero cola nenhuma na prova", a intenção do aluno é mostrar que ele não vai aceitar qualquer tipo de cola na prova.*

2.1.4 Implicações

Matemática é feita de afirmações da forma "P implica Q". Isto é, "se a afirmação P é verdadeira, então a afirmação Q também é verdadeira". Muitas vezes essa estrutura é omitida, principalmente para tornar a matemática mais compreensível. Seria difícil se escrevêssemos sempre desse modo.

Exemplo 2.1.8. *(1) Se x é um número par, então x^2 é um número par.*

(2) Se $x \neq 0$, então $x^2 > 0$.

(3) Todos os números primos maiores que 2 são ímpares.

Em uma implicação $P \Rightarrow Q$ existem duas partes: a afirmação P é dita **hipótese** (ou premissa) e a afirmação Q é chamada **conclusão** (ou tese). Nem sempre é fácil demarcar a hipótese e a conclusão; por exemplo, "Seja x um número inteiro positivo. Se x é ímpar, então x^2 é ímpar", quer dizer que "Se x é um inteiro positivo e x é ímpar, então x^2 é ímpar".

Direi a voces o seguinte: "Se vocês estudarem, então vocês passarão na disciplina Fundamentos de Matemática". Em que situação estarei mentindo? Somente no caso de vocês terem estudado e tiverem sido reprovados. Observe que vocês podem não estudar e mesmo assim conseguir aprovação! Assim, uma implicação $P \Rightarrow Q$ é falsa somente quando a hipótese P é verdadeira e a conclusão Q é falsa. Um modo de entender o valor verdade de uma afirmação condicional é pensar nela como uma obrigação ou um contrato.

Observação 2.1.9. *É claro que podemos partir de falsidades e chegar em verdades. Por exemplo, "se $1 = -1$, então $1 = 1$"(basta elevar ao quadrado a hipótese). Logo a veracidadde de uma implicação não nos permite concluir nada sobre os valores lógicos da hipótese e da conclusão.*

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabela 2.5 Tabela-verdade para a implicação

Na literatura, existem algumas formas equivalentes de escrever uma implicação $P \Rightarrow Q$:

(1) "Q se P- por exemplo, "Rubinho Barrichello seria campeão mundial de Fórmula 1 se não fosse Michael Schumacher."

(2) "Q é uma condição necessária para P"

(3) "P somente se Q- por exemplo, "xy é ímpar somente se x e y são ímpares".

(4) "P é suficiente para Q"

Definição 2.1.10. *Duas afirmações são* ***logicamente equivalentes*** *se possuem a mesma tabela-verdade, ou seja, se possuem os mesmos valores lógicos. Denotamos este fato pelo símbolo* $\equiv$.

Assim, verificamos que $\sim (P \vee Q) \equiv \sim P \wedge \sim Q$ e $\sim (P \wedge Q) \equiv \sim P \vee \sim Q$. Ou seja, dizer que "não é verdade que Vasco ou São Paulo será campeão brasileiro este ano"é equivalente a dizer que "nem Vasco, nem São Paulo será campeão brasilero este ano". Observe a semelhança das equivalências acima com as leis de De Morgan para conjuntos:

$$(A \cup B)^c = A^c \cap B^c \text{ e } (A \cap B)^c = A^c \cup B^c,$$

onde A^c significa o complementar do conjunto A.

Podemos formar novas afirmações condicionais a partir de uma implicação, a saber:

A Inversa de uma implicação $P \Rightarrow Q$ é $\sim P \Rightarrow \sim Q$.

O erro inicial mais comum que pessoas cometem em lógica se origina no uso da linguagem comum. Por exemplo, ao dizer que "se chover não irei à praia", em geral interpretamos isso como "se não chover, vou à praia". Mas o fato é que foi dito apenas o que acontece caso chova! Construindo as tabelas-verdade de $P \Rightarrow Q$ e $\sim P \Rightarrow \sim Q$ verificaremos que essas implicações não são equivalentes. Em geral, a veracidade de $P \Rightarrow Q$ nada diz sobre a veracidade de $\sim P \Rightarrow \sim Q$.

Exemplo 2.1.11. *(1) "Se eu sou sergipano, então eu sou brasileiro"é uma implicação válida, porém sua inversa é falsa: "Se eu não sou sergipano, então eu não sou brasileiro".*

(2) "Se x é par, então x^2 é par"é uma implicação verdadeira que possui um inversa também verdadeira: "Se x é ímpar, então x^2 é ímpar".

A Contrapositiva de uma implicação $P \Rightarrow Q$ é $\sim Q \Rightarrow \sim P$.

Surpreendentemente estas afirmações são logicamente equivalentes (verifique!). Assim por exemplo, a contrapositiva da afirmação "Se x é um número primo, então $x = 2$ ou x é ímpar"é "Se $x \neq 2$ e x é par, então o número x não é primo".

A Recíproca de uma implicação $P \Rightarrow Q$ é $Q \Rightarrow P$.

A veracidade de $P \Rightarrow Q$ nem sempre conduz à veracidade de $Q \Rightarrow P$ (construa as tabelas-verdade e verifique que essas proposições não são logicamente equivalentes). Por exemplo, "Se uma função é derivável num ponto, então ela é contínua nesse ponto"é uma implicação verdadeira, porém sua recíproca é falsa. Por exemplo, a função modular $f(x) = |x|$ na origem.

2.1.5 Se, e somente se

Relacionado à sentença condicional (implicação) está a sentença bicondicional $P \Leftrightarrow Q$. A dupla seta significa que tanto a implicação $P \Rightarrow Q$ como sua recíproca $Q \Rightarrow P$ são verdadeiras. Assim, $P \Leftrightarrow Q$ é verdade quando P e Q possuem extamente os mesmos valores. Em outras palavras, temos a equivalência lógica

$$[P \Leftrightarrow Q] \equiv [(P \Rightarrow Q) \wedge (Q \Rightarrow P)],$$

de forma que para verificarmos a validade de uma bicondicional é equivalente a verificar a validade de duas condicionais.

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Tabela 2.6 Tabela-verdade para a bicondicional

Exemplo 2.1.12. *As afirmações "um retangulo é um quadrado se, e somente se, suas diagonais são perpendiculares"e "*$1+7=6 \Rightarrow \sqrt{2}+\sqrt{3}=\sqrt{5}$*"são verdadeiras.*

Existem algumas variações em como escrever a afirmação $P \Leftrightarrow Q$. É comum escrever P é necessário e suficiente para Q.

2.2 Tautologias e Contradições

Agora que definimos modos básicos de combinar afirmações, podemos formar proposições mais complicadas por usar combinações das operações básicas. Por exemplo, $P \vee (Q \Rightarrow \sim R)$ das afirmaçòes P, Q e R. Necessitamos usar parênteses, colchetes e chaves para evitar ambiguidades.

A tabela-verdade para a proposição $P \Rightarrow (P \vee Q)$ é dada abaixo. Note que independente-

P	Q	$P \vee Q$	$P \Rightarrow (P \vee Q)$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

Tabela 2.7 Tabela-verdade representando uma tautologia

mente dos valores de P e Q, a proposição $P \Rightarrow (P \vee Q)$ é sempre verdadeira. Uma proposição com esta propriedade é chamada uma **tautologia**. Existem também proposições cuja estrutura é tal que elas são sempre falsas, seja qual for os valores de suas componentes. Tais proposições são chamadas **contradições**. Um exemplo é a expressão $(\sim P \wedge Q) \wedge (P \vee \sim Q)$, como mostra a tabela abaixo.

P	Q	$\sim P$	$\sim Q$	$\sim P \wedge Q$	$P \vee \sim Q$	$(\sim P \wedge Q) \wedge (P \vee \sim Q)$
V	V	F	F	F	V	F
V	F	F	V	F	V	F
F	V	V	F	V	F	F
F	F	V	V	F	V	F

Tabela 2.8 Tabela-verdade para uma contradição

Observação 2.2.1. *Existe uma diferença sutil, mas importante entre o conectivo bicondicional e o conceito de equivalência lógica. Quando escrevemos $P \Leftrightarrow Q$ expressamos uma simples fórmula. Equivalência lógica, por outro lado, é uma relação entre duas expressões lógicas (fórmulas). Os dois conceitos estão relacionados da seguinte forma: duas expressões lógicas α e β são logicamente equivalentes se, e somente se, $\alpha \Leftrightarrow \beta$ é uma tautologia.*

Exemplo 2.2.2. *Verifique que $[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$ é uma tautologia.*

É possível ter tautologias e contradições mais complicadas (e não intuitivos). Por exemplo, a tabela-verdade da afirmação

$$[(P \wedge Q) \Rightarrow R] \Rightarrow [P \Rightarrow (Q \Rightarrow R)]$$

expressa uma tautologia. Como mais um exemplo de contradição, verifique com uma tabela-verdade que a afirmação $[Q \Rightarrow (P \wedge \sim Q)] \wedge Q$ é sempre falsa.

2.3 Quantificadores

A menos que algum valor de x tenha sido associado, a sentença "$x > 3$"não é uma proposição porque ela não é verdadeira nem falsa. Quando a variável x é trocada por certos valores, por exemplo 7, a proposição resultante é verdadeira, enquanto para outros valores de x, digamos 2, ela é falsa. Este é um exemplo de uma **sentença aberta** ou **predicado**. Isto é, uma sentença

contendo uma ou mais variáveis que torna-se uma proposição somente quando as variáveis são trocadas por objetos particulares. Por notação, se uma sentença aberta é chamada P e as variáveis são $x_1, x_2, \cdots, x_k$, escrevemos $P(x_1, x_2, \cdots, x_k)$. A sentença "$x_1 = x_2 + x_3$"é aberta com três variáveis $P(x, x_2, x_3)$. Assim, $P(2,1,1)$ é verdadeira, enquanto $P(1,2,3)$ é falsa. O conjunto no qual as variáveis pertencem é dito o **universo de discurso**.

Outro modo para construir proposições a partir de uma sentença aberta é modificar ela com um quantificador.

Definição 2.3.1. *Para uma sentença aberta $P(x)$ com variável x, a sentença $\forall x \in U, P(x)$ (lida para todo x em U, $P(x)$) é verdadeira precisamente quando $P(x)$ é verdadeiro qualquer que seja x no universo de discurso U. O símbolo $\forall$ é chamado o* ***quantificador universal****. A sentença $\exists x \in U, P(x)$ (lida existe x em U tal que $P(x)$) é verdadeira quando existe pelo menos um x no universo de discurso tal que $P(x)$ é verdadeiro. O símbolo $\exists$ é chamado o* ***quantificador existencial****.*

Frequentemente, também lemos: para todos os valores de x em U, a afirmação $P(x)$ é verdadeira, ou ainda, todos os valores de x em U satisfazem $P(x)$.

Definição 2.3.2. *A sentença $\exists x \in U, P(x)$ (lida existe x em U tal que $P(x)$) é verdadeira quando existe pelo menos um x no universo de discurso U tal que $P(x)$ é verdadeiro. O símbolo $\exists$ é chamado o* ***quantificador existencial****.*

Exemplo 2.3.3. *(1)* $\forall x \in \mathbb{R}, x^2 \geq 0$;

(2) $\forall x, y \in \mathbb{Q}$,*(o produto xy e a soma $x+y$ são racionais);*

(3) $\forall x \in \mathbb{R}, (x \geq 3 \Rightarrow x^2 \geq 9)$;

(4) $\exists x \in \mathbb{Z}, x^2 = 4$;

(5) Existem dois números primos tal que sua soma é um número primo;

(6) Para cada número primo x menor que 10, $x^2 + 4$ é primo.

Podemos formar afirmações com mais de um quantificador, bem como com quantificadores envolvendo variáveis diferentes. Suponha que $P(x,y) =$ "$x + y^2 = 3$", onde x e y são números reais. A afirmação $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}; P(x,y)$ pode ser lida como: para todo número real y existe algum número real x tal que $x + y^2 = 3$. Esta afirmação é verdadeira porque para qualquer real y, podemos resolver x em termos de y, fornecendo $x = 3 - y^2$. Notemos que se mudarmos a ordem dos quantificadores a afirmação passa a ser falsa, pois $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}; P(x,y)$ diz que existe ao menos um número real x tal que qualquer que seja $y \in \mathbb{R}$, temos $x + y^2 = 3$ e isso acontece somente para no máximo dois valores de y, dados por $y = \pm\sqrt{3-x}$. Um exemplo usual da combinação de quantificadores é dado pela definição de continuidade de uma função f num ponto $x = a$, a saber: $\forall \varepsilon > 0, \exists \delta > 0$ tal que $|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon$.

O número de quantificadores em uma afirmação matemática fornece uma medida da complexidade desta afirmação. Isto é a principal razão porque é difícil entender as definições rigorosas de limite, convergência, continuidade e diferenciabilidade em cálculo.

Consideremos agora a seguinte afirmação: "Todos serão reprovados em Fundamentos de Matemática."Qual seria uma negação para esta afirmação? Temos uma afirmação do tipo $\forall x \in U, P(x)$. A negação disso é que $P(x)$ é falso para pelo menos um x no universo de discurso U, ou seja, $\exists x \in U, \sim P(x)$. Logo,

$$\sim (\forall x \in U, P(x)) \equiv \exists x \in U, \sim P(x).$$

Analogamente, verificamos que

$$\sim (\exists x \in U, P(x)) \equiv \forall x \in U, \sim P(x).$$

Diferente do que foi discutido antes, não podemos usar tabela verdade para verificar a veracidade dessas equivalências.

Exemplo 2.3.4. *(1) Existe um vascaíno que não é feliz. Claro que não! Todos os vascaínos são felizes.*

(2) $\sim [\forall x, (P(x) \Rightarrow Q(x))] \equiv \exists x, \sim (P(x) \Rightarrow Q(x)) \equiv \exists x, \sim (\sim P(x) \vee Q(x)) \equiv \exists x, (P(x) \wedge \sim Q(x))$. *Assim, se* $P(x)$ *significa "x é uma loira"e* $Q(x)$ *significa "x é burra", então* $\forall x, P(x) \Rightarrow Q(x)$ *significa que "toda loira é burra"e a negação seria "existe pelo menos uma loira que não é burra".*

(3) Fazemos a negação de uma combinação de quantificadores, negando um de cada vez. Por exemplo, tomando a função $f : \mathbb{R} \to \mathbb{R}$ *dada por* $f(x) = x^2$ *e a afirmação que para todo* $y \in \mathbb{R}$ *existe* $x \in \mathbb{R}$ *tal* $f(x) = y$*, em símbolos,* $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}; P(x,y) = "f(x) = y"$ *(isto define a sobrejetividade da função* f*), sua negação, conforme uso da equivalência lógica acima, será* $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}; \sim P(x,y)$*. Ou seja, existe pelo menos um* y *real tal que qualquer que seja o* $x \in \mathbb{R}$ *nunca teremos* $f(x) = y$*.*

2.4 Validade de Argumentos

Uma prova é uma justificação de uma afirmação chamada um **teorema**. A importância da lógica é que ela fornece um meio de estabelecer quando uma linha de raciocínio, chamada um **argumento**, é correta ou não. Um argumento nesse sentido, consiste de um conjunto de proposições (simples ou compostas) chamadas **hipóteses** (ou premissas) e outra proposição dita **conclusão** (ou tese), a qual é uma consequência inevitável das hipóteses. Cada passo do argumento segue as leis da lógica. Em matemática, uma afirmação não é aceita como válida sem que seja acompanhada de uma prova. Esta insistência por provas é uma das coisas que torna a matemática distinta de outras ciências.

Escrever provas é uma tarefa difícil; não existem procedimentos que assegurem sucesso sempre. Por isto, iniciaremos discutindo provas lógicas. Elas serão escritas no formato coluna, com cada passo sendo justificado por uma regra de inferência.

Definição 2.4.1. *Um argumento com hipóteses* $P_1, P_2, \cdots, P_n$ *e conclusão* Q *é dito ser válido, se sempre que* $P_1, P_2, \cdots, P_n$ *forem verdadeiros, então* Q *também o for. Ou seja,*

$$P_1 \wedge P_2 \wedge \cdots \wedge P_n \Rightarrow Q$$

é uma tautologia. Caso contrário, dizemos que o argumento é inválido.

É importante ressaltar que não é o conteúdo de um argumento que determina quando ou não ele é válido. O que é importante é sua estrutura.

2.4.1 Tabela-Verdade

A verificação da veracidade ou falsidade de um argumento via tabela-verdade é estabelecida por considerar todos os modos possíveis nas quais as proposições componentes podem ser verdadeiras ou falsas.

Exemplo 2.4.2. *Se Dilma não ganhar a eleição, então Serra será eleito. Marina desistiu da candidatura. Serra não foi eleito ou Marina continuou candidata. Portanto, Dilma ganhou a eleição.*

Simbolicamente, temos $[(\sim B \Rightarrow M) \wedge (\sim L) \wedge (\sim M \vee L)] \Rightarrow B$. Para decidirmos se o argumento é válido, devemos examinar os possíveis valores verdade de B para os casos em que as hipóteses são verdadeiras. Assim, numa tabela-verdade temos que o nosso argumento é válido pois

B	M	L	$\sim Q \Rightarrow M$	$\sim L$	$\sim M \vee L$
V	V	V	V	F	V
V	V	F	V	V	F
V	F	V	V	F	V
V	F	F	V	V	V
F	V	V	V	F	V
F	V	F	V	V	F
F	F	V	F	F	V
F	F	F	F	V	V

Tabela 2.9 Validade de argumento

Exemplo 2.4.3. *Se eu ganhar na megasena darei um carro a cada um de vocês. Eu não ganhei. Logo, voces perderam os carros prometidos. Em símbolos temos as seguintes afirmações:* P_1*: Paulo ganhou na megasena;* P_2*: Vocês ganharão um carro; e a seguinte conclusão:* $Q = \sim P_2$*. Portanto, nosso argumento é* $[(P_1 \Rightarrow P_2) \wedge \sim P_1] \Rightarrow \sim P_2$*, cuja tabela-verdade é dada por*

P_1	P_2	$P_1 \Rightarrow P_2$	$\sim P_1$	$\sim P_2$
V	V	V	F	F
V	F	F	F	V
F	V	V	V	F
F	F	V	V	V

Tabela 2.10 Tabela-verdade para o Exemplo

Assim, a veracidade das hipóteses no argumento não implicam logicamente a conclusão e o argumento é inválido.

Observação 2.4.4. *Considere o seguinte argumento: "Se $a \mid b$, então $mdc\{a,b\} = a$. Ou $a \mid b$ ou $mmc\{a,b\} = ab$. Se $mmc\{a,b\} \neq ab$ e $mdc\{a,b\} \neq a$, então $a \nmid b$."O argumento tem premissas $P \Rightarrow Q$, $P \vee R$ e $\sim R \wedge \sim Q$, tais que a tabela verdade da conjunção $(P \Rightarrow Q) \wedge (P \vee R) \wedge (\sim R \wedge \sim Q)$ fornece uma contradição. Em outras palavras, é impossível para as premissas serem verdadeiras simultaneamente. Um conjunto de premissas com essa propriedade é dito* ***inconsistente****. Neste caso o argumento é válido, embora não tenha utilidade, pois suporta qualquer conclusão.*

2.4.2 Regras de Inferência

O método de tabela-verdade para assegurar a validade de um argumento pode tornar-se inviável se as hipóteses são complicadas ou são numerosas. Existe um método alternativo que não necessita construir uma tabela-verdade. O método consiste em derivar uma sequência de proposições a partir das hipóteses até atingir a conclusão:

$$P_1 \wedge P_2 \wedge \cdots \wedge P_n \Rightarrow P_{n+1} \Rightarrow P_{n+2} \Rightarrow \cdots \Rightarrow Q.$$

Considere a seguinte coleção de afirmações: "Se o governo manter a inflação baixa ou diminuir a taxa de desemprego, então não haverá crise financeira. Se as bolsas de valores cairem, então teremos uma crise financeira. O governo conteve a taxa de inflação. Assim as bolsas não caíram". Esta coleção de afirmações é um exemplo de um argumento lógico, a última sendo a conclusão e as demais as premissas do argumento. Um argumento é válido se a conclusão necessariamente segue das premissas.

Como podemos mostrar que o argumento fornecido acima é válido? Iniciamos por converter o argumento para símbolos. Seja $I =$ o governo manteve a inflação baixa, $D =$ o governo diminuiu a taxa de desemprego, $F =$ haverá crise financeira, e $B =$ as bolsas de valores caíram. O argumento então torna-se onde a linha horizontal separa as premissas da conclusão.

$$\begin{array}{c} (I \vee D) \Rightarrow \sim F \\ B \Rightarrow F \\ D \\ \hline \sim B \end{array}$$

Alternativamente, poderíamos escrever

$$\{[(I \vee D) \Rightarrow \sim F] \wedge (B \Rightarrow F) \wedge D\} \Rightarrow \sim B.$$

Se quisessemos usar tabela-verdade aqui, esta teria 16 linhas, o que seria um trabalho tedioso. Além disso, a tabela-verdade não nos dá intuição do porque a veracidade do argumento e, mais ainda, quando provamos afirmações matemáticas, frequentemente usamos quantificadores, o que torna o uso de tabela-verdade inviável. Assim, um modo mais frutífero de mostrar uma implicação lógica mais complicada, é quebrá-la em uma coleção de implicações mais simples, tomando uma de cada vez.

Na construção de provas formais será de grande ajuda termos um estoque de argumentos válidos, ditos **regras de inferência**:

NOME	PREMISSAS	CONCLUSÃO
Simplificação	$P \wedge Q$	P
Adição	P	$P \vee Q$
Conjunção	P,Q	$P \wedge Q$
Silogismo Disjuntivo	$P \vee Q, \sim P$	Q
Modus Ponens	$P \Rightarrow Q, P$	Q
Modus Tollens	$P \Rightarrow Q, \sim Q$	$\sim P$
Silogismo Hipotético	$P \Rightarrow Q, Q \Rightarrow R$	$P \Rightarrow R$
Absorção	$P \Rightarrow Q$	$P \Rightarrow (P \wedge Q)$
Dilema Construtivo	$(P \Rightarrow Q) \wedge (R \Rightarrow S), P \vee R$	$Q \vee S$

Tabela 2.11 Regras de Inferência

Usando as regras de inferência listadas acima, podemos construir uma justificação para o argumento: Para um dado argumento existe mais que uma forma possível de combinar as regras

(1)	$(I \vee D) \Rightarrow \sim F$	Premissa
(2)	$B \Rightarrow F$	Premissa
(3)	D	Premissa
(4)	$I \vee D$	(3) Adição
(5)	$\sim F$	(1,4) Modus Ponens
(6)	$\sim B$	(2,5) Modus Tollens

de inferencia para mostrar a validade do argumento. No exemplo acima também poderíamos ter: Este fato nos leva ao problema de que para provar a invalidade precisamos mostrar que

(1)	$(I \vee D) \Rightarrow \sim F$	Premissa
(2)	$B \Rightarrow F$	Premissa
(3)	D	Premissa
(4)	$I \vee D$	(3) Adição
(5)	$\sim F \Rightarrow \sim B$	(2) Contrapositiva
(6)	$(I \vee D) \Rightarrow \sim B$	(1,5) Silogismo Hipotético
(7)	$\sim B$	(4,6) Modus Ponens

nenhuma combinação de regras de inferência é possível.

Exemplo 2.4.5. *Voltando ao nosso primeiro exemplo, temos:*

Exemplo 2.4.6. *Se Pai André estiver certo, o Vasco será...*

(1)	$\sim B \Rightarrow M$	Premissa
(2)	$\sim L$	Premissa
(3)	$\sim M \vee L$	Premissa
(4)	$\sim M$	(2,3) Silogismo Disjuntivo
(5)	$\sim (\sim B)$	(1,4) Modus Tollens
(6)	B	(5) Dupla Negação

Tabela 2.12 Regras de Inferência

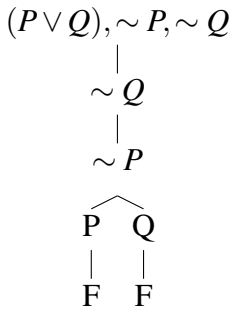
(1)	$(M \Rightarrow B) \wedge (P \Rightarrow A)$	Premissa
(2)	P	Premissa
(3)	$P \Rightarrow A$	(1) Simplificação
(4)	A	(2,3) Modus Ponens
(5)	$A \vee B$	(4) Adição

Tabela 2.13 Regras de Inferência

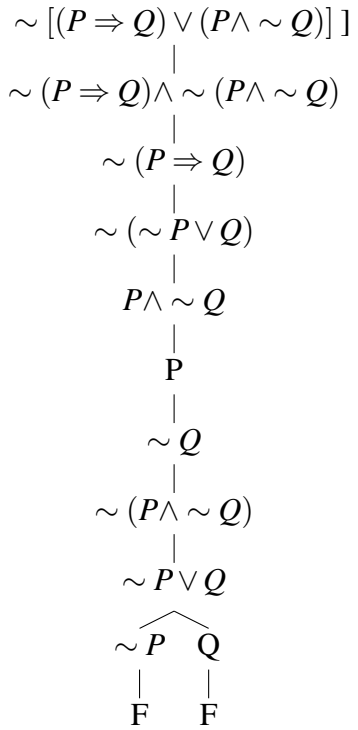
2.4.3 Árvore de Refutação

Nesse método analisamos argumentos do tipo $P_1 \wedge P_2 \wedge \cdots \wedge P_n \Rightarrow Q$ assumindo a negação da conclusão $\sim Q$ como uma hipótese adicional. Imaginamos uma árvore ao contrário. A raiz será constituída pelas hipóteses (incluindo a hipótese adicional). Então construímos seus galhos utilizando regras de inferência. Uma conjunção gera somente um galho (ramo), enquanto uma disjunção gera dois ramos. A árvore termina quando utilizamos todas as hipóteses e proposições compostas, de forma que restam apenas proposições simples. Se encontrarmos em todos os ramos uma contradição (marcamos por F cada ramo nesta condição), então a tentativa de refutação falhou e o argumento é válido. Caso contrário, se em algum ramo não foi possível encontrar contradição, então o argumento é inválido (refutamos).

Exemplo 2.4.7. *Verificar por meio de árvore de refutação a validade do argumento* $[(P \vee Q) \wedge \sim P] \Rightarrow Q$.

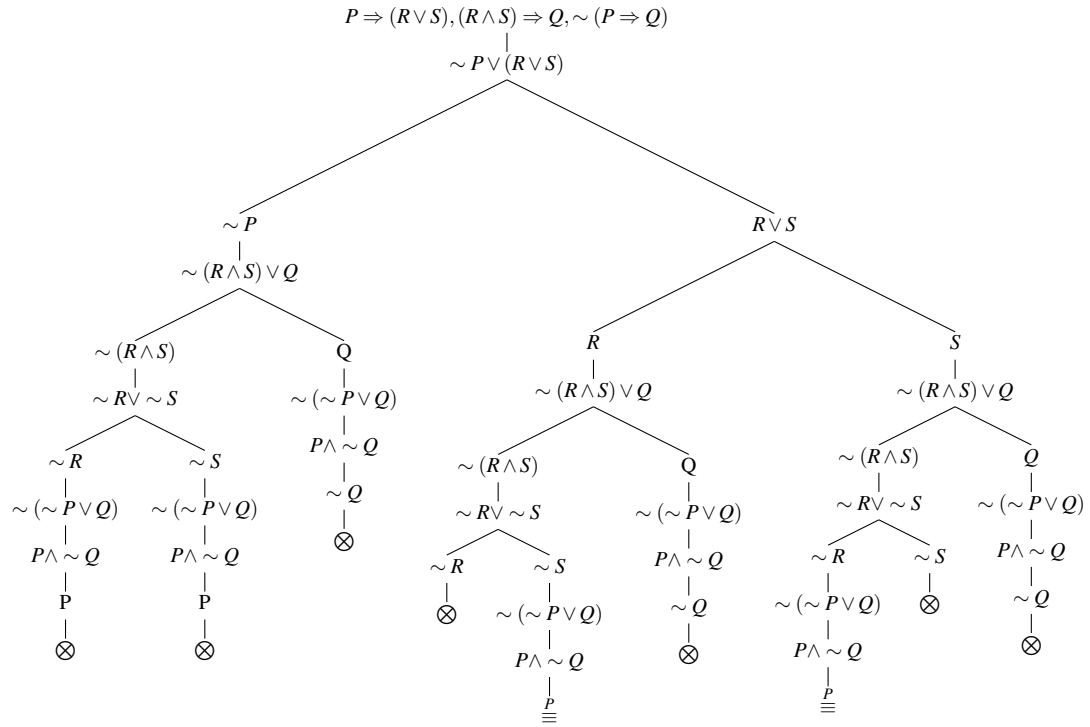


Exemplo 2.4.8. *Construir uma árvore de refutação para verificar se a fórmula* $(P \Rightarrow Q) \vee (P \wedge \sim Q)$ *é uma tautologia.*



Desde que em todos os galhos obtemos contradições, segue que não conseguimos refutar o argumento. Logo, o argumento é válido.

Exemplo 2.4.9. *Faça o mesmo para* $\{[P \Rightarrow (R \vee S)] \wedge [(R \wedge] S) \Rightarrow Q]\} \Rightarrow (P \Rightarrow Q)$.



Como restaram galhos onde não conseguimos uma contradição, concluímos que o argumento é inválido.

Observação 2.4.10. *A ordem de tomar as premissas não importa. A aparencia diferente da árvore não interfere na conclusão sobre a validade ou não do argumento.*

2.4.4 Argumentos envolvendo quantificadores

Listaremos duas regras que nos capacitarão obter proposições sem quantificadores, cuja verdade seguirá da verdade das funções proposicionais quantificadas.

Regra 1: Dada qualquer função proposicional $P(x)$, da verdade de $\forall x, P(x)$, podemos ser inferida a verdade de $P(a)$ para qualquer a no universo de discurso.

Regra 2: Dada qualquer função proposicional $P(x)$, da verdade de $\exists x, P(x)$, podemos inferir que existe pelo menos um elemento a no universo de discurso para o qual $P(a)$ é verdadeiro.

Procure utilizar primeiro as proposições que envolvem quantificadores existenciais.

Exemplo 2.4.11. *Prove a validade do seguinte argumento: "Todos os atletas são fisicamente fortes. Paulo é uma atleta. Então Paulo é fisicamente forte."Sejam $A(x) : x$ é um atleta; $F(x) : x$ é fisicamente forte. Assim,*

(1)	$\forall x, A(x) \Rightarrow F(x)$	Premissa
(2)	$A(p)$	Premissa
(3)	$A(p) \Rightarrow F(p)$	Regra 1
(4)	$F(p)$	$(2,3)$ Modus Ponens

Tabela 2.14 Regras de Inferência

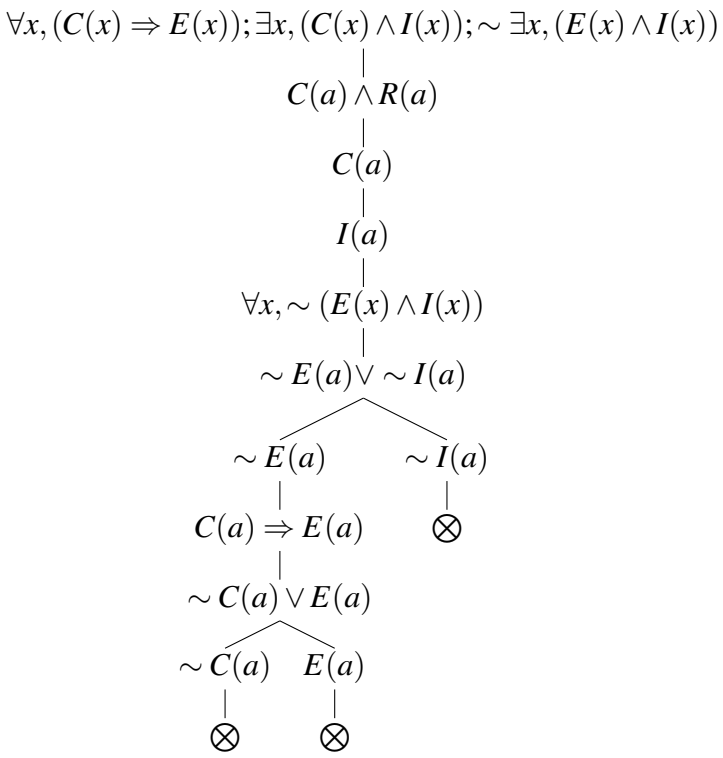
Exemplo 2.4.12. *"Tudo é caro ou ruim para voce. Nem tudo é ruim para você. Assim, existem algumas coisas que são caras e não são ruins para voce."Fazendo $C(x) : x$ é caro e $R(x) : x$ é ruim, obtemos:*

(1)	$\forall x, [C(x) \vee R(x)]$	Premissa
(2)	$\sim \forall x, R(x)$	Premissa
(3)	$\exists x, \sim R(x)$	(2) Negação
(4)	$\sim R(a)$	Regra 2
(5)	$C(a) \vee R(a)$	Regra 1
(6)	$C(a)$	$(5,4)$ Silogismo Disjuntivo
(7)	$C(a) \wedge \sim R(a)$	$(4,6)$ Conjunção
(8)	$\exists x, [C(x) \wedge \sim R(x)]$	Regra 2

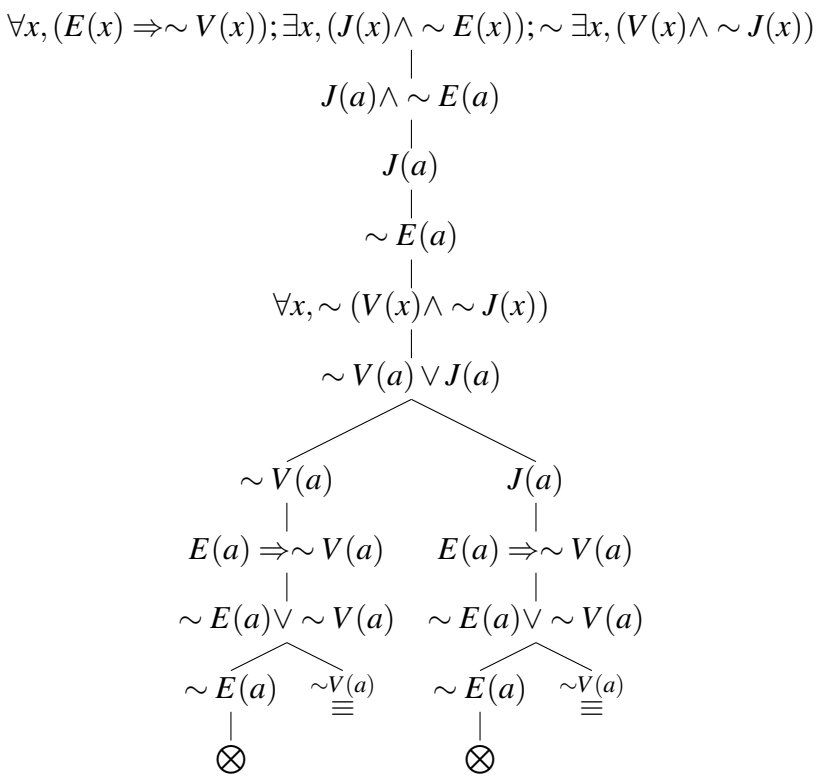
Tabela 2.15 Regras de Inferência

Árvores de refutação também podem ser usadas em argumento envolvendo quantificadores.

Exemplo 2.4.13. *Verifique a validade do argumento: "Todos os cientistas são estudiosos. Alguns cientistas são inventores. Alguns estudiosos são inventores."Faça $C(x)$: x é cientista; $E(x)$: x é estudioso; e $I(x)$: x é inventor. Tomando a negação da conclusão como hipótese adicional, obtemos que o argumento é válido, conforme a árvore de refutação abaixo:*



Exemplo 2.4.14. *"Nenhum estudante é velho. Alguns jovens não são estudantes. Logo, alguns velhos não são jovens."Faça $E(x)$: x é estudante; $V(x)$: x é velho; e $J(x)$: x é jovem. Então*



Desde que sobraram ramos em que não encontramos contradições, concluímos que o argumento não é válido.

Primeira Lista de Exercícios

1. Quais das seguintes sentenças são afirmações? Para as respostas afirmativas indique seu valor lógico.

   (a) O inteiro 123 é primo;

   (b) É $5\times 2=10$?

   (c) $x^2-4=0$;

   (d) Multiplique $5x+2$ por 3;

   (e) $5x+3$ é um inteiro ímpar.

2. Para a sentença aberta $P(A):A\subseteq\{1,2,3\}$ sob o domínio $S=\mathscr{P}(\{1,2,4\})$, determine:

   (a) todo $A\in S$ para o qual $P(A)$ é verdadeiro;

   (b) todo $A\in S$ para o qual $P(A)$ é falso;

   (c) todo $A\in S$ para o qual $A\cap\{1,2,3\}=\emptyset$.

3. Estabeleça a negação de cada uma das seguintes afirmações:

   (a) $\sqrt{2}$ é um número racional;

(b) Zero não é um inteiro negativo;

(c) 111 é um número primo.

4. Seja $S = \{1,2,\cdots,6\}$ e seja $P(A) : A \cap \{2,4,6\} = \emptyset$ e $Q(A) : A \neq \emptyset$ sentenças abertas sobre o domínio $\mathscr{P}(S)$.

   (a) Determine todos os $A \in \mathscr{P}(S)$ para os quais $P(A) \wedge Q(A)$ é verdadeiro;

   (b) Determine todos os $A \in \mathscr{P}(S)$ para os quais $P(A) \vee (\sim Q(A))$ é verdadeiro;

   (c) Determine todos os $A \in \mathscr{P}(S)$ para os quais $(\sim P(A)) \wedge (\sim Q(A))$ é verdadeiro;

5. Considere as afirmações $P : \sqrt{2}$ é racional e $Q : \frac{22}{7}$ é racional. Escreva cada uma das seguintes afirmações em palavras e indique seu valor lógico:

   (a) $P \Rightarrow Q$;

   (b) $Q \Rightarrow P$;

   (c) $(\sim P) \Rightarrow (\sim Q)$;

   (d) $(\sim Q) \Rightarrow (\sim P)$.

6. Em cada uma das seguintes sentenças abertas $P(x,y)$ e $Q(x,y)$ dadas, onde o domínio de ambas as variáveis é $\mathbb{Z}$, determine o valor lógico de $P(x,y) \Rightarrow Q(x,y)$ para os valores x e y dados:

   (a) $P(x,y) : x^2 - y^2 = 0$ e $Q(x,y) : x = y$ com $(x,y) \in \{(1,-1),(3,4),(5,5)\}$;

   (b) $P(x,y) : x^2 + y^2 = 1$ e $Q(x,y) : x + y = 1$ com $(x,y) \in \{(1,-1),(-3,4),(0,-1),(1,0)\}$.

7. Seja $S = \{1,2,3\}$. Considere as seguintes sentenças abertas sobre o domínio S:

$$P(n) : \frac{n(n-1)}{2} \text{ é par,}$$
$$Q(n) : 2^{n-2} + 3^{n-2} + 6^{n-2} > (\frac{5}{2})^{n-1}.$$

   Determine três elementos distintos a,b,c em S tais que $P(a) \Rightarrow Q(a)$ é falso, $Q(b) \Rightarrow P(b)$ é falso e $P(c) \Leftrightarrow Q(c)$ é verdadeiro.

8. Para afirmações P e Q mostre que $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ é uma tautologia.

9. Para as afirmações P, Q e R mostre que $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ é uma tautologia.

10. Para as afirmações P, Q e R use uma tabela verdade para mostrar que as afirmações $P \Rightarrow (Q \vee R)$ e $(\sim Q) \Rightarrow ((\sim P) \vee R)$ são logicamente equivalentes. Idem para as afirmações $P \vee (Q \wedge R)$ e $(P \vee Q) \wedge (P \vee R)$.

11. Considere a implicação: se x e y são pares, então xy é par.

(a) Estabeleça a implicação usando "somente se";

(b) Estabeleça a recíproca, a inversa e a contrapositiva da implicação;

(c) Estabeleça a implicação como uma disjunção;

(d) Estabeleça a negação da implicação como uma conjunção.

12. Seja S o conjuntos de inteiros ímpares e seja $P(x) : x^2 + 1$ é par e $Q(x) : x^2$ é par sentenças abertas sobre o domínio S. Estabeleça em palavras $\forall x \in S, P(x)$ e $\exists x \in S, Q(x)$.

13. Estabeleça a negação das seguintes sentenças quantificadas:

(a) Para cada número racional r, o número $1/r$ é racional;

(b) Existe um número racional r tal que $r^2 = 2$.

14. Determine o valor lógico de cada uma das seguintes afirmações:

(a) $\exists x \in \mathbb{R}, x^2 - x = 0$;

(b) $\forall n \in \mathbb{N}, n + 1 \geq 2$;

(c) $\forall x \in \mathbb{R}, \sqrt{x^2} = x$;

(d) $\exists x \in \mathbb{Q}, 3x^2 - 27 = 0$.

15. A afirmação "Para cada inteiro m tal que $m \leq 1$ ou $m^2 \geq 4$"pode ser expressa usando um quantificador como "$\forall m \in \mathbb{Z}, m \leq 1$ ou $m^2 \geq 4$". Faça o mesmo para as afirmações (a) e (b) abaixo.

(a) Existem inteiros a e b tais que $ab < 0$ e $a + b > 0$;

(b) Para todos os números reais x e y, $x \neq y$ implica que $x^2 + y^2 > 0$;

(c) Expresse em palavras a negação das afirmações (a) e (b);

(d) Usando quantificadores, expresse em símbolos a negação das afirmações (a) e (b).

16. Explique por que os significados das sentenças a seguir são distintos. Determine quais sentenças são verdadeiras e quais são falsas. Em seguinda, discuta o que ocorre ao se mudar a posição dos quantificadores em cada uma delas.

(a) $\forall y \in \mathbb{Z}, \exists x \in \mathbb{N}$ tal que $y^2 = x$;

(b) $\exists x \in \mathbb{N}$, tal que $\forall y \in \mathbb{Z}$ temos $y^2 = x$;

(c) $\exists x \in \mathbb{N}$ e $\exists y \in \mathbb{Z}$, tais que $y^2 = x$;

(d) $\forall x \in \mathbb{N}$ e $\forall y \in \mathbb{Z}$ temos $y^2 = x$.

17. Determine a validade ou não dos seguintes argumentos usando regras de inferência:

(a) $E \Rightarrow F, \sim G \Rightarrow \sim F, H \Rightarrow I, E \vee H \vdash G \vee I$;

(b) $P \Rightarrow Q, \sim R \Rightarrow (S \Rightarrow T), R \vee (P \vee T), \sim R \vdash Q \vee S$;

(c) $\sim A \Rightarrow (B \Rightarrow \sim C), C \Rightarrow \sim A, (\sim D \vee A) \Rightarrow \sim\sim C, \sim D \vdash \sim B$.

18. Suponha que os valores possiveis de x e y estão dentro do conjunto universo U constituídos de todos os carros. Sejam $L(x,y) = x$ é tão rápido quanto y, $M(x,y) = x$ é tão caro quanto y e $N(x,y) = x$ tão velho quanto y. Traduza as seguintes afirmações em palavras:

    (a) $\exists x \in U, \forall y \in U; L(x,y)$;

    (b) $\forall x \in U, \exists y \in U; M(x,y)$;

    (c) $\exists y \in U, \forall x \in U; [L(x,y) \vee M(x,y)]$.

19. Escreva a negação de cada uma das sentenças abaixo.

    (a) Todos os garotos são bons;

    (b) Existem homens que pesam 200kg ou mais;

    (c) A inequação $x^2 - 2x > 0$ vale para todos os números reais x;

    (d) Toda casa tem uma porta que é branca;

    (e) Pelo menos uma pessoa em Aracaju adora Matemática.

20. Alguém afirmou que o argumento

$$\exists x \in U; [P(x) \wedge Q(x)], \exists x \in U; M(x) \vdash \exists x \in U; [M(x) \wedge Q(x)]$$

    é válido, usando a seguinte justificativa: Encontre as falhas nessa justificativa.

(1)	$\exists x \in U; [P(x) \wedge Q(x)]$	Premissa
(2)	$\exists x \in U; M(x)$	Premissa
(3)	$P(a) \wedge Q(a)$	(1) Regra 2
(4)	$Q(a)$	(3) Simplificação
(5)	$M(a)$	(2) Regra 2
(6)	$M(a) \wedge Q(a)$	(5,4) Conjunção
(7)	$\exists x \in U; [M(x) \wedge Q(x)]$	(6) Regra 2

21. Tres professores, Antônio, Júlio e Marco, ensinam apenas uma disciplina dentre as de Lógica, Cálculo e Análise. Certa ocasião, foram abordados por uma aluna caloura querendo saber qual deles era seu professor de Lógica. Para a aluna já começar treinando o raciocínio lógico, combinaram que cada um diria uma frase. Apenas uma das frases era verdadeira, e com isso a aluna deveria deduzir quem era o professor que procurava. Júlio disse "Marco é o professor de Cálculo"; Antônio respondeu "Júlio não é o professor de Cálculo"; e Marco disse "Antônio não é o professor de Análise". Quem é o professor de lógica?

22. Brincando, quatro rapazes esconderam a bolsa do amigo Jugurta. Ao entrar na sala de aula, irritado, Jugurta os pergunta: "Qual dos espertinhos escondeu minha bolsa?Eu não fui!", respondeu Tomás. "Foi o Tche!", garantiu Marcelo. "Foi o Lord!", disse o Tchê. "O Marcelo está mentindo!", retrucou o Lord. Apenas um dos amigos mentiu, e somente um deles escondeu a bolsa. Qual?

23. Reescreva cada teorema abaixo na sua forma condicional "Se..., então".

    (a) Uma condição necessária para um número ser divisível por 6 é que ele seja simultaneamente divisível por 2 e por 3.

    (b) Ser um triângulo retangulo é condição suficiente para ter a altura correspondente ao vértice do ângulo reto igual a média geométrica das projeções dos catetos sobre a hipotenusa.

    (c) Uma condição suficiente para que um triangulo seja isósceles é que ele tenha dois ângulos internos congruentes.

    (d) Não ser primo é uma condição necessária para que o número seja da forma n^4+4, para $n \geq 2$.

24. Suponha que José gosta de feijão, não gosta de arroz, não gosta de macarrão e adora farinha. Quais das seguintes setenças são verdadeiras e quais são falsas?

    (a) Se José gosta de feijão, então gosta de macarrão;

    (b) José gosta de macarrão se, e somente se, ele gosta de arroz;

    (c) José gosta de arroz e farinha se ele gosta de feijão;

    (d) Se José gosta de macarrão então ele gosta de farinha, ou José gosta de macarrão se, e somente se, ele gosta de arroz;

    (e) Para José gostar de feijão e macarrão é necessário e suficiente que ele goste de arroz ou farinha.

25. Quais das seguintes setenças são tautologias, quais são contradições e quais são contingências?

    (a) $P \vee (\sim P \wedge Q)$;

    (b) $(X \vee Y) \Leftrightarrow (\sim X \Rightarrow Y)$;

    (c) $(A \wedge \sim B) \wedge (\sim A \vee B)$;

    (d) $[Z \vee (\sim Z \vee W)] \wedge \sim (W \wedge U)$;

    (e) $[L \Rightarrow (M \Rightarrow N)] \Rightarrow [M \Rightarrow (L \Rightarrow N)]$.

26. Para cada um dos seguintes argumentos estabeleça uma justificativa para sua validade ou falsidade.

    (a) Se Carira é pequeno, então é difícil de localizá-lo. Se Carira não tem bom comércio, então não é difícil de localizá-lo. Carira é pequeno. Logo Carira tem bom comércio.

(b) Se o novo CD de Roberto Carlos é barulhento ou tedioso, então ele não é longo e não custa caro. O novo CD de Roberto Carlos é tedioso. Assim, o CD não é longo.

(c) Se Susan gosta de peixe, então ela gosta de cebolas. Se Susan não gosta de alho, então ela não gosta de cebolas. Se ela gosta de alho, então ela gosta de goiabas. Assim Susan gosta de coentro.

27. Forneça uma negação para: "Você pode enganar alguma pessoa todo o tempo e todas as pessoas por algum tempo, mas você não pode enganar todas as pessoas todo o tempo".

28. Proporcione provas formais para cada um dos argumentos ? utilize tabela-verdade, regras de inferência ou árvores de refutação:

(a) Você vencerá o jogo se, e somente se, você seguir as regras. Se você seguir as regras então você é convencional. Você não é convencional e você tem sempre sucesso. Se você tem sempre sucesso então você vencerá o jogo. Assim você vencerá o jogo.

(b) Se fantasmas são reais, então existem espíritos errantes na terra e se fantasmas não são reais, então nós não temos medo do escuro. Ou temos medo do escuro ou não temos imaginação. Nós temos uma imaginação e fantasmas não são reais. Logo, existem espíritos errantes na terra.

(c) Não existem polinômios que não são funções diferenciáveis. Todas as funções diferenciáveis são contínuas. Assim todos os polinômios são contínuos.

(d) (AFTN 1996 ESAF) José quer ir ao cinema assistir ao filme "Fogo contra fogo", mas não tem certeza se o mesmo está sendo exibido. Seus amigos, Maria, Luís e Júlio têm opiniões discordantes sobre se o filme está ou não em cartaz. Se Maria estiver certa, então Júlio está enganado. Se Júlio estiver enganado, então Luís está enganado. Se Luís estiver enganado, então o filme não esta sendo exibido. Ora, ou o filme "Fogo contra Fogo"está sendo exibido ou José não irá ao cinema. Entretanto, sabe-se que Maria está certa. Logo:

(i) o filme "Fogo contra Fogo"está sendo exibido;

(ii) Luís e Júlio não estão enganados;

(iii) Júlio está enganado, mas Luís não;

(iv) José Não irá ao cinema.

(e) (Assistente de Chancelaria MRE 2004 ESAF) No final de semana, Chiquita não foi ao parque. Ora, sabe-se que sempre que Didi estuda, Didi é aprovado. Sabe-se, também, que, nos finais de semana, ou Dadá vai à missa ou vai visitar tia Célia. Sempre que Dadá vai visitar tia Célia, Chiquita vai ao parque, e sempre que Dadá vai à missa, Didi estuda. Então, no final de semana,

(i) Dadá foi à missa e Didi foi aprovado.

(ii) Didi não foi aprovado e Dadá não foi visitar tia Célia.

(iii) Didi não estudou e Didi foi aprovado.

(iv) Didi estudou e Chiquita foi ao parque.

(v) Dadá não foi à missa e Didi não foi aprovado.

29. Matilda sempre come pelo menos um dos seguintes alimentos em seu café da manhã: cereal, pão ou iogurte. Na segunda-feira ela é especialmente seletiva. Se ela come cereal e pão, ela também come iogurte. Se ela come pão ou iogurte, então come cereal. Ela nunca come ambos cereal e iogurte. Ela sempre come pão ou cereal. Você pode dizer o que Matilda come na segunda-feira?

30. (FCC/TRT-PE - Analista/2006) Uma turma de alunos de um curso de Direito reuniu-se em um restaurante para um jantar de confraternização e coube a Francisco receber de cada um a quantia a ser paga pela participação. Desconfiado que Augusto Berenice e Carlota não tinham pago as suas respectivas partes, Francisco conversou com os três e obteve os seguintes depoimentos:

    Augusto: Não é verdade que Berenice pagou ou Carlota não pagou.

    Berenice: Se Carlota pagou, então Augusto também pagou.

    Carlota: Eu paguei, mas sei que pelo menos um dos dois outros não pagou.

    Considerando que os três falaram a verdade, é correto afirmar que:

    (a) apenas Berenice não pagou a sua parte;

    (b) apenas Carlota não pagou a sua parte;

    (c) Augusto e Carlota não pagaram suas partes;

    (d) Berenice e Carlota pagaram suas partes;

    (e) os três pagaram suas partes.

31. (Cespe-Unb/Anac/2009) As equipes A, B e C disputaram as finais de um torneio de futebol, jogando cada equipe contra as outras duas uma vez. Sabe-se que a equipe B ganhou da equipe A por 2×1; a equipe A marcou 3 gols; e cada equipe ficou com saldo de gols zero. As regras do torneio para a classificação final são, nessa ordem: maior número de vitórias; maior número de gols feitos; se as tres equipes ficarem empatadas segundo os critérios anteriores, as três serão consideradas campeãs. Se uma equipe for campeã ou terceira colocada e as outras duas equipes ficarem empatadas segundo os critérios anteriores, será considerada mais bem colocada a equipe vencedora do confronto direto entre as duas.

    A respeito dessa situação hipotética e considerando que os três critérios listados foram suficientes para definir a classificação final das três equipes, julgue os itens seguintes quanto aos valores lógicos das proposições apresentadas.

    Item 1. Se a equipe B fez 3 gols, então a equipe C foi campeã é uma proposição falsa.

    Item 2. A equipe B foi campeã e a equipe A ficou em último lugar é uma proposição falsa.

Item 3. O número de gols marcados pelas equipes nas finais foi maior que 6 é uma proposição verdadeira.

Item 4. Se a equipe A foi campeã então a equipe C foi campeã ou segunda colocada é uma proposição falsa.

Item 5. A equipe A foi campeã ou a equipe C foi campeã é uma proposição verdadeira.

32. (Esaf/Fiscal - Recife/2003) Um jardineiro deve plantar cinco árvores em um terreno em que não há qualquer árvore. As cinco árvores devem ser escolhidas entre sete diferentes tipos, a saber: A, B, C, D, E, F, G, obedecidas as seguintes condições:

    1. Não pode ser escolhida mais de uma árvore de um mesmo tipo.
    2. Deve ser escolhida uma árvore ou do tipo D ou do tipo C, mas não podem ser escolhida uma árvore de ambos os tipos.
    3. Se uma árvore do tipo B for escolhida, então não pode ser escolhida uma árvore do tipo D. Ora, o jardineiro não escolheu nenhuma árvore do tipo G.

    Logo, ele também não escolheu nenhuma árvore do tipo:

    (a) D;

    (b) A;

    (c) C;

    (d) B;

    (e) E.

33. (Esaf/AFTN/1998) Há três suspeitos de um crime: o cozinheiro, a governanta e o mordomo. Sabe-se que o crime foi efetivamente cometido por um ou por mais de um deles, já que podem ter agido individualmente ou não. Sabe-se, ainda, que: A) se o cozinheiro é inocente, então a governanta é culpada; B) ou o mordomo é culpado ou a governanta é culpada, mas não os dois; C) o mordomo não é inocente. Logo:

    (a) a governanta e o mordomo são os culpados;

    (b) o cozinheiro e o mordomo são os culpados;

    (c) somente a governanta é culpada;

    (d) somente o cozinheiro é inocente;

    (e) somente o mordomo é culpado.

CAPÍTULO 3

Técnicas de Provas

O que é uma prova? Heuristicamente, uma prova é um dispositivo retórico para convencer alguém que uma afirmação matemática é verdadeira. Assim, uma prova é um dispositivo de comunicação. E como podemos fazer isso? Um modo natural é provar que algo novo, digamos B, é verdade relacionando ele a algo antigo A, que já tenha sido aceito como verdadeiro. Ou seja, $A \Rightarrow B$. Mas como foi o resultado antigo verificado? Aplicando o pensamento anterior repetidamente, encontramos uma cadeia de raciocínios tipo

$$A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_k \Rightarrow B$$

Poderíamos perguntar então: "Quando a cadeia inicia?"E esta é uma questão fundamental. Se não quisermos voltar indefinidamente, usamos objetos que são assumidos sem definição, bem como alguns fatos sobre esses objetos que são assumidos sem prova. Euclides foi o primeiro a formalizar o modo que hoje usamos para estabelecer fatos matemáticos, iniciando com um conjunto de definições e um conjunto de axiomas.

Que é uma definição? Uma **definição** explica o significado matemático de uma palavra, permitindo separar uma classe de objetos de outra. A palavra é geralmente definida em termos de propriedades. Por exemplo: (i) um inteiro é par se ele é o produto de 2 e outro inteiro; (ii) um número natural é primo se ele é maior que 1 e é divisível somente por 1 e ele mesmo. Mas então recaímos no mesmo problema de volta infinita! Assim, nossas primeiras definições devem ser formuladas em termos de palavras que não requeiram outras explicações. Por exemplo, Euclides definiu um ponto como sendo aquele que não tem parte.

O que é um axioma? Um **axioma** (ou postulado) é uma afirmação matemática auto-evidente. Eles são assumidos como verdadeiros sem a necessidade de provas. Um dos mais famosos axiomas em toda a matemática é o postulado das paralelas de Euclides que afirma que "se um ponto P não pertence a uma reta ℓ, então existe uma única reta ℓ' passando por P que é paralela à reta ℓ.

O que é que provamos em matemática? Provamos afirmações que são usualmente chamadas de teoremas, proposições, lemas, corolários e exercícios. Não existe muita distinção entre esses tipos de afirmações: todas necessitam de provas. Em geral, em qualquer área da matemática, iniciamos com uma breve lista de definições e axiomas. A partir daí deduzimos diversas outras afirmações. Demonstra-se que um teorema é verdadeiro por uma sequência de afirmações que formam um argumento, chamado prova. Para construir provas, precisamos de métodos que nos permitam deduzir novas afirmações a partir de afirmações já provadas. As afirmações usadas numa prova incluem axiomas ou postulados (afirmações que assumimos como verdadeiras), as hipóteses do teorema a provar e teoremas previamente provados. Teoremas são as mais importantes afirmações matemáticas. Muita (se não todas) afirmações de teoremas são

essencialmente afirmações condicionais ou combinações delas, mesmo que as palavras "se,$\cdots$, então"não apareçam explicitamente.

Proposições são afirmações consideradas menos importantes. Por exemplo, nos teoremas abaixo encontre as hipóteses e as conclusões.

(1) Todo número natural pode ser escrito como um produto de números primos.

(2) Existem infinitos números primos.

(3) O número $\sqrt{2}$ é irracional.

(4) **Teorema de Pitágoras**: Seja $\triangle ABC$ um triângulo retângulo, com lados de comprimento a, b e c, onde c é o comprimento da hipotenusa. Então $c^2 = a^2 + b^2$.

Observação 3.0.15. *Os melhores teoremas têm hipóteses fracas e conclusões fortes. Uma hipótese forte refere-se a um pequeno conjunto de objetos. Uma conclusão forte diz respeito a algo muito definido e preciso sobre esses objetos. Por exemplo, a hipótese de* (2) *é forte, pois refere-se somente ao conjunto de primos, enquanto a hipótese de* (1) *é fraca. Podemos enfraquecer as hipóteses do teorema* (3) *por investigar a raiz quadrada de números primos, digamos "Se* p *é primo, então* $\sqrt{p}$ *é um número irracional."Uma parte importante do desafio matemático é sabermos o quanto podemos enfraquecer as hipóteses. Por exemplo, se fizermos* (3) *para* n *um número natural, esta afirmação se torna falsa.*

Observação 3.0.16. *A recíproca é verdadeira? Considerar a recíproca nos força a considerar as hipóteses e conclusões e muitas vezes nos diz algo importante. Por exemplo, "Se* f *é uma função derivável, então* f *é uma função contínua."A recíproca é verdadeira?*

Um lema é uma afirmação que serve de base para provar um teorema ou uma proposição. Um corolário é uma afirmação de interesse que é deduzida (consequência) de um teorema ou proposição. Exercícios são afirmações que são deixadas para o leitor provar.

Uma prova é uma explanação do porque uma afirmação é verdadeira. Provas são difíceis de entender porque o trabalho inicial em geral é removido. Outra razão para os estudantes não gostarem de provas é que elas são difíceis de criar. Não existe procedimentos, nem algoritmos ou mágica para criar provas. Existem técnicas que podemos empregar.

Exemplo 3.0.17. *Sejam* m *e* n *inteiros. Se* m *e* m *são ímpares, então* $m+n$ *é par.*

Antes de iniciarmos a prova, precisamos saber o que significa um número inteiro ser par ou ser ímpar.

Definição 3.0.18. *Seja* n *um número inteiro. O número* n *é* ***par*** *se existe algum inteiro* k *tal que* $n = 2k$*. O número* n *é* ***ímpar*** *se existe algum interio* j *tal que* $n = 2j+1$*.*

Demonstração. Suponha que n e m são pares. Então existem inteiro k e j tais que $n = 2k$ e $m = 2j$. Assim, $n+m = 2k+2j = 2(k+j)$. Desde que k e j são inteiro, tal é $k+j$. Logo, $m+n$ é par. □

Embutido nesta prova está o uso de regras de inferência. Por exemplo, nossa hipótese é da forma $P \wedge Q$ e queremos mostrar algo do tipo $P \wedge Q \Rightarrow R$. Para tal mostramos que $P \Rightarrow R_1$ e $Q \Rightarrow R_2$. Usamos então o silgismo hipotético para concluir que $P \wedge Q \Rightarrow R$.

Ao ler uma prova, faça o seguinte procedimento: primeiro, procure quebrar ela em pedaços (nesse caso, implicação e recíproca); segundo, identifique os métodos usados - cálculo, direto, indução, contrapositiva, contradição, casos, contra-exemplo, etc.; terceiro, encontre onde as hipóteses foram utilizadas; quarto, verifique (se houver) o texto sem perda de generalidade.

Conjectura é uma afirmação que acreditamos ser verdadeira, geralmente com base em alguma evidência, um argumento heurístico ou intuição, mas não temos prova. Quando uma prova de uma conjectura é encontrada, a conjectura torna-se um teorema. Muitas vezes conjecturas são mostradas serem falsas. Em matemática há uma certa confusão: por exemplo, o último teorema de Fermat que era uma conjectura é um corolário da conjectura Taniyama-Shimura, que é na verdade um teorema.

O principal propósito de uma definição é fazer com que alguém saiba o que estamos falando. Dada uma definição, necessitamos perguntar se um tal objeto existe, como eles são, se é único, se existe um número finito deles.

Articular um número de razões para assegurar que algo é verdadeiro. Argumentos convincentes que mostram que as conclusões seguem logicamente das hipóteses. Pensar ou escrever provas é uma tarefa árdua, especialemente sob coisas mais abstratas. Não espere construí-las rapidamente.

3.1 O Método Direto

Os métodos de prova são importantes não apenas porque são usados para provar teoremas matemáticos, mas também por suas aplicações em ciência da computação, incluindo verificação da correção de programas de computadores, estabelecer a segurança de sistemas operacionais, fazer inferência em inteligência artificial, mostrar que as especificações do sistema são consistentes, etc.. O objetivo é ensinar você a ler e entender uma prova escrita por identificar a técnica que tem sido usada.

Quando resolve um problema, voce tenta todo tipo de visão para encontrar algo que funcione, talvez iniciando com as hipóteses e trabalhando para a frente, ou iniciando com a conclusão e trabalhando para trás, ou uma combinação dos dois.

Para provar que $P \Rightarrow Q$ diretamente, você prova que $P \Rightarrow P_1$, que $P_1 \Rightarrow P_2$, e assim por diante, até obter $P_n \Rightarrow Q$. Então a hipótese que P é verdade e o uso repetido de *modus ponens* mostra que Q é verdade.

O método direto é o método de prova mais amplamente usado. Na prática, pode ser completamente difícil entender as várias afirmações intermediárias que permitem você proceder de P a Q. Com o objetivo de encontrar elas, a maioria dos matemáticos usam um processo chamado técnica pra frente-pra trás. Você inicia trabalhando para frente e perguntando a si mesmo: o que eu sei sobre a hipótese? Quais afirmações seguem desse fato? E assim por diante. Nesse ponto temos uma lista de afirmações implicadas por P cuja conexão com a conclusão Q ainda não está clara.

Agora trabalhamos para trás a partir de Q perguntando: Quais fatos garantem que Q é

verdadeiro? Quais afirmações implicam nesses fatos? Temos agora uma lista de afirmações que implicam Q. Compare ela com a primeira lista. Se você for um felizardo, alguma afirmação estará em ambas as listas, ou mais provavelmente, existirá uma afirmação S da primeira lista e uma afirmação T da segunda lista tal que você será capaz de mostrar que $S \Rightarrow T$. Logo, teremos que $P \Rightarrow S$ e $S \Rightarrow T$ e $T \Rightarrow Q$, donde $P \Rightarrow Q$.

Obtendo sucesso na técnica pra frente-pra trás, devemos reescrever a prova numa forma mais polida, contendo somente os fatos que são necessários na prova.

Exemplo 3.1.1. *Sejam a, b e c inteiros. Se a divide b e, por sua vez, b divide c, então a divide c.*

Antes de tudo necessitamos saber o que significa um número dividir outro. Dizemos que o inteiro a divide o inteiro b se existir algum número inteiro q tal que $aq = b$. Denotamos este fato por $a \mid b$. Desde que nosso objetivo é mostrar que $a \mid c$, precisamos determinar algum inteiro k tal que $ak = c$. Ora, considerando as hipóteses, temos que existem inteiros q e r tais que $aq = b$ e $br = c$. Um olhar atento a essas duas equações percebemos que $c = br = (aq)r = a(qr)$. Logo, $k = qr$ é o inteiro que procuramos.

Exemplo 3.1.2. *Se a soma de dois números inteiros é par, então a sua diferença também é par.*

Para provarmos este fato, suponhamos $m, n \in \mathbb{Z}$ tais que $m+n$ é par. Ou seja, $m+n = 2k$ para algum inteiro k. Assim, $m = 2k - n$ e daí a diferença pode ser expressa como

$$m - n = (2k - n) - n = 2(k - n).$$

Desde de que a diferença entre dois inteiros continua sendo um inteiro, segue que o número $m - n$ é par, como queríamos demonstrar.

Um erro comum é querer argumentar através de exemplos: se $m = 14$ e $n = 6$, então $m+n = 20$ que é par e $m - n = 88$ que também é par. Logo a afirmação está correta. ISSO NÃO É PROVA!

Exemplo 3.1.3. *Às vezes assumimos o que é para ser mostrado com o intuito de descobrirmos uma técnica de prova. Consideremos o seguinte teorema: Sejam m e n números reais. Se $n > m > 0$, então $\frac{m+1}{n+1} > \frac{m}{n}$.*

Assim, assumindo que nossa conclusão é verdadeira, temos que $(m+1)n > (n+1)m$ (note que isso é verdadeiro porque $m > 0$ e $n > 0$). Dessa forma, $mn + n > mn + m$ e cancelando a parcela em comum, obtemos que $n > m$. Nossa esperança é poder reverter o argumento. De fato, partindo de nossa hipótese temos que

$$\begin{aligned} n &> m \\ &\Rightarrow mn + n = mn + n \\ &\Rightarrow (m+1)n > (n+1)m \\ &\Rightarrow \frac{m+1}{n+1} > \frac{m}{n}. \end{aligned}$$

Muitas vezes um teorema afirma que determinadas proposições $P_1, P_2, \cdots, P_n$ são equivalentes, isto é, $P_1 \Leftrightarrow P_2 \Leftrightarrow P_3 \Leftrightarrow \cdots \Leftrightarrow P_n$ (o que assegura que as n proposições têm a mesma tabela verdade). Uma maneira de provar o teorema é usa a tautologia

$$[P_1 \Leftrightarrow P_2 \Leftrightarrow P_3 \Leftrightarrow \cdots \Leftrightarrow P_n] \equiv [(P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_3) \wedge \cdots \wedge (P_n \Rightarrow P_1)]$$

*Exemplo:*Para cada inteiro n as seguintes afirmações são equivalentes:

(i) n é ímpar;

(ii) n^2 é ímpar;

(iii) $n^2 - 2n + 1$ é par.

Assim, devemos mostrar que $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$ e $(iii) \Rightarrow (i)$. A prova da primeira implicação é direta, pois se n é ímpar, então $n = 2k+1$ para algum inteiro k. Assim, $n^2 = (2k+1)^2 = 2(2k^2+2k)+1 = 2m+1$ expressa que n^2 é ímpar. Na segunda implicação, $(ii) \Rightarrow (iii)$, nossa hipótese é que n^2 é impar. Dessa forma, n^2+1 é par, ou seja $n^2+1 = 2k$ para algum inteiro k. Logo, $n^2 - 2n + 1 = 2k - 2n = 2(k-n)$ o que nos mostra a validade da afirmação (iii). Finalmente, devemos mostrar a terceira implicação. Acontece que o método direto aqui já não é tão óbvio. Usaremos uma expressão lógica equivalente à implicação $P \Rightarrow Q$ que é a sua **contrapositiva** $\sim Q \Rightarrow \sim P$. Dese modo, devemos mostrar que se n é par, então $n^2 - 2n + 1$ é ímpar. Mas isso é fácil, pois se $n = 2k$ para algum inteiro k, segue que $n^2 - 2n + 1 = (2k)^2 - 2(2k) + 1 = 2(2k^2 - 2k) + 1$. Logo, da veracidade da contrapositiva segue a veracidade da implicação em sua forma direta $(iii) \Rightarrow (i)$.

Prova por Contradição (Redução ao Absurdo)

Suponha que você assume a verdade de uma afirmação R e que por um argumento válido verifica-se que $R \Rightarrow S$. Se a afirmação S é de fato falsa, então existe somente uma conclusão possível: a afirmação original R deve ser falsa porque se R e $R \Rightarrow S$ são verdadeiras, então por modus ponens, S teria que ser verdadeiro. Nesse sentido, para provarmos um teorema do tipo $P \Rightarrow Q$, assumiremos como habitual que P é verdadeiro. Então supondo $\sim Q$ como sendo verdade, verificamos que $P \wedge \sim Q \Rightarrow S$, onde S é uma afirmação conhecida ser falsa. Concluímos então que $\sim Q$ deve ser falso, donde Q é verdadeiro.

Veremos agora um exemplo simples de uma prova por contradição e, na sequência, a justificativa para dois resultados famosos.

Teorema: Os únicos inteiros não negativos consecutivos a, b e c que satisfazem $a^2 + b^2 = c^2$ são 3,4 e 5.

A afirmação deste teorema tem a forma $P \Rightarrow Q$, porque ele pode ser reescrito como "se a, b e c são inteiros não negativos e consecutivos tais que $a^2 + b^2 = c^2$, então a, b e c são 3.4 e 5". É difícil provar o resultado diretamente, pois estamos tentando mostrar que algo não existe. Assumiremos então que inteiros consecutivos a, b e c diferentes de 3.4 e 5 satisfazem

$a^2+b^2=c^2$, e encontraremos dessa hipótese uma contradição. Observamos também que se a,b e c são inteiros consecutivos, então $b=a+1$ e $c=a+2$.

Prova: Provamos o resultado por contradição. Suponhamos que a,b e c são inteiros não negativos e consecutivos diferentes de 34 e 5 tais que $a^2+b^2=c^2$. Assim, $a\neq 3$ e como eles são consecutivos, temos que $b=a+1$ e $c=a+2$. De $a^2+b^2=c^2$ deduzimos que $a^2+(a+1)^2=(a+2)^2$. Após expandir e rearrumar os termos, obtemos $a^2-2a-3=0$. Esta equação fatora-se como $(a-3)(a+1)=0$. Logo, os únicos valores possiveis para a seriam $a=3$ ou $a=-1$. Mas isto contradiz o fato que $a\neq 3$ e a é um inteiro não negativo. Portanto, temos uma contradição, e o teorema está provado.

Teorema: A raiz quadrada de 2 é um número irracional.

Prova: Suponha que $\sqrt{2}$ seja um número racional, ou seja, que existam inteiros m e $n\neq 0$ tais que $\sqrt{2}=\frac{m}{n}$. Sem perda de generalidade, podemos assumir que m e n seja tais que $mdcm,n=1$. Então temos que

$$\sqrt{2}=\frac{m}{n}\Rightarrow 2=\frac{m^2}{n^2}\Rightarrow m^2=2n^2.$$

Isto implica que 2 divide o número m^2 e assim 2 divide m (verifique!). Logo, podemos escrever $m=2k$, para algum inteiro k. Substituindo m na expressão acima, obtemos que $(2k)^2=2n^2$, donde $n^2=2k^2$. Dessa forma, concluímos que 2 também divide n, mas isso não é possível pois tomamos m e n tais que $mdcm,n=1$. Portanto, $\sqrt{2}$ é um número irracional.

Note que há uma diferença sutil entre uma prova por contradição e uma prova utilizando a contrapositiva. A prova por contradição termina quando encontramos um absurdo, que necessariamente não tem ligação direta com a hipótese P ou a hipótese assumida $\sim Q$, enquanto que na contrapositiva precisamos determinar exatamente $\sim P$.

Exemplo 3.1.4. *Consideremos um teorema clássico de Euclides: existem infinitos números primos.*

Recorde que um inteiro p maior que 1 é dito ser **primo** se os únicos divisores de p é 1 e ele próprio. Caso contrário, dizemos que p é um número composto. Mostraremos a afirmação por contradição supondo que existe um número finito de números primos, digamos n. Assim, podemos listá-los na forma $p_1,p_2,\cdots,p_n$. Chegaremos a uma contradição exibindo um outro número primo fora desta lista. Consideremos o número $q=p_1\times p_2\times\cdots\times p_n+1$. Ora, como q é maior que quaisquer dos números $p_1,p_2,\cdots,p_n$, segue que q é um número composto. Logo, ele é divisível por algum número primo, digamos p_k, e podemos escrever $q=rp_k$ para um certo inteiro r. Dessa forma,

$$rp_k=p_1\times p_2\times\cdots\times p_n+1,$$

e, consequentemente,

$$p_k(r-p_1\times\cdots\times P-k-1\times p_{k+1}\times\cdots\times p_k)=1.$$

Portanto, p_k divide 1, o que é impossível, pois p_k é primo.

Provas tipo P se, e somente se, Q

Temos que provar as duas condicionais: $P \Rightarrow Q$ e sua recíproca $Q \Rightarrow P$.

Exemplo 3.1.5. *Seja $a \neq 0$,b e c números reais. Então*

$$ax^2 + bx + c = 0 \Leftrightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Desde que $a \neq 0$, podemos dividir a expressão $ax^2 + bx + c = 0$ por a para obtermos $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$. Sem perda de generalidade, podemos assumir que estamos resolvendo $x^2 + \alpha x + \beta = 0$. Posteriormente podemos substituir por $\alpha = \frac{b}{a}$ e $\beta = \frac{c}{a}$. Assim, por completar os quadrados, temos que

$$\begin{aligned}
&\Rightarrow (x + \frac{\alpha}{2})^2 - (\frac{\alpha}{2})^2 + \beta = 0 \\
&\Rightarrow x + \frac{\alpha}{2} = \pm\sqrt{(\frac{\alpha}{2})^2 - \beta} \\
&\Rightarrow x = -\frac{\alpha}{2} \pm \sqrt{(\frac{\alpha}{2})^2 - \beta} \\
&\Rightarrow -\frac{b}{2a} \pm \sqrt{(\frac{b}{2a})^2 - \frac{c}{a}} \\
&\Rightarrow -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} \\
&\Rightarrow \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.
\end{aligned}$$

Faça a prova da recíproca.

Exemplo 3.1.6. *Sejam X e Y conjuntos. Então $X = Y$ se, e somente se, $X \subset Y$ e $Y \subset X$.*

Se $X = Y$, então X e Y têm os mesmos elementos. Assim, se $x \in X$,então $x \in Y$ o que implica $X \subset Y$. Analogamente, se $x \in Y$, então $x \in X$ o que implica $Y \subset X$. Agora para a recíproca suponhamos que $X \subset Y$ e $Y \subset X$. Então cada elemento de X está em Y e cada elemento de Y está em X. Isto significa que X e Y possuem os mesmos elementos, ou seja, $X = Y$.

Exemplo 3.1.7. *Um inteiro positivo n é divisível por 3 se, e somente se, a soma dos dígitos de n é divisível por 3.*

Uma leve versão de teoremas do tipo "se, e somente se"é um teorema que estabelece três ou mais afirmações que são mutuamente equivalentes. Um exemplo é o seguinte teorema:

Teorema: Seja $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ uma matriz triangular superior 2×2. Suponha que a, b e d são inteiros. As seguintes afirmações são equivalentes:

1. $det(M) = 1$;

2. $a = d = \pm 1$;

3. $tr(M) = \pm 2$ e $a = d$.

O teorema acima nos diz que $(a) \Leftrightarrow (b)$, que $(a) \Leftrightarrow (c)$ e que $(b) \Leftrightarrow (c)$. Assim, a princípio, teríamos que provar seis implicações mas na prática, usamos a propriedade da transitividade da implicação lógica e verificamos apenas que $(a) \Rightarrow (b)$, $(b) \Rightarrow (c)$ e $(c) \Rightarrow (a)$. Vamos então a uma prova do referido teorema.

$(a) \Rightarrow (b)$. Suponhamos que $det(M) = 1$. Então $ad = 1$ e, como a e d são inteiros, devemos ter $a = 1$ e $d = 1$, ou $a = -1$ e $d = -1$.

$(b) \Rightarrow (c)$. Suponha que $a = d = \pm 1$. Primeiro consideremos $a = d = 1$. Então $tr(M) = a + d = 2$. Segundo, suponhamos que $a = d = -1$. Então $tr(M) = a + d = -2$. Portanto, $tr(M) = \pm 2$ e $a = d$.

$(c) \Rightarrow (a)$. Suponhamos agora que $tr(M) = \pm 2$ e $a = d$. Podemos reescrever $tr(M) = \pm 2$ como $a + d = \pm 2$. Assim $4 = (a + d)^2 = a^2 + 2ad + d^2$. Porque $a = d$ temos que $a^2 = ad = d^2$, e daí $4 = 4ad$. Segue que $ad = 1$ e, consequentemente, $det(M) = ad = 1$.

Prova por Casos

Algumas vezes não podemos provar um teorema usando um único argumento que valha para todos os casos possíveis. Introduzimos então um método que pode ser usado para provar um teorema por considerar diferentes casos separadamente. Este método é baseado na regra de inferência

$$[(P_1 \vee P_2 \vee \cdots \vee P_n) \Rightarrow Q] \equiv [(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q) \wedge \cdots \wedge (P_n \Rightarrow Q)].$$

Assim, para provarmos uma condicional $P \Rightarrow Q$ é conveniente, às vezes, fazermos a decomposição $P \equiv (P_1 \vee P_2 \vee \cdots \vee P_n)$. Temos visto que $X = Y$ pode ser provado por mostrarmos que $X \subset Y$ e $Y \subset X$. Em outras palavras, quebramos o problema em dois casos. No método de casos precisamos exaurir todas as possibilidades, mesmo que tenhamos casos não exclusivos.

Teorema(Desigualdade Triangular): Suponha que x e y sejam números reais. Então

$$|x + y| \leq |x| + |y|.$$

Prova: Consideremos os casos em que x e y são ambos positivos, ambos negativos ou diferentes em sinal.

Caso 1: Suponha $x \geq 0$ e $y \geq 0$. Então $x + y \geq 0$ e por definição de valor absoluto temos que $|x + y| = x + y = |x| + |y|$.

Caso 2: Suponha $x < 0$ e $y < 0$. Então $x + y < 0$ e por definição de valor absoluto temos que $|x + y| = -(x + y) = -x + (-y) = |x| + |y|$.

Caso 3: Suponha que x e y tenha sinais diferentes, digamos $x \geq 0$ e $y < 0$. Assim temos dois subcasos a considerar: $x+y \geq 0$ ou $x+y < 0$. No primeiro subcaso encontramos que $|x+y| = x+y \leq x+(-y) = |x|+|y|$. Observe que trocamos $y < 0$ por algo maior $-y > 0$. No segundo subcaso, segue da definição de valor absoluto que $|x+y| = -(x+y) = -x+(-y) \leq x+(-y) = |x|+|y|$.

Esses três casos exaure todas as possibilidades e nossa prova está completa.

Exemplo 3.1.8. *O quadrado de qualquer inteiro ímpar tem a forma* $8m+1$ *para algum inteiro* m.

Suponhamos que n é um inteiro ímpar. Pelo Teorema do Algoritmo da Divisão, n pode ser escrito em uma das seguintes formas

$$4q \text{ ou } 4q+1 \text{ ou } 4q+2 \text{ ou } 4q+3,$$

para algum inteiro q. Desde que n é ímpar e $4q$ e $4q+2$ são pares, o número n deve ter uma das formas: $4q+1$ ou $4q+3$. Consideremos então esses dois casos.

Caso 1: Se $n = 4q+1$, então $n^2 = (4q+1)^2 = 8(2q^2+q)+1$ é ímpar;

Caso 2: Se $n = 4q+3$, então $n^2 = (4q+3)^2 = 8(2q^2+3q+1)+1$ é ímpar.

Provas de Existência

Retornaremos nossa atenção para provas de teoremas de existência, isto é, teoremas que afirmam dentro do universo de discurso a existência de um objeto ou mais objetos com uma certa propriedade P. Simbolicamente, $\exists x, P(x)$.

Exemplo 3.1.9. *(1) Alguns números primos são da forma* $32n+1$, *onde* n *é um inteiro.*

(2) Nem todos os números reais são racionais.

(3) O Teorema do Valor Médio diz que se f *é uma função contínua sobre o intervalo fechado* $[a,b]$ *e derivável sobre o intervalo aberto* (a,b), *então existe* $c \in (a,b)$ *tal que* $\frac{df}{dx}(c) = \frac{f(b)-f(a)}{b-a}$.

A maneira mais óbvia de provarmos um teorema da forma $\exists x, P(x)$ é encontrar (construir) um objeto específico a no universo de discurso para o qual $P(a)$ é verdadeiro. Este método de prova é também chamado prova por construção.

Uma prova de $\exists x \in U, P(x)$ consiste então de definir/construir um z_0 e mostrar que $z_0 \in U$ e que $P(z_0)$ é verdadeiro. Frequentemente, construimos z_0 assumindo a priori que $P(z_0)$ é válido.

Exemplo 3.1.10. *Existe uma matriz* 2×2 *com entradas inteiras tal que* $det(A) = 4$ *e* $tr(A) = 7$.

Demonstração. Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. A condição $det(A) = 4$ significa que $ad - bc = 4$; e a condição $tr(A) = 7$ significa que $a + d = 7$. Temos então duas equações com quatro variáveis. Uma solução seria $a = 3$ e $d = 4$, donde $-bc = -8$ e, consequentemente, $b = 2$ e $c = 4$. Logo, $A = \begin{pmatrix} 3 & 2 \\ 4 & 4 \end{pmatrix}$. □

Exemplo 3.1.11. *Consideremos o seguinte teorema: Para qualquer inteiro n, a multiplicação de matrizes $n \times n$ não é comutativa. Dizer que a multiplicação é comutativa é dizer que $\forall x, y; (xy = yx)$. Assim, o nosso teorema afirma justamente a negação desse fato, ou seja,*

$$\sim \forall x, y; (xy = yx) \equiv \exists x \exists y; (xy \neq yx).$$

Logo, para provarmos o teorema, devemos encontrar duas matrizes, digamos 2×2, A e B, com a propriedade que $AB \neq BA$. Por exemplo, $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ e $B = \begin{pmatrix} -1 & 1 \\ 3 & 2 \end{pmatrix}$ satisfazem tal condição.

Também é possível dá uma prova de existência não construtiva, isto é, não encontramos um elemento a tal que $P(a)$ seja verdade, mas provamos que $\exists x, P(x)$ é verdadeiro em alguma forma. Há teoremas em matemática que afirmam a existência de determinados objetos sem produzir um exemplo do tipo desejado. Por exemplo, todo polinômio de grau ímpar tem pelo menos uma raiz real. Note que $f(x) = x^5 + 2x - 5 = 0$ possui uma raiz entre $x = 1$ e $x = 2$.

Exemplo 3.1.12. *Mostre que existem números irracionais x e y tais que x^y é racional. Consideremos o número $\sqrt{2}^{\sqrt{2}}$. Se ele é racional, então $x = \sqrt{2}$ e $y = \sqrt{2}$ são dois números irracionais tais que x^y é racional. Por outro lado, se $\sqrt{2}^{\sqrt{2}}$ é irracional, então fazendo $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ temos que*

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$$

é racional. Mostramos então que a existência do par x e y.

Provas para trás são tão comuns em matemática que infelizmente passam despercebidas pelos alunos, e raramente são criticadas. O cuidado aqui é verificar se todos os passos computacionais podem ser revertidos. Por exemplo, considere a afirmação que existe $x \in \mathbb{R}$ tal que

$$\begin{aligned} &\sqrt{x+3} = x+1 \\ \Rightarrow &x+3 = (x+1)^2 \\ \Rightarrow &x+3 = x^2+2x+1 \\ \Rightarrow &0 = x^2+x-2 \\ \Rightarrow &0 = (x-1)(x+2). \end{aligned}$$

Então $x = 1$ ou $x = -2$ são nossas soluções. Devemos observar que $x = -2$ não é solução. Isso se deve porque nem todas as implicações são reversíveis. Descubra qual.

Provas de Unicidade

Algumas vezes em Matemática, desejamos provar não somente que um objeto com certas propriedades existe, mas também que existe somente um tal objeto, isto é, o objeto é único. Precisamos então provar duas coisas: existencia e unicidade; e é bom provarmos cada uma dessas coisas separadamente. Não faz diferença qual parte é provada primeiro. Para provarmos existência agimos como antes, e produzimos um exemplo do objeto desejado. Para provarmos unicidade, o método é essencialmente o método de prova por contradição. Seja $P(x)$ a função proposicional e x um objeto com as propriedades requeridas. Então supomos que existem dois objetos distintos satisfazendo as mesmas propriedades, ou seja,

$$\exists x \exists y, [P(x) \wedge P(y) \wedge (x \neq y)].$$

A conclusão falsa que é geralmente obtida da nossa hipótese é que $x = y$.

Exemplo 3.1.13. *Mostre que se a, b, c e d são números reais tais que $ad - bc \neq 0$, então existe uma única solução para o sistema de equações*

$$\begin{aligned} ax + by &= s \\ cx + dy &= t \end{aligned}$$

quaisquer que sejam os reais s e t.

Para provarmos a existência construiremos uma solução. É claro que a ou c é diferente de zero, pois se ambos fossem zero teríamos $ad - bc = 0$, contrariando nossa hipótese. Vamos supor $a \neq 0$. Então podemos "tirar"o valor de x na primeira equação e substituir na segunda equação. De fato,

$$x = \frac{s - by}{a} \Rightarrow c\frac{s - by}{a} + dy = t \Rightarrow (ad - bc)y = at - cs \Rightarrow y = \frac{at - cs}{ad - bc}.$$

Retornando esse valor de y na expressão em x, encontramos que

$$x = \frac{ds - bt}{ad - bc}.$$

Logo exibimos uma solução. Agora para mostrarmos que esta é única, supomos a existência de duas soluções distintas, digamos (x_1, y_1) e (x_2, y_2). Ou seja,

$$\begin{aligned} ax_1 + by_1 &= s \\ cx_1 + dy_1 &= t \end{aligned}$$

e

$$\begin{aligned} ax_2 + by_2 &= s \\ cx_2 + dy_2 &= t. \end{aligned}$$

Agindo de forma semelhante ao realizado para encontrar uma solução, verificamos que

$$x_1 = \frac{ds - bt}{ad - bc} = x_2 \text{ e } y_1 = \frac{at - cs}{ad - bc} = y_2.$$

Exemplo 3.1.14. *Seja A uma matriz 2×2 tal que $det(A)\neq 0$. Então A tem uma única matriz inversa.*

A frase "A tem uma única matriz inversa"significa que existe uma matriz inversa para A e que esta é única. Iniciamos provando a unicidade. Para isso, assumiremos que A tem duas matrizes inversas B e C e então usaremos propriedades de matrizes para mostrar que $B=C$. Ora, por definição de matriz inversa, temos as seguintes identidades: $AB=I=BA$ e $AC=I=CA$, onde I é a matriz identidade de ordem 2×2. Assim,

$$B=BI=B(AC)=(BA)C=IC=C.$$

Agora, para provarmos a existência, podemos adotar duas estratégias: uma construtivista e outra exibicionista. Na primeira alternativa, supomos a matriz A como sendo $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e construiremos uma matriz $B=\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ satisfazendo $AB=I=BA$. Ou seja,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

que fornece quatro equações

$$\begin{aligned} ax+bz&=1\\ ay+bw&=0\\ cx+dz&=0\\ cy+dw&=1, \end{aligned}$$

onde x,y,z e w são nossa incógnitas a serem determinadas em função de a,b,c e d. Ora, a solução para esse sistema é dada por

$$\begin{aligned} x&=\frac{d}{ad-bc},\\ y&=\frac{-b}{ad-bc},\\ z&=\frac{-c}{ad-bc},\\ w&=\frac{a}{ad-bc}. \end{aligned}$$

Vemos aqui a necessidade da hipótese $det(A)=ad-bc\neq 0$ para que a matriz B encontrada faça sentido.

Por outro lado, poderíamos, "de bate pronto", exibir a matriz inversa B, descoberta talvez por intuição, por sorte, por tentativa e erro, por experiencia,... E aí o que nos resta é verificar que esta matriz é de fato inversa da matriz A. Ou seja, se $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, com a condição que $det(A)\neq 0$, e supormos que

$$B=\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc}, \end{pmatrix}$$

basta mostrarmos que $AB=I=BA$.

Uso de Contra-Exemplos

Um entendimento de quantificadores é também útil quando queremos provar que uma dada afirmação é falsa. Suponha que queremos provar que uma afirmação da forma "$\forall x \in U, P(x)$"é falsa. Então isto equivale a encontrar um x_0 em U tal que $\sim P(x_0)$ é verdadeiro. O elemento x_0 é chamado um **contra-exemplo** para a afirmação original. Em outras palavras, um contra-exemplo é um exemplo que desaprova uma afirmação universal. Ou seja, dada uma afirmação tipo $\forall x, P(x)$, queremos encontrar um a no universo de discurso tal que $P(a)$ seja falso. De fato, recorde que

$$\sim \forall x, P(x) \equiv \exists x, \sim P(x).$$

Exemplo 3.1.15. *Em 1540 Fermat afirmou que para todo inteiro positivo n, o inteiro $F_n = 2^{2^n} + 1$ é primo, mas não foi capaz de fornecer uma prova. De fato, observamos que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65.537$ são primos. Mas isto não constitui uma prova! Somente em 1732 é que Euler (Óiler) estabeleceu que $F_5 = 4.294.967.297 = 641 \times 6.700.417$ era um número composto e, portanto, a conjectura de Fermat era falsa.*

Observações:

(1) Um único exemplo não pode provar uma afirmação universal, mas um único contra-exemplo pode desaprová-la.

(2) Para dá um contra-exemplo de uma afirmação condicional $P \Rightarrow Q$, encontre um caso onde P é verdade, mas Q é falso.

(3) A conjectura de Goldbach - "Todo inteiro par maior que 4 pode ser representado como uma soma de dois primos", cuja solução vale um milhão de dólares, teve sua veracidade verificada no computador para números até 10^{17}. Mas prova que é bom, nada!

Exemplo 3.1.16. *Encontre um contra-exemplo para a proposição: para todos os números reais x e y, se $x \leq y$, então $|x| \leq |y|$. Precisamos encontrar números reais a e b tais que $a \leq b$, porém $|a| > |b|$. Tente!*

A presença de quantificadores, e especialmente quantificadores múltiplos, nas afirmações de teoremas é uma fonte de erros na construção de provas válidas para os iniciantes. A definição de limite é um exemplo de uma afirmação de existência. Sejam $f : \mathbb{R} \to \mathbb{R}$ e $c \in \mathbb{R}$. A afirmação

$$\lim_{x \to c} f(x) = L$$

significa que para cada $\varepsilon > 0$ dado, existe um $\delta > 0$ tal que, se $0 < |x - c| < \delta$ então

$$|f(x) - L| < \varepsilon.$$

Assim, para mostrarmos que

$$\lim_{x \to 2}(5x + 4) = 14,$$

tomamos um $\varepsilon > 0$ qualquer e exibimos para ele um $\delta > 0$ de forma que a definição de limite seja satisfeita. Para construirmos um tal $\delta > 0$ usamos o que queremos provar. Ou seja,

$$|(5x+4)-14| = |5x-10| = 5|x-2|$$

e observamos que esta expressão será menor que ε se fizermos $|x-2| < \delta \leq \frac{\varepsilon}{5}$. Logo, dado $\varepsilon > 0$, existe $\delta \leq \frac{\varepsilon}{5}$ tal que se $|x-2| < \delta$ temos $|(5x+4)-14| < \varepsilon$.

Afirmações envolvendo mais de um quantificador tipicamente têm a forma $\forall y, \exists x; P(x,y)$ ou $\exists x, \forall y; Q(x,y)$, com x e y num universo de discurso U. Usaremos sempre a mesma estratégia: tomaremos um quantificador por vez, de fora para dentro.

Exemplo 3.1.17. *Para cada número real a, existe um número real b tal que* $a^2 - b^2 + 4 = 0$.

Esta afirmação possui a forma $\forall a, \exists b; (a^2 - b^2 + 4 = 0)$, onde a e b são números reais. Iniciamos a prova então com o quantificador de fora, isto é, $\forall a$. Podemos reescrever a afirmação a ser provada como $\forall a, Q(a)$, onde $Q(a) =$ "$\exists b, (a^2 - b^2 + 4 = 0)$". Tomamos então um número real arbitrário a_0 tal que $Q(a_0)$ é válida. Logo, devemos mostrar que $\exists b, ((a_0)^2 - b^2 + 4 = 0)$ vale. Facilmente, obtemos dois números reais b que validam tal afirmação, a saber: $b = \pm\sqrt{(a_0)^2+4}$. Duvida? Verifique!

Exemplo 3.1.18. *Existe um número real x tal que* $(3-x)(y^2+1) > 0$ *para todo número real y.*

Esta afirmação tem a forma $\exists x, \forall y; ((3-x)(y^2+1) > 0)$, onde x e y são números reais. Outra vez iniciamos com o quantificador externo. Reescrevemos a sentença como $\exists x, R(x)$, onde $R(x) = \forall y, ((3-x)(y^2+1) > 0)$. Assim, devemos produzir um número real x_0 tal que $R(x_0)$ seja válido. Ou seja, precisamos encontrar um real x_0 tal que, se escolhermos um número real arbitrário y_0, então $(3-x)(y^2+1) > 0$ vale. Ora, sabemos que $(y_0)^2 + 1 > 0$ qualquer que seja $y_0 \in \mathbb{R}$, de forma que basta tomarmos x_0 tal que $3 - x_0 > 0$. Portanto, nossa afirmação é válida se tomarmos $x_0 < 3$.

3.2 Indução Matemática

Existem muitas situações matemáticas que podem ser formuladas como

$$\forall n \in \mathbb{N}, P(n),$$

onde o universo de discurso é o conjunto dos números naturais.

Exemplo 3.2.1. *(1) A soma dos n primeiros números naturais é dada pela expressão* $\frac{n(n+1)}{2}$;

(2) Para todo número natural n, qualquer conjunto com n elementos possui 2^n *subconjuntos;*

(3) $\forall n \in \mathbb{N}, n! \leq n^n$;

(4) Para todo número natural n, $8^n - 3^n$ *é divisível por 5.*

Assumiremos o **Axioma da Boa-Ordenação** que nos diz que

"Todo subconjunto não-vazio dos números naturais contém um menor elemento".

Teorema 3.2.2 (O Princípio de Indução Matemática)**.** *Suponha que para cada número natural n, uma afirmação $P(n)$ é dada. Se valem as seguintes condições:*

(i) $P(1)$ *é uma afirmação verdadeira;*

(ii) $P(k)$ *verdadeiro implicar* $P(k+1)$ *verdadeiro;*

concluímos que a afirmação $P(n)$ *é verdadeira para todo* $n \in \mathbb{N}$.

Numa linguagem de conjuntos, temos que se $G = \{n \in \mathbb{N} : P(n)\}$ contido em $\mathbb{N}$ é tal que $1 \in G$ e $k+1 \in G$ sempre que $k \in G$, então $G = \mathbb{N}$.

Demonstração. Seja S o subconjuntos dos números naturais constituído pelos números naturais $k \geq 1$ tais que $P(k)$ é falso. Provaremos que S é vazio. Para isso usamos uma prova por contradição. Suponha que S é não-vazio. Então podemos usar o Princípio da Boa-Ordenação para garantir a existência de um menor elemento em S, digamos d. Desde que $P(d)$ é falso, segue da hipótese (i) que $d > 1$. Consequentemente, $d-1 \geq 1$. Como $d-1 < d$, ele não pode está em S. Logo $P(d-1)$ é verdadeiro. Mas pela hipótese (ii) temos que $P[(d-1)+1] = P(d)$ também é verdadeiro. Isto é uma contradição, pois $d \in S$. Portanto, S é vazio. □

Observação 3.2.3. *Note que a hipótese* (ii) *não afirma que* $P(k)$ *é verdadeiro para todo* k *natural, mas somente que uma relação condicional vale. A hipótese* (ii) *é chamada a* ***hipótese de indução****.*

Expresso como uma regra de inferência, o Princípio de Indução Matemática pode ser estabelecido como

$$\{P(1) \wedge (\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1))\} \Rightarrow \forall n \in \mathbb{N}, P(n)$$

Exemplo 3.2.4. *Para todo número natural* n*, a soma dos primeiros* n *números naturais é dada pela expressão*

$$P(n) : 1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Assim, para provarmos que de fato essa afirmação vale para todo $n \in \mathbb{N}$*, devemos verificar que as hipóteses* (i) *e* (ii) *são válidas.*

Segunda Lista de Exercícios

1. Reformule cada um dos seguintes teoremas na forma $P \Rightarrow Q$.

   (a) A área da região dentro de um círculo de raio r é πr^2;

   (b) Dados uma reta l e um ponto P fora dela, existe exatamente uma reta m contendo P que é paralela a l;

(c) Seja $\triangle ABC$ um triângulo com lados a, b e c. Então

$$\frac{a}{sen(A)} = \frac{b}{sen(B)} = \frac{c}{sen(C)}.$$

(d) (Teorema Fundamental do Cálculo) Seja f uma função contínua sobre $[a,b]$ e seja F qualquer função para a qual $F'(x) = f(x)$. Então

$$\int_a^b f(x)dx = F(b) - F(a).$$

2. Escreva uma prova direta para as seguintes afirmações:

(a) Sejam A, B e C conjuntos. Se $A \subset B$ e $B \subset C$, então $A \subset C$.

(b) Todo inteiro ímpar é a diferença de dois quadrados.

(c) Seja $x \in \mathbb{Z}$. Se 2^{2x} é um inteiro ímpar, então 4^x é um inteiro ímpar.

3. Use a contrapositiva para provas as seguintes afirmações:

(a) Seja $n \in \mathbb{Z}$. Se $15n$ é par, então $9n$ é par.

(b) Seja $n \in \mathbb{Z}$. Prove que $(n+1)^2 - 1$ é par se, e somente se, n é par.

4. Prove por casos as seguintes afirmações:

(a) Se n é um número natural, então $n^2 + n + 3$ é ímpar.

(b) Sejam $x, y \in \mathbb{Z}$. Prove que se xy é ímpar, então x e y são ímpares.

(c) Sejam $x, y \in \mathbb{Z}$. Prove que $x - y$ é par se, e somente se, x e y têm a mesma paridade.

(d) Sejam $x, y \in \mathbb{Z}$. Prove que se $x + y$ e xy têm a mesma paridade, então x e y são pares.

5. Prove por contradição as seguintes afirmações:

(a) $\sqrt[3]{2}$ não é racional.

(b) Se n é um número natural, então $\frac{n}{n+1} > \frac{n}{n+2}$.

(c) Se x é irracional, então $1/x$ é irracional.

(d) Não existe número racional x para o qual $x^3 + x + 1 = 0$.

(e) Prove que se x e y são números reais positivos, então $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$.

6. Seja a e b inteiros. Dizemos que dois inteiros a e b são **relativamente primos** se $mdca, b = \pm 1$. Ou seja, os únicos dividores comuns de a e b são 1 e -1. Mostre que as seguintes afirmações são equivalentes:

(a) a e b são relativamente primos;

(b) a e $-b$ são relativamente primos;

(c) $a + b$ e b são relativamente primos;

(d) $a-b$ e b são relativamente primos.

7. Prove que:

   (a) não existem inteiros m e n tais que $2m+4n=7$.

   (b) se m é um inteiro ímpar, então $m^2 = 8k+1$, para algum k inteiro. Use o fato que $k(k+1)$ é par para qualquer inteiro k.

   (c) para todos os inteiros a,b e c, se a divide b e a divide c, então a divide bc.

   (d) se existirem inteiros m e n tais que $am+bn=1$ e $d>1$, então d não divide a ou d não divide b.

   (e) se x e y são racionais com $x<y$, então existe um número racional entre x e y.

8. Proporcione uma prova ou um contra-exemplo para cada uma das afirmações:

   (a) Para todo inteiro positivo n, n^2-n+17 é um número primo;

   (b) para todo x e y reais, se $x>1$ e $y>0$, então $y^x > x$;

   (c) para todos os inteiros a,b e c, se a divide bc, então a divide b ou a divide c;

   (d) para todos os números reais positivos x, $x^2-x>0$.

9. Prove que $mmc(a,b).mdc(a,b) = ab$, para todos os números naturais a e b.

10. Prove ou desaprove que se a e b são números racionais, então a^b é também racional.

11. Sejam $a,b \in \mathbb{Z}$, onde $a \neq 0$ e $b \neq 0$. Prove que se $a \mid b$ e $b \mid a$, então $a=b$ ou $a=-b$.

12. Sejam $x,y \in \mathbb{Z}$. Prove que se $3 \nmid x$ e $3 \nmid y$, então $3 \mid (x^2-y^2)$.

13. Prove que se a e b são números reais positivos, então $\sqrt{ab} \leq \frac{a+b}{2}$. Sob quais condições vale a igualdade?

14. Sejam $x,y \in \mathbb{R}$. Prove que $|xy| = |x| \cdot |y|$.

15. Prove que para quaisquer dois números reais a e b, não ambos nulos, temos $\frac{a}{b}+\frac{b}{a} \geq 2$.

16. Uma prova do seguinte resultado é dada.
Resultado: Seja $n \in \mathbb{Z}$. Se n^4 é par, então $3n+1$ é ímpar.
Prova: Suponha que $n^4 = (n^2)^2$ é par. Desde que n^4 é par, n^2 é par. Além disso, como n^2 é par, segue que n é par. Porque n é par, $n=2k$ para algum inteiro k. Então

$$3n+1 = 3(2k)+1 = 6k+1 = 2(3k)+1.$$

Desde que $3k$ é um inteiro, $3n+1$ é ímpar.
Responda as seguintes questões:

   (1) Qual técnica de prova está sendo usada?

   (2) Qual é a hipótese inicial?

(3) O que deve ser mostrado para fornecer uma prova completa?

(4) Dê uma razão para cada um dos seguintes passos na prova.

(a) Desde que n^4 é par, n^2 é par.

(b) Além disso, como n^2 é par, segue que n é par.

(c) Porque n é par, $n = 2k$ para algum inteiro k.

(d) Então $3n+1 = 3(2k)+1 = 6k+1 = 2(3k)+1$.

(e) Desde que $3k$ é um inteiro, $3n+1$ é ímpar.

17. Prove que cada uma das seguintes sentenças são válidas para todo $n \in \mathbb{N}$.

(a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(n+2)}{6}$;

(b) $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$;

(c) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.

18. Encontre uma fórmula para $1 + 4 + 7 + \cdots + (3n-2)$, onde n é um inteiro positivos e então verifique a validade dessa fórmula por indução matemática.

19. Prove que $1 + 2n \leq 3^n$ para todo $n \in \mathbb{N}$.

20. Sejam $a, b \in \mathbb{N}$. Prove que $a^n - b^n$ é divisível por $a - b$, para todo $n \in \mathbb{N}$.

21. Prove que $(1 + \frac{1}{n})^n < n$ para todo $n \geq 3$.

22. Prove que $3^n > n^3$ para todo $n \in \mathbb{N}$ tal que $n \geq 4$.

23. Seja $r \neq 1$ um número real. Use indução para provar que $a + ar + ar^2 + \cdots + ar^{n-1} = \frac{a(1-r^n)}{1-r}$ para cada inteiro positivo n.

24. Prove a identidade de Bernoulli: para cada número real $x > -1$ e cada inteiro positivo n, $(1+x)^n \geq 1 + nx$.

25. Seja $r_1, r_2, r_3, \cdots$ uma sequência definida por $r_1 = 1$ e $r_{n+1} = 4r_n + 7$, para todo $n \in \mathbb{N}$. Prove que $r_n = \frac{1}{3}(10 \cdot 4^{n-1} - 7)$, para todo $n \in \mathbb{N}$.

26. Seja $b_1, b_2, b_3, \cdots$ a sequência definida por $b_1 = 1$, $b_2 = 1$ e $b_n = \frac{1}{3}\left(b_{n-1} + \frac{3}{b_{n-2}}\right)$ para todo $n \in \mathbb{N}$ tal que $n \geq 3$. Prove que $1 \leq b_n \leq \frac{3}{2}$ para todo $n \in \mathbb{N}$.

27. Seja $d_1, d_2, d_3, \cdots$ a sequência definida por $d_1 = 2$, $d_2 = 3$ e $d_n = d_{n-1} \cdot d_{n-2}$ para todo $n \in \mathbb{N}$ tal que $n \geq 3$. Encontre uma fórmula explícita para d_n e prove que sua fórmula funciona.

CAPÍTULO 4

Conjuntos

Todos os conceitos básicos em matemática podem ser colocados em termos de conjuntos. Quando contamos, estamos contando o número de elementos em um conjunto; quando analisamos a forma de uma figura, estamos analisando um conjunto de pontos; quando olhamos para uma função, vemos uma relação entre dois conjuntos. Conjuntos proporcionam a estrutura para o discurso matemático; eles são os blocos fundamentais para todos os conceitos quantitativos e espaciais.

Toscamente falando, um **conjunto** é uma coleção de objetos. Os objetos são chamados os membros ou **elementos** do conjunto. Em geral, letras maiúsculas são usadas para denotar conjuntos, e letras minúsculas para denotar elementos. Se o objeto x é um elemento do conjunto A, escrevemos $x \in A$; se não, isto é, se $\sim (x \in A)$, escrevemos $x \notin A$.

Conjuntos podem ser descritos em palavras, tais como "o conjunto de todos os inteiros pares", ou você pode definir um conjunto listando seus elementos entre chaves, como em $\{1,3,5,7,9\}$. A ordem dos elementos na lista é irrelevante; assim, $\{1,2,3\}$, $\{1,3,2,2\}$ e $\{2,3,1\}$ representam o mesmo conjunto. De fato, um conjunto é completamente determinado por seus elementos, de forma que:

Definição 4.0.5. *Dois conjuntos são iguais se, e somente se, possuem os mesmos elementos.*

Mas o modo mais conveniente para expressar um conjunto é especificar uma propriedade que determina os membros do conjunto. A propriedade é estabelecida em termos de uma sentença aberta a qual todos os elementos do conjunto devem satisfazer. Escrevemos então $\{x : P(x)\}$, onde $P(x)$ expressa o critério para ser membro do conjunto. Por exemplo,

$$A = \{n \in \mathbb{Z} : n = 2k, k \in \mathbb{Z}\}.$$

Definição 4.0.6. *O conjunto sem elementos será chamado o* ***conjunto vazio****, e é denotado por* $\emptyset$*.*

Definição 4.0.7. *Sejam A e B conjuntos. Dizemos que A é um* ***subconjunto*** *de B se, e somente se, cada elemento de A é também um elemento de B. Em símbolos,*

$$(A \subset B) \Leftrightarrow \forall x, (x \in A \Rightarrow x \in B).$$

Neste caso, dizemos que A está **contido** em B. Note que A é sempre um subconjunto dele mesmo, ou seja, $A \subset A$. Contudo, um subconjunto pode ser estritamente "menor", como por exemplo, $\{1,2\} \subset \{1,2,3\}$. Dizemos que o conjunto A é um **subconjunto próprio** de B se $A \subset B$ e $A \neq B$.

Teorema 4.0.8. *Para qualquer conjunto A temos que $\emptyset \subset A$.*

Demonstração. Seja A um conjunto qualquer. Desde que a implicação $x \in \emptyset \Rightarrow x \in A$ é sempre verdadeira, pois o antecedente é falso, segue que $\emptyset \subset A$. □

Teorema 4.0.9. *Sejam A e B conjuntos. Então $A = B$ se, e somente se, $A \subset B$ e $B \subset A$.*

Demonstração. Tente verificar este teorema! □

Exemplo 4.0.10. *Sejam $P = \{x \in \mathbb{R} : x^2 - 5x + 6 < 0\}$ e $Q = \{x \in \mathbb{R} : 2 < x < 3\}$. Mostremos que $P = Q$. Primeiro mostramos que $P \subset Q$. Seja $y \in P$. Então $y^2 - 5y + 6 < 0$. Assim, $(y-2)(y-3) < 0$. Temos então dois casos possíveis: (i) $y-2 < 0$ e $y-3 > 0$ ou (ii) $y-2 > 0$ e $y-3 < 0$. No caso (i) obtemos que $y < 2$ e $y > 3$, mas isto é impossível para um número real. Resta então o caso (ii) em que $y > 2$ e $y < 3$. Ou seja, $2 < y < 3$, donde $y \in Q$.*

Agora mostremos que $Q \subset P$. Seja $z \in Q$. Então $2 < z < 3$ e daí $y-2 > 0$ e $y-3 < 0$. Logo, $(y-2)(y-3) < 0$ e, consequentemente, $z^2 - 5z + 6 < 0$. Portanto, $z \in P$.

Para provar uma afirmação da forma $A \not\subset B$, necessitamos encontrar algum elemento $a \in A$ tal que $a \notin B$, um fato que parece intuitivamente claro e que pode ser visto formalmente como segue. A afirmação $A \subset B$ pode ser escrita como $\forall x, (x \in A \Rightarrow x \in B)$. Então $A \not\subset B$ é a negação da expressão anterior que é equivalente a $\exists x, [(x \in A) \wedge (x \notin B)]$.

É importante distinguir a noção de um objeto ser um elemento de um conjunto e a noção de um conjunto ser um subconjunto de outro conjunto. Por exemplo, seja $A = \{a, b, c\}$. Então $a \in A$ e $\{a\} \subset A$ são verdadeiros, enquanto que as afirmações $a \subset A$ e $\{a\} \in A$ são falsas. Também, observe que um conjunto pode ser um elemento de um outro conjunto. Seja $B = \{\{a\}, b, c\}$. Note que B é diferente do conjunto A. Então $\{a\} \in B$ e $\{\{a\}\} \subset B$ são verdadeiros, mas $a \in B$ e $\{a\} \subset B$ são falsas.

Definição 4.0.11. *Seja A um conjunto. O conjunto* ***potência*** *(ou o conjunto das partes) de A é o conjunto cujos elementos são todos os subconjuntos de A e é denotado por $\mathscr{P}(A)$. Ou seja, $\mathscr{P}(A) = \{X : X \subset A\}$.*

Exemplo 4.0.12. *(1) Desde que $\emptyset \subset \emptyset$, segue que $\mathscr{P}(\emptyset) = \{\emptyset\}$. Em particular, $\mathscr{P}(\emptyset) \neq \emptyset$.*

(2) Considere o conjunto $S = \{0, 1\}$. Então $\mathscr{P}(S) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$. Note que $\{1\} \subset S$, $\{1\} \in \mathscr{P}(S)$, $\emptyset \in \mathscr{P}(S)$ e $\{\emptyset\} \subset \mathscr{P}(S)$.

Teorema 4.0.13. *Se A é um conjunto com n elementos, então $\mathscr{P}(A)$ é um conjunto com 2^n elementos.*

Demonstração. Já provado. □

Teorema 4.0.14. *Sejam A e B conjuntos. Então $A \subset B$ se, e somente se, $\mathscr{P}(A) \subset \mathscr{P}(B)$.*

Demonstração. Suponha inicialmente que $A \subset B$ e tome $X \in \mathscr{P}(A)$. Então $X \subset A$ e assim $X \subset B$. Logo, $X \in \mathscr{P}(B)$ e $\mathscr{P}(A) \subset \mathscr{P}(B)$.

Reciprocamente, seja $\mathscr{P}(A) \subset \mathscr{P}(B)$ e considere o fato que $A \subset A$. Então $A \in \mathscr{P}(A)$ e daí $A \in \mathscr{P}(B)$. Consequentemente, $A \subset B$. □

Existem alguns modos de produzir novos conjuntos a partir de conjuntos dados.

Definição 4.0.15. *Sejam A e B conjuntos. A **união** de A e B é definida por*

$$A \cup B = \{x : x \in A \text{ ou } x \in B\}.$$

*A **interseção** de A e B é definida como sendo o conjunto*

$$A \cap B = \{x : x \in A \text{ e } x \in B\}.$$

*A **diferença** entre A e B é definida por*

$$A - B = \{x : x \in A \text{ e } x \notin B\}.$$

Observação 4.0.16. *Como auxílio na visualização de operações de conjuntos, introduzimos diagramas de Venn, que podem ser úteis para convencer você da verdade intuitiva de várias proposições relativamente a conjuntos. Alerto que um diagrama de Venn não substitui uma prova.*

Exemplo 4.0.17. *Para os intervalos $A = [1,4)$ e $B = (2,6]$ temos $A \cup B = [1,6]$, $A \cap B = (2,4)$ e $A - B = [1,2]$. Além disso, $[1,2] \cap (2,4) = \emptyset$.*

Observação 4.0.18. *(i) No caso em que $A \cap B = \emptyset$, dizemos que os conjuntos A e B são **disjuntos**.*

(ii) Segue da definição acima que

$$\begin{aligned} &x \notin A \cup B \Rightarrow x \notin A \text{ e } x \notin B; \\ &x \notin A \cap B \Rightarrow x \notin A \text{ ou } x \notin B; \\ &x \notin A - B \Rightarrow x \notin A \text{ ou } x \in B. \end{aligned}$$

Existem uma porção de regras envolvendo conjuntos cujas provas recaem nas definições. Por exemplo, se A, B e C são conjuntos, então

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

Verificamos este fato da seguinte forma:

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow x \in A \text{ e } x \in B \cup C \\ &\Leftrightarrow x \in A \text{ e } (x \in B \text{ ou } x \in C) \\ &\Leftrightarrow (x \in A \text{ e } x \in B) \text{ ou } (x \in A \text{ e } x \in C) \\ &\Leftrightarrow x \in A \cap B \text{ ou } x \in A \cap C \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

O universo de discurso é uma coleção de objetos entendido do contexto ou especificado no problema, no qual todos os objetos sob consideração devem pertencer.

Definição 4.0.19. *Se $\mathscr{U}$ é o universo de discurso e $A \subset \mathscr{U}$, então definimos o* ***complemento*** *de A como sendo o conjunto $A^c = \mathscr{U} - A$.*

Teorema 4.0.20. *Seja $\mathscr{U}$ o universo de discurso e sejam $A, B \subset \mathscr{U}$. Então:*

(a) $(A^c)^c = A$;

(b) $A - B = A \cap B^c$;

(c) $(A \cup B)^c = A^c \cap B^c$;

(d) $(A \cap B)^c = A^c \cup B^c$.

Demonstração. Mostraremos o item (c) somente (a verificação dos demais fica como exercício). Temos que:

$$\begin{aligned} x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \\ &\Leftrightarrow x \notin A \text{ e } x \notin B \\ &\Leftrightarrow x \in A^c \text{ e } x \in B^c \\ &\Leftrightarrow x \in A^c \cap B^c. \end{aligned}$$

□

Até aqui trabalhamos com uniões e interseções de somente dois conjuntos. Agora aplicaremos essas operações para mais que dois conjuntos. Seja I um conjunto. Uma coleção de conjuntos indexados por I é uma coleção de conjuntos S_i, para cada $i \in I$.

Exemplo 4.0.21. *Seja $I = \{1,2,3,4\}$. Uma coleção de conjuntos indexados por I consiste de quatro conjuntos S_1, S_2, S_3 e S_4. Por exemplo,*

$$S_1 = \emptyset, \quad S_2 = \{a,b,c\}, \quad S_3 = \mathbb{Z} \quad e \quad S_4 = \{\pi, \ln(543), \sqrt{2}\}.$$

Exemplo 4.0.22. *Seja $I = \mathbb{N}$. Uma coleção de conjuntos indexados por I é uma coleção infinita de conjuntos $S_1, S_2, S_3, \cdots$. Por exemplo,*

$$S_1 = (0,1), \quad S_2 = (0, \frac{1}{2}), \quad S_3 = (0, \frac{1}{3}), \quad \cdots, \quad S_n = (0, \frac{1}{n}), \quad \cdots.$$

Exemplo 4.0.23. *Seja $I = \mathbb{R}$. Uma coleção de conjuntos indexados por I é dada por $S_x = \{-x, x\}$. Neste caso não podemos listar numa ordem os elementos dessa coleção (veremos adiante que o conjunto dos números reais é não-enumerável). Alguns exemplos são $S_{\sqrt{2}} = \{-\sqrt{2}, \sqrt{2}\}$ e $S_{102} = \{-102, 102\}$.*

Definição 4.0.24. *Seja I um conjunto e seja $\{S_i\}_{i \in I}$ uma coleção de conjuntos indexados por I.*

(a) a ***união*** *dos S_i é o conjunto $\bigcup_{i \in I} = \{x : x \in S_i, \text{ para algum } i \in I\}$.*

(b) a ***interseção*** *dos S_i é o conjunto* $\bigcap_{i\in I} = \{x : x \in S_i, \text{ para todo } i \in I\}$.

Exemplo 4.0.25. *No segundo exemplo acima, temos que*

$$\bigcup_{n=1}^{\infty} S_n = \bigcup_{n=1}^{\infty} (0, \frac{1}{n}) = (0,1) \quad e \quad \bigcap_{n=1}^{\infty} S_n = \bigcap_{n=1}^{\infty} (0, \frac{1}{n}) = \emptyset.$$

Para verificarmos a interseção, suponhamos que exista um $x \in \bigcap_{n=1}^{\infty} S_n$. Em particular, $x \in S_1 = (0,1)$. Mas para n suficientemente grande temos que $\frac{1}{n} < x$, donde $x \notin (0, \frac{1}{n}) = S_n$. Isto contradiz o fato que $x \in \bigcap_{n=1}^{\infty} S_n$.

Exemplo 4.0.26. *Prove que* $\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right) = \{0\}$

É possível generalizar algumas propriedades vistas anteriormente.

Teorema 4.0.27. *Seja $\mathscr{A} = \{\mathscr{A}_\alpha : \alpha \in I\}$ uma família indexada de conjuntos e B um conjunto. Então:*

(1) $B \cup (\cap_{\alpha\in I} \mathscr{A}_\alpha) = \cap_{\alpha\in I}(B \cup \mathscr{A}_\alpha)$.

(2) $B \cap (\cup_{\alpha\in I} \mathscr{A}_\alpha) = \cup_{\alpha\in I}(B \cap \mathscr{A}_\alpha)$.

(3) $[\cup_{\alpha\in I} \mathscr{A}_\alpha]^c = \cap_{\alpha\in I} \mathscr{A}_\alpha^c$.

(4) $[\cap_{\alpha\in I} \mathscr{A}_\alpha]^c = \cup_{\alpha\in I} \mathscr{A}_\alpha^c$.

Existe um outro modo fundamental de formar novos conjuntos a partir de antigos. Para isso necessitaremos da noção de **par ordenado** de elementos, denotado por (a,b), onde a e b são elementos de conjuntos dados. Num sentido formal, definimos o par ordenado (a,b) como sendo o conjunto $\{\{a\},\{a,b\}\}$. Desta forma, diferentemente do que ocorre com conjuntos, a ordem dos elementos num par ordenado é relevante, ou seja, $(a,b) \neq (b,a)$. Além disso, segue de nossa definição que dois pares ordenados (a,b) e (c,d) são iguais se, e somente se, $a = c$ e $b = d$. Verifique essas afirmações.

Definição 4.0.28. *Sejam A e B conjuntos. O produto de A e B, denotado por $A \times B$. é o conjunto*

$$A \times B = \{(a,b) : a \in A \text{ e } b \in B\},$$

onde (a,b) denota um par ordenado.

Exemplo 4.0.29. *Sejam $A = \{a,b,c\}$ e $B = \{1,2\}$. Então*

$$A \times B = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}.$$

Observação 4.0.30. *Note que nos novos conjuntos $A \cup B$, $A \cap B$ e $A - B$ formados a partir dos conjuntos A e B, os objetos continuam sendo da mesma espécie, ou sejam continuam no universo de discurso. Contudo, isto não acontece com produto $A \times B$, pois seus elementos constituintes deixam de estar no universo de discurso.*

Ora, se o conjunto A tem n elementos e o conjunto B tem m elementos, quantos elementos tem o conjunto $A \times B$?

Podemos formar o produto de mais que dois conjuntos, porém nesse caso há uma sutileza técnica. Suponha que queremos forma o produto dos conjuntos A, B e C. Mantendo esses conjuntos numa dada ordem, poderíamos formar o produto de duas maneiras, fornecendo os conjuntos $A \times (B \times C)$ e $(A \times B) \times C$. Estritamente falando, esses conjuntos não são os mesmos, pois seus elementos são $(a,(b,c))$ e $((a,b),c)$, respectivamente, os quais são distintos. Encobriremos essa dificuldade técnica, simplesmente referindo-se ao conjunto $A \times B \times C$ como sendo o conjunto formado pelas triplas (a,b,c).

O seguinte teorema fornece algumas propriedades padrões de produtos de conjuntos.

Teorema 4.0.31. *Sejam A, B, C e D conjuntos.*

(1) Se $A \subset B$ e $C \subset D$, então $A \times C \subset B \times D$.

(2) $A \times (B \cup C) = (A \times B) \cup (A \times C)$ e $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(3) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

Demonstração. Provaremos somente $A \times (B \cap C) = (A \times B) \cap (A \times C)$. As demais afirmações são mostradas de forma análoga. □

4.1 Uma pausa para o rigor

Neste momento muitos de nós achamos que entendemos o significado de conjunto - pelo menos intuitivamente, e não percebemos o que há de errado em considerar que para cada sentença aberta $P(x)$ corresponde um conjunto $\{x : P(x)\}$. Foi o famoso filósofo inglês Bertrand Russel (1872-1970) que chamou a comunidade matemática em 1902, declarando que a admissão de um conjunto de todos os conjuntos (o "conjunto universal") levaria a uma contradição. Este é o famoso "Paradoxo de Russel". Suponha que poderíamos formar o conjunto de todos os conjuntos; denote por S esse conjunto. Observe que $S \in S$. Então defina o conjunto $T = \{A \in S : A \notin A\}$. É T um membro de si mesmo? Suponha primeiro que $T \notin T$. Então $T \in T$. Agora suponha que $T \in T$. Então $T \notin T$. Existe algo de errado aqui. O problema é que estamos tentando usar um conjunto de todos os conjuntos.

Para tratar teoria de conjuntos rigorosamente desenvolveu-se vários sistemas axiomáticos, evitando assim paradoxos como o de Russel. O mais utilizado é referido como Axiomas de Zarmelo-Fraenkel. Os axiomas são formulados no contexto de lógica simbólica e são listados abaixo, de modo informal.

Axioma de Extensão Sejam x e y conjuntos. Se x e y tem os mesmos elementos, então $x = y$.

Axioma do Conjunto Vazio Existe um conjunto z tal que $x \notin z$ para todo conjunto x.

Axioma de Paridade Sejam x e y conjuntos. Existe um conjunto z tal que $w \in z$ se, e somente se, $w = x$ ou $w = y$.

Axioma de União Seja x um conjunto. Existe um conjunto z tal que $w \in z$ se, e somente se, existe algum conjunto $y \in x$ tal que $w \in y$.

Axioma do Conjunto Potência Seja x um conjunto. Existe um conjunto z tal que $w \in z$ se, e somente se, $w \subset x$.

Axioma de Regularidade Seja x um conjunto. Suponha que $x \neq \emptyset$. Então existe algum $y \in x$ tal que $x \cap y = \emptyset$.

Axioma de Seleção Seja $P(t)$ uma propriedade lógica de conjuntos com uma variável livre t que pode ser formulada no contexto dos axiomas de Zarmelo-Fraenkel. Seja x um conjunto. Então existe um conjunto z tal que $y \in z$ se, e somente se, $y \in x$ e $P(y)$ é verdade.

Axioma de Infinidade Existe um conjunto z tal que $\emptyset \in z$ e se $x \in z$, então $x \cup \{x\} inz$.

Axioma de Deslocamento Seja $F(s,t)$ uma propriedade funcional de conjuntos com duas variáveis livres que pode ser formulada no contexto dos axiomas de Zarmelo-Fraenkel. Seja x um conjunto. Então existe um conjunto z tal que $y \in z$ se, e somente se, existe algum $w \in x$ tal que $F(w,y)$ é verdade.

Em adição aos axiomas de Zarmelo-Fraenkel, trabalha-se em teoria de conjuntos com o **Axioma da Escolha** que, intuitivamente, estabelece que se temos uma família de conjuntos não-vazios, podemos simultaneamente escolher um elemento da cada um dos conjuntos. Para uma família finita de conjuntos não-vazios, podemos escolher um elemento do primeiro conjunto, e então um elemento do segundo conjunto, e assim por diante, não havendo problema em fazer tais escolhas. O problema começa quando temos uma família infinita de conjuntos (particularmente uma família não-enumerável - a ser definida na aula sobre cardinalidade). Nesse caso, não podemos escolher um elemento de cada vez - a escolha deve ser simultânea.

Terceira Lista de Exercícios

1. Quais das seguintes afirmações são verdadeiras e quais são falsas?

   (a) $10 \notin (-\infty, \pi^2)$;

   (b) $\pi \in (2, \infty)$;

   (c) $-1,3 \in \{\cdots, -3, -2, -1\}$;

   (d) $[1,2] \subset \{0,1,2,3\}$;

   (e) $\{-1,0,1\} \subset [-1,1]$;

   (f) $\{\emptyset\} \subset A$ para todo conjunto A;

(g) $\emptyset \subset \mathscr{P}(A)$ para todo conjunto A;

(h) $\mathscr{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

2. Escreva cada um dos conjuntos na forma de uma sentença aberta.

   (a) O conjunto de todos os números reais positivos;

   (b) O conjunto de todos os inteiros ímpares;

   (c) O conjunto de todos os números racionais que tem fator 5 em seu denominador;

   (d) O conjunto $\{-64, -27, -8, -1, 0, 1, 8, 27, 64\}$.

3. Entre os seguintes subconjuntos, quem é subconjunto de quem?

   M é o conjunto de todos os homens; **W** é o conjunto de todas as mulheres; **P** é o conjunto de todos os parentes; **O** é o conjunto de todas as mães; **F** é o conjunto de todos os pais; **U** é o conjunto de todos os tios; **A** é o conjunto de todas as tias; e **C** é o conjunto de todas as pessoas que filhos de outras pessoas.

4. Entre os seguintes subconjuntos, quem é subconjunto de quem?

   $C = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k^4\}$;

   $E = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = 2k\}$;

   $P = \{n \in \mathbb{Z} : n \text{ é um número primo}\}$;

   $N = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k^8\}$;

   $S = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = 6k\}$;

   $D = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = k - 5\}$;

   $B = \{n \in \mathbb{Z} : n \text{ é não negativo}\}$.

5. Encontre conjuntos A e B tais que $A \in B$ e $A \subset B$.

6. Liste todos os elementos do conjunto $\mathscr{P}(\mathscr{P}(\emptyset))$

7. Sejam $x = [0,5)$, $Y = [2,4]$, $Z = (1,3]$ e $W = (3,5)$ intervalor em $\mathbb{R}$. Encontre cada um dos seguintes conjuntos: $Y \cup Z$, $Z \cap W$, $Y - W$, $X \times W$, $(X \cap Y) \cup Z$ e $X - (Z \cup W)$.

8. Sejam $G = \{n \in \mathbb{Z} : n = 2m \text{ para algum } m \in \mathbb{Z}\}$, $H = \{n \in \mathbb{Z} : n = 3k \text{ para algum } k \in \mathbb{Z}\}$, $I = \{n \in \mathbb{Z} : n^2 \text{ é ímpar}\}$ e $J = \{n \in \mathbb{Z} : 0 \leq n \leq 10\}$. Encontre cada um dos seguinte conjuntos: $G \cup I$, $G \cap I$, $G \cap H$, $J - G$, $I - H$ e $J \cap (G - H)$.

9. Dados dois conjuntos A e B, são os conjuntos $A - B$ e $B - A$ necessariamente disjuntos? De uma prova ou um contraexemplo.

10. Sejam A e B dois conjuntos. Prove que $(A \cup B) - A = B - (A \cap B)$.

11. Sejam A, B e C conjuntos. Prove que

$$(A-B)\cap C = (A\cap C) - B = (A\cap C) - (B\cap C).$$

12. Sejam A e B conjuntos. A **diferença simétrica** de A e B, denotada por $A \triangle B$, é o conjunto $A \triangle B = \{(A-B)\cup(B-A)\}$. Sejam X, Y e Z conjuntos. Prove as seguinte afirmações:

    (a) $X \triangle \emptyset = X$;

    (b) $X \triangle X = \emptyset$;

    (c) $X \triangle Y = Y \triangle X$;

    (d) $X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z$;

    (e) $X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z)$;

    (f) $X \triangle Y = (X \cup Y) - (X \cap Y)$.

13. Prove ou encontre um contraexemplo para a seguinte afirmação. Sejam A, B e C conjuntos. Então $(A\cup C) - B = (A-B)\cup(C-B)$.

14. Prove ou dê um contraexemplo para cada uma das seguintes afirmações:

    (a) Sejam A e B conjuntos. Então $\mathscr{P}(A\cup B) = \mathscr{P}(A)\cup\mathscr{P}(B)$.

    (b) Sejam A e B conjuntos. Então $\mathscr{P}(A\cap B) = \mathscr{P}(A)\cap\mathscr{P}(B)$.

15. Em cada uma das seguintes partes, é dado um conjunto B_k para cada $k \in \mathbb{N}$. Encontre $\bigcup_{k\in\mathbb{N}} B_k$ e $\bigcap_{k\in\mathbb{N}} B_k$.

    (a) $B_k = \{0, 1, 2, 3, \cdots, k\}$;

    (b) $B_k = \{k-1, k, k+1\}$;

    (c) $B_k = \{\frac{3}{k}, \frac{5k+2}{k}\} \cup \{10+k\}$;

    (d) $B_k = \{[-1, 3+\frac{1}{k}] \cup [5, \frac{5k+1}{k})\}$.

16. Em cada uma das seguintes partes, voce necessita encontrar uma família de conjuntos $\{E_k\}_{k\in\mathbb{N}}$ tal que $E_k \subset \mathbb{R}$ para cada $k \in \mathbb{N}$, de forma que todos os E_k seja distintos e tornem as condiçoes dadas verdadeiras.

    (a) $\bigcup_{k\in\mathbb{N}} E_k = [0,\infty)$ e $\bigcap_{k\in\mathbb{N}} E_k = [0,1]$;

    (b) $\bigcup_{k\in\mathbb{N}} E_k = (0,\infty)$ e $\bigcap_{k\in\mathbb{N}} E_k = \emptyset$;

    (c) $\bigcup_{k\in\mathbb{N}} E_k = \mathbb{R}$ e $\bigcap_{k\in\mathbb{N}} E_k = \{3\}$;

    (d) $\bigcup_{k\in\mathbb{N}} E_k = (2,8)$ e $\bigcap_{k\in\mathbb{N}} E_k = [3,6]$.

CAPÍTULO 5

Relações

Definição 5.0.1. *Sejam A e B conjuntos. Uma* ***relação*** *R entre A e B é um subconjunto de $A \times B$. Assim, se $(a,b) \in R$, escrevemos aRb (ou $a \sim b$) para expressar que a e b estão relacionados.*

Exemplo 5.0.2. *(1) Sobre $\mathbb{Z}$ consideremos a relação $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x+y = 0\}$. Então $R = \{\cdots, (-1,1), (1,-1), (0,0), (2,-2), \cdots\}$.*

(2) Sobre o conjunto $\mathbb{N} \times \mathbb{N}$ considere a relação $(m,n)R(s,r)$ se, e somente se, $m+r = n+k$.

(3) Seja $E = \{(x,y) \in \mathbb{R} \times \mathbb{R} : \frac{x^2}{324} + \frac{y^2}{64} \leq 1\}$. O gráfico de E é dado por

(4) Outro tipo importante de gráfico que pode ser usado para representar uma relação R sobre um conjunto A é o gráfico dirigido ou dígrafo. Pensamos nos objetos de A como vértices e na relação R como lados dirigidos, conectando vértices relacionados. Por exemplo, a relação R sobre o conjunto $A = \{3,4,5,6,7,8\}$ dada por xRy se, e somente se, $x-y$ é par, pode ser representada como

(5) Um fluxograma também é uma relação. Por exemplo, usando o critério de pré-requisito construímos uma relação sobre o conjunto de disciplinas do DMA-UFS.

Veremos agora novas maneiras de construir novas relações a partir de relações dadas.

Definição 5.0.3. *Se R é uma relação entre os conjuntos A e B, então definimos a inversa de R, denotada por R^{-1}, como sendo a relação*

$$R^{-1} = \{(y,x) \in B \times A : (x,y) \in R\}.$$

Exemplo 5.0.4. *1. No caso do dígrafo acima, temos R^{-1} como sendo*

2. Seja R uma relação sobre o conjunto dos números reais $\mathbb{R}$ definida por xRy se, e somente se, $y = 2^x$.

Definição 5.0.5. *Seja R uma relação entre os conjuntos A e B e seja S uma relação entre os conjuntos B e C. A composição de R e S é definida como sendo o subconjunto de $A \times C$ dado por*

$$S \circ R = \{(a,c) \in A \times C : \exists b \in B \text{ tal que } (a,b) \in R \text{ e } (b,c) \in S\}.$$

Exemplo 5.0.6. *1. Consideremos os conjuntos $A = \{1,2,3,4\}$, $B = \{p,q,r,s\}$ e $C = \{x,y,z\}$. Seja $R = \{(1,p), (1,q), (2,q), (3,r), (4,s)\}$ uma relação entre A e B, e seja $S = \{(p,x), (q,x), (q,y), (s,z)\}$ uma relação entre B e C. Então*

$$S \circ R = \{(1,x), (1,y), (2,x), (2,y), (4,z)\}$$

.

2. *Se R é uma relação entre A e B e S é uma relação entre B e A, então nem sempre é verdade que $S \circ R = R \circ S$. Por exemplo, tome sobre $\mathbb{R} \times \mathbb{R}$ as seguintes relações*

$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : y = x+1\} \text{ e } S = \{(y,z) \in \mathbb{R} \times \mathbb{R} : z = y^2\}.$$

Então

$$\begin{aligned} R \circ S =& \{(y,x) \in \mathbb{R} \times \mathbb{R} : \exists z \in \mathbb{R} \text{ com } (y,z) \in S \text{ e } (z,x) \in R\} \\ =& \{(y,x) \in \mathbb{R} \times \mathbb{R} : \exists z \in \mathbb{R} \text{ com } z = y^2 \text{ e } x = z+1\} \\ =& \{(y,x) \in \mathbb{R} \times \mathbb{R} : x = y^2+1\}. \end{aligned}$$

Analogamente, verificamos que $S \circ R = \{(y,x) \in \mathbb{R} \times \mathbb{R} : x = (y+1)^2\}$.

Teorema 5.0.7. *Suponha A, B, C e D conjuntos. Sejam R uma relação entre A e B, S uma relação entre B e C, e T uma relação entre C e D. Então*

(i) $(R^{-1})^{-1} = R$;

(ii) $T \circ (S \circ R) = (T \circ S) \circ R$;

(iii) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Demonstração. São consequências diretas das definições. Mostraremos os itens (ii) e (iii). □

5.1 Relações de Equivalência

Uma relação R sobre um conjunto X é chamada **relação de equivalência** se as seguintes propriedades forem satisfeitas:

(1) Reflexividade: para todo $x \in X$, xRx;

(2) Simetria: para todo $x, y \in X$, se xRy então yRx;

(3) Transitividade: para todo $x, y, z \in X$, se xRy e yRz, então xRz.

Exemplo 5.1.1. *Seja n um inteiro positivo fixado. Então definimos sobre $\mathbb{Z}$ a seguinte relação: aRb se, e somente se, $a-b$ é um múltiplo de n, ou seja, $a-b = kn$ para algum $k \in \mathbb{Z}$. Esta relação é chamada* ***congruência módulo*** *n. Ao invés de escrever aRb, costuma-se denotar esta relação por $a \equiv b (mod n)$. Verifiquemos que esta é uma relação de equivalência.*

(1) Vale a reflexividade pois $a \equiv a (mod n)$ para todo $a \in \mathbb{Z}$ uma vez que $a - a = 0n$.

(2) Vale a simetria pois se $a \equiv b (mod n)$, então

$$b - a = -(a-b) = -(kn) = (-k)n,$$

o que implica, por definiçao da relação, que $b \equiv a (mod n)$.

(3) Vale a transitividade pois, para todo $a,b,c \in \mathbb{Z}$ tais que $a \equiv b(mod n)$ e $b \equiv c(mod n)$, temos que existem $k_1,k_2 \in \mathbb{Z}$ satisfazendo $a-b=k_1n$ e $b-c=k_2n$. Assim,

$$a-c=(a-b)+(b-c)=(k_1+k_2)n$$

e isto implica que $a \equiv c(mod n)$.

Exemplo 5.1.2. *Definimos uma relação sobre $\mathbb{Z}$ por: xRy se, e somente se, $x+3y$ é par. Verifiquemos que esta é uma relação de equivalência.*

(1) Vale a reflexividade pois para todo $x \in \mathbb{Z}$ temos que $x+3x=4x$ que é um número par.

(2) Vale a simetria pois se xRy, então $x+3y$ é par, ou seja, existe inteiro k tal que $x+3y=2k$. Consequentemente,

$$y+3x=y+2y-2y+x+2x=x+3y+2(x-y)=2(k+x-y)$$

nos diz que $y+3x$ é par. Ou seja, yRx.

(3) Vale a transitividade pois, para todo $x,y,z \in \mathbb{Z}$ tais que xRy e yRz, temos que existem $k_1,k_2 \in \mathbb{Z}$ satisfazendo $x+3y=2k_1$ e $y+3z=2k_2$. Assim,

$$x+3z=x+3y-3y+y-y+3z=(x+3y)+(y+3z)-4y=2(k_1+k_2-2y)$$

é par, e isto implica que xRz como queríamos mostrar.

Exemplo 5.1.3. *Definimos agora a relação sobre $\mathbb{R}$ por: xRy se, e somente se, $|x-y| \leq 1$. Verifiquemos que esta não é uma relação de equivalência.*

(1) Vale a reflexividade pois para todo $x \in \mathbb{R}$ temos que $|x-x|=0 \leq 1$.

(2) Vale a simetria pois se xRy, então $|x-y| \leq 1$. Assim, $|y-x|=|x-y| \leq 1$ implica que yRx.

(3) Não vale a propriedade transitiva pois, $5R4$ e $4R3$ porém $|5-3|=2>1$.

Definição 5.1.4. *Uma vez que temos uma relação de equivalência R sobre um conjunto X, definimos a **classe de equivalência** de um elemento $x \in X$, denotada por $[x]$, como sendo o subconjunto de todos os elementos em X que estão relacionados a x, isto é,*

$$[x]=\{y \in X : yRx\}.$$

*O conjunto de todas as classes de equivalência é chamado **conjunto quociente** e denotado por*

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

.

Exemplo 5.1.5. *No caso da relação de equivalência $x \equiv y(mod3)$ sobre $\mathbb{Z}$, temos que*

$$\begin{aligned}[x] &= \{y \in \mathbb{Z} : y \equiv x(mod3)\} \\ &= \{y \in \mathbb{Z} : y = 3k + x, \text{ para algum } k \in \mathbb{Z}\} \\ &= \{3k + x : x \in \mathbb{Z}\}.\end{aligned}$$

Assim, a classe de equivalência do elemento $x \in \mathbb{Z}$ é constituída pelos inteiros que ao serem divididos por 3 deixam resto x. Logo, há somente três classes distintas:

$$\begin{aligned}[0] &= \{0, \pm 3, \pm 6, \cdots\} \\ [1] &= \{1, 4, -2, 7, -5, \cdots\} \\ [2] &= \{2, 5, -1, 8, -4, \cdots\},\end{aligned}$$

correspondentes aos elementos que deixam restos $0, 1$ ou 2, respectivamente. Portanto,

$$Z/R = \{[0], [1], [2]\}.$$

Generalizando para um inteiro n fixado...

Exemplo 5.1.6. *A relação R definida sobre o conjunto dos números reais $\mathbb{R}$ por xRy se, e somente se, $x^2 = y^2$ é uma relação de equivalência (verifique!). As classes de equivalência têm a forma*

$$[x] = \{y \in \mathbb{R} : yRx\} = \{y \in \mathbb{R} : y^2 = x^2\} = \{-x, x\}.$$

Logo, $\mathbb{R}/R$ possui infinitas classes de equivalência. Por exemplo, $[\pi] = \{-\pi, \pi\}$ e $[\sqrt{2}] = \{-\sqrt{2}, \sqrt{2}\}$.

Sobre o conjunto quociente X/R podemos definir uma operação de adição e uma operação de multiplicação da seguinte forma:

$$[x] + [y] = [x + y] \quad \text{e} \quad [x] \cdot [y] = [xy].$$

Com estas operações podemos construir o conjunto dos inteiros a partir dos números naturais da seguinte forma: defina a relação de equivalência R sobre $\mathbb{N} \times \mathbb{N}$ por $(a, b)R(c, d)$ se, e somente se, $a + d = b + c$. Um bom exercício é verificar que, de fato, R é uma relação de equivalência. As classes de equivalência são então

$$\begin{aligned}[(x, y)] &= \{(a, b) \in \mathbb{N} \times \mathbb{N} : (a, b)R(x, y)\} \\ &= \{(a, b) \in \mathbb{N} \times \mathbb{N} : a + y = b + x\}.\end{aligned}$$

Ou seja, os elementos da classe $[(x, y)]$ são tais que "$a - b = x - y$". Por exemplo,

$$\begin{aligned}[(0, 2)] &= \{(0, 2), (1, 3), (2, 4), \cdots\} \\ [(0, 1)] &= \{(0, 1), (1, 2), (2, 3), \cdots\} \\ [(0, 0)] &= \{(0, 0), (1, 1), (2, 2), \cdots\} \\ [(1, 0)] &= \{(1, 0), (2, 1), (3, 2), \cdots\}\end{aligned}$$

Rotulando $-2 = [(0,2)]$, $-1 = [(0,1)]$, $0 = [(0,0)]$, $1 = [(1,0)]$, e assim por diante, verificamos que

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{R}.$$

Agora, subtração e multiplicação envolvendo números negativos ficam bem definidas. Por exemplo,

$$\begin{aligned} 1-2 &= [(1,0)] + [(0,2)] = [(1,0)+(0,2)] = [(1,2)] = -1; \\ (-1)\cdot(-2) &= [(0,1)] \cdot [(0,2)] = [(0,1)\cdot(0,2)] = [(2,0)] = 2, \end{aligned}$$

onde usamos o produto $(x,y)\cdot(u,v) = (xu+yv, xv+yu)$ em $\mathbb{N}\times\mathbb{N}$.

Teorema 5.1.7. *Suponha que R á uma relação de equivalência sobre um conjunto X. Então:*

(1) $X = \bigcup_{x\in X}[x]$;

(2) xRy *se, e somente se,* $[x] = [y]$;

(3) quaisquer duas classes são ou disjuntas ou idênticas.

Demonstração. (1) Seja $y \in X$. Desde que yRy, por reflexividade, segue que $x \in [x]$ e daí $x \in \bigcup[x]$. Reciprocamente, como cada $[x] \subset X$, temos que $\bigcup_{x\in X}[x] \subset X$.

(2) Suponha que xRy. Temos uma igualdade de conjuntos a ser mostrada. Seja $w \in [x]$. Então wRx e, por transitividade, wRy. Assim, $w \in [y]$. Por outro lado, se $z \in [y]$, então zRy e, por simetria, temos que yRx. Logo, usando a transitividade, concluímos que zRx. Ou seja, $z \in [x]$. Reciprocamente, suponha agora que $[x] = [y]$. Desde de que $x \in [x]$ sempre, segue que $x \in [y]$. Portanto, xRy.

(3) Sejam $[x]$ e $[y]$ classes de equivalência. Se elas são disjuntas, não há mais o que fazer. Suponha então que $[x] \cap [y] \neq \emptyset$ e tome $z \in [x] \cap [y]$. Assim, por definição de classe, zRx e zRy. Usando as propriedades simétrica e transitividade verificamos que xRy e, conforme o provado no item (2), concluímos que $[x] = [y]$. □

Dessa maneira uma relação de equivalência particiona o conjunto em subconjuntos (classes) disjuntos. Será que se tivermos um modo de dividir um conjunto então podemos obter uma relação de equivalência?

Definição 5.1.8. *Seja X um conjunto não-vazio e seja I um conjunto de índices. Uma* ***partição*** *é uma coleção de subconjuntos $\{A_\alpha\}_{\alpha\in I}$ de X tal que:*

(1) Para cada $\alpha \in I$, o conjunto $A_\alpha \neq \emptyset$;

(2) $X = \bigcup_{\alpha\in I} A_\alpha$;

(3) Para todos $\alpha, \beta \in I$, se $A_\alpha \cap A_\beta \neq \emptyset$, então $A_\alpha = A_\beta$.

Exemplo 5.1.9. *A família de intervalos $A_n = [n, n+1)$, com $n \in \mathbb{Z}$, particiona o conjunto $\mathbb{R}$. De fato, cada $A_n \neq \emptyset$, $\mathbb{R} = \bigcup_{n\in\mathbb{Z}} A_n$ e se $A_n \cap A_m \neq \emptyset$, como os intervalos $[n, n+1)$ e $[m, m+1)$ são ou iguais ou disjuntos, segue que $A_n = A_m$.*

Teorema 5.1.10. *Seja $\{A_\alpha\}_{\alpha\in I}$ uma partição do conjunto X. Para $x,y\in X$ defina xRy se, e somente se, existe A_α tal que $x,y\in A_\alpha$. Então R é uma relação de equivalência sobre X e $X/R=\{A_\alpha:\alpha\in I\}$.*

Demonstração. Desde que $X=\bigcup_{\alpha\in I}A_\alpha$, segue que para todo $x\in X$ temos $x\in A_\alpha$, para algum $\alpha\in I$. Logo xRx para todo $x\in X$ (mostrando que vale a reflexividade). Obviamente, se xRy, ou seja, $x,y\in A_\alpha$ para algum $\alpha\in I$, então $y,x\in A_\alpha$ e isto implica que yRx (simetria). Agora, supondo que xRy e yRx, temos pela definição da relação, que existem $\alpha,\beta\in I$ tais que $x,y\in A_\alpha$ e $y,z\in A_\beta$. Desde que $y\in A_\alpha\cap A_\beta$, segue por hipótese que $A_\alpha=A_\beta$. Logo $x,z\in A_\alpha$ e daí xRz (mostrando a transitividade). Portanto, R é uma relação de equivalência.

Primeiro mostremos que $X/R\subset\{A_\alpha:\alpha\in I\}$. Seja $[x]\in X/R$. Desde que $\{A_\alpha\}_{\alpha\in I}$ é uma partição de X, $x\in A_\alpha$ para algum $\alpha\in I$. Afirmamos que $[x]=A_\alpha$. De fato, se $y\in[x]$ então yRx, e por definição da relação, $x,y\in A_\alpha$. Ou seja, $[x]\subset A_\alpha$. Por outro lado, se $z\in A_\alpha$ então $x,z\in A_\alpha$ e daí zRx. Logo, $z\in[x]$. Portanto, $[x]=A_\alpha$. Por fim, para mostrarmos que $\{A_\alpha\}_{\alpha\in I}\subset X/R$, tomemos $A_\beta\in\{A_\alpha\}_{\alpha\in I}$. Como $A_\beta\neq\emptyset$, podemos tomar $w\in A_\beta$. Afirmamos que $A_\beta=[w]$. A prova é análoga a anterior. □

5.2 Relação de Ordem

Há algumas relações que permitem impor uma ordem sobre os conjuntos, tal que podemos falar em alguns elementos serem "menor ou igual"que outros. Por exemplo, os sistemas numéricos têm uma ordem particular denotada por $\leq$. Neste caso temos, por exemplo, $3\leq 3$ e de $x\leq 5$ e $5\leq y$ podemos concluir que $x\leq y$. Sobre o conjunto potência $\mathscr{P}(X)$ de um dado conjunto X temos uma ordem dada por $\subset$ (inclusão). Mas o que é uma relação de ordem?

Definição 5.2.1. *Uma relação R sobre um conjunto X é dita uma* ***relação de ordem parcial*** *se ela é reflexiva, anti-simétrica e transitiva, onde anti-simetria significa que para todos $x,y\in X$ tais que xRy e yRx temos que $x=y$. O conjunto X é dito parcialmente ordenado.*

Exemplo 5.2.2. *Para o conjunto dos números naturais $\mathbb{N}$, a relação R definida por aRb se, e somente se, a divide b, é uma relação de ordem. Com efeito, a propriedade reflexiva é válida, pois para todo número natural $n\in\mathbb{N}$ temos que $n=n\cdot 1$, donde n divide n. A relação R também é anti-simétrica, pois se aRb e bRa então existem naturais m e n tais que $b=am$ e $a=bn$. Assim, $a=(am)n=a(mn)$. Mas isto somente é possível se $mn=1$, donde concluímos que $m=n=1$. Portanto, $a=b$. Por fim, verificamos que a propriedade transitiva também é válida. De fato, se aRb e bRc, então existem naturais m e n tais que $b=am$ e $c=bn$. Assim, $c=(am)n=a(mn)=ak$. Portanto, a divide c e isto implica que aRc.*

Exemplo 5.2.3. *Verifique que as relações $(\mathbb{R},\leq)$ e $(\mathscr{P}(X),\subset)$ são relações de ordem parciais.*

Definição 5.2.4. *Uma relação de ordem parcial R sobre um conjunto X é dita* ***relação de ordem total*** *(ou linear) se para quaisquer dois elementos $x,y\in X$ temos xRy ou yRx.*

Em outras palavras, numa relação de ordem total quaisquer dois elementos do conjunto X podem ser comparados. Por exemplo, a relação $(\mathbb{R},\leq)$ é de ordem total, enquanto a relação

$(\mathbb{N}, R)$, onde R é a relação do primeiro exemplo, não é de ordem total (note, por exemplo, que o par $(3,5) \in \mathbb{N} \times \mathbb{N}$ é tal que "3 não divide 5" e "5 não divide 3".

Definição 5.2.5. *Seja R uma relação de ordem parcial sobre um conjunto X e sejam $x, y \in X$, com $x \neq y$. Então x é dito um* ***predecessor imediato*** *de y se xRy e não existe $z \in X$ tal que $x \neq z$, $y \neq z$, xRz e zRy.*

Exemplo 5.2.6. *Para $X = \{1,2,3,4,5\}$, a ordem parcial $\subset$ sobre o conjunto potência $\mathscr{P}(X)$ implica que para o elemento $A = \{2,3,5\}$ existem três predecessores imediatos $\{2,3\}, \{2,5\}$ e $\{3,5\}$. Note que $\emptyset \in \mathscr{P}(X)$ não tem prdecessor imediato. Qual é o predecessor do conjunto $\{4\}$?*

Definição 5.2.7. *Seja R uma relação parcial sobre um conjunto X e seja A qualquer subconjunto de X. Então $x \in X$ é uma* ***cota superior*** *para A se, para cada $a \in A$, temos aRx. Dizemos que $x \in X$ é o* ***supremo*** *de A se x é a menor cota superior de A, isto é, xRy para toda cota superior y de A. Escrevemos $x = sup(A)$. Analogamente, definimos uma* ***cota inferior*** *para A como sendo $w \in X$ tal que wRa, para todo $a \in A$. Dizemos que $x \in X$ é o* ***ínfimo*** *de A se w é a maior cota inferior para A, ou seja, zRw para cada cota inferior z de A. Escrevemos $w = inf(A)$.*

Quarta Lista de Exercícios

1. Sejam $x, y \in \mathbb{R}$. Trace o gráfico da relação R. Encontre o domínio e a imagem de R.
   (a) $R = \{(x,y) : x^2 + y^2 \leq 1\}$;
   (b) $R = \{(x,y) : x = y^3\}$;
   (c) $R = \{(x,y) : 1 \leq x \leq 3 \text{ e } y = 3x - 5\}$.
2. Encontre a inversa das seguintes relações:
   (a) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} = 7x - 10\}$;
   (b) $S = \{(x,y) \in \mathbb{R} \times \mathbb{R} : y = x^2 + 2\}$.
3. Seja $R = \{(1,5),(2,2),(3,4),(5,2)\}$, $S = \{(2,4),(3,4),(3,1),(5,5)\}$ e $T = \{(1,4),(3,5),(4,1)\}$. Encontre
   (a) $R \circ (S \circ T)$;
   (b) $(R \circ S) \circ T$.
4. Seja $A = \{a,b,c,d\}$. Dê um exemplo de relações R e S sobre A tais que:
   (a) $R \circ S \neq S \circ R$;
   (b) $(S \circ R)^{-1} \neq S^{-1} \circ R^{-1}$.
5. Para cada um dos itens abaixo, verifique que a relação é de equivalência. Então forneça a informação solicitada sobre as classes de equivalências:

(a) A relação R definida sobre $\mathbb{Z}$ por xRy se, e somente se, $x^2 = y^2$. Dê as classes $[0], [4]$ e $[-72]$;

(b) A relação R sobre $\mathbb{N} \times \mathbb{N}$ dada por $(x,y)R(z,w)$ se, e somente se, $xw = yz$. Encontre um elemento (a,b) da classe $[(2,3)]$ tal que $a = 6$. Descreva todos os elementos nessa classe;

(c) Para o conjunto $X = \{m,n,p,q,r,s\}$ seja R a relação sobre $\mathscr{P}$ dada por ARB se, e somente se, A e B têm o mesmo número de elementos. Liste todos os elementos em $\{m\}$. Quantos elementos estão em $\mathscr{P}/R$?

6. Calcule as classes de equivalência para a relação de congruência módulo 5. Ou seja, xRy se, e somente se, $x - y = 5k$, para algum $k \in \mathbb{Z}$, com $x, y \in \mathbb{R}$.

7. Considere as relações R e S sobre $\mathbb{N}$ definidas por xRy se, e somente se, $2|(x+y)$ e xSy se, e somente se, $3|(x+y)$, respectivamente. Mostre que R é uma relação de equivalência, mas S não.

8. Suponha que R e S são relações de equivalência sobre um conjunto A. Mostre que $R \cap S$ é uma relação de equivalência sobre A.

9. Seja R uma relação de equivalência sobre um conjunto A. Prove que a relação inversa R^{-1} é uma relação de equivalência sobre o conjunto A.

10. Descreva a partição para cada uma das relações de equivalência abaixo:

(a) Para $m,n \in \mathbb{Z}$, mRn se, e somente se, $m+n$ é par;

(b) Para $x,y \in \mathbb{R}$, xRy se, e somente se, $sen(x) = sen(y)$.

11. Descreva a relação de equivalência sobre o conjunto $A\{n \in \mathbb{N} : 1 \leq n \leq 15\}$ de forma que $\{\{1\};\{2,3\};\{4,5,6,7\};\{8,9,10,11,12,13,14,15\}\}$ seja uma partição de A.

12. Quais das seguintes relações sobre o conjunto dado são anti-simétricas?.

(a) $\mathbb{Z}$, xRy se, e somente se, $x = 2y$;

(b) $\mathbb{R}$, xRy se, e somente se, $x = 2^y$.

13. Mostre que a relação R sobre $\mathbb{N}$ dada por aRb se, somente se, $b = 2^k$, para algum $k \geq 0$ inteiro é de ordem parcial.

14. Defina a relação sobre $\mathbb{R} \times \mathbb{R}$ por $(a,b)R(x,y)$ se, e somente se, $a \leq x$ e $b \leq y$. Mostre que R é de ordem parcial.

15. Seja $\mathbb{C}$ o conjunto dos números complexos. Defina $(a+bi)R(c+di)$ se, e somente se, $a^2 + b^2 \leq c^2 + d^2$. É R uma relação de ordem parcial?

CAPÍTULO 6

Funções

Uma função f de um conjunto X em um conjunto Y é uma relação que associa a cada elemento $x \in X$ exatamente um elemento $y \in Y$. Assim, uma função $f : X \to Y$ satisfaz duas condições:

(1) $D(f) = X$;

(2) Se $(x,y) \in f$ e $(x,z) \in f$, então $y = z$.

Aqui $D(f)$ é dito o **domínio** da função f e o conjunto de Y dado por $f(X) = Im(f) = \{f(x) : x \in X\}$ é chamado **imagem** de f. Designamos o conjunto Y como o **contra-domínio**.

Exemplo 6.0.8. *(1) Suponha que um conjunto universo X tenha sido especificado e que $A \subset X$. Defina $\chi_A : X \to \{0,1\}$ por $\chi_A(x) = 1$ se $x \in A$ e $\chi_A(x) = 0$ se $x \notin A$. χ_A é chamada a função característica de A.*

(2) Definimos a função maior inteiro como sendo a função $g : \mathbb{R} \to \mathbb{Z}$ dada por

$$g(x) = [[x]] = \text{maior inteiro } n \text{ tal que } n \leq x.$$

Seu gráfico tem o seguinte aspecto:

(3) Uma função com domínio $\mathbb{N}$ pode ser chamada uma sequência $a : \mathbb{N} \to \mathbb{R}$ dada por $a(n) = a_n$. Por exemplo, $a(n) = \frac{1}{n}$ tem imagem $\{1, \frac{1}{2}, \frac{1}{3}, \cdots\}$.

(4) Se R é uma relação de equivalência sobre um conjunto X, então a função $f : X \to X/R$ que envia cada $x \in X$ em sua classe $f(x) = [x]$ é chamada a aplicação canônica.

Observação 6.0.9. *Muitas vezes. funções são dadas sem haver menção ao domínio. Nesse caso, o domínio é entendido como o maior subconjunto de $\mathbb{R}$ para o qual f está definida. Por exemplo, para $f(x) = \frac{\sqrt{x}}{x-2}$, o domínio de f é $[0,\infty) - \{2\} = D(f)$.*

Teorema 6.0.10. *Duas funções f e g são iguais se, e somente se, $D(f) = D(g)$ e $f(x) = g(x)$ para todo $x \in D(f)$.*

Exemplo 6.0.11. *Consideremos as seguintes funções $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}_+$ e $h : \mathbb{R}_+ \to \mathbb{R}$, dadas por $f(x) = x^2$, $g(x) = x^2$ e $h(x) = x^2$, respectivamente.*

Desde que cada função é uma relação, as operações de composição e inversão são executadas do mesmo modo que o realizado para relações. Assim, se $f : A \to B$, então a relação inversa f^{-1} é dada por

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

Se esta nova relação for uma função então dizemos que f é invertível e f^{-1} é a sua inversa.

Exemplo 6.0.12. *Para a função* $f = \{(x,y) : y = 2x+1\} \subset \mathbb{R} \times \mathbb{R}$, *a inversa de* f *é a função*

$$f^{-1} = \{(x,y) : (y,x) \in f\} = \{(x,y) : x = 2y+1\} = \{(x,y) : y = \frac{x-1}{2}\}.$$

Contudo, para a função $g = \{(x,y) : y = x^2\} \subset \mathbb{R}^+ \times \mathbb{R}^+$, *temos que a relação inversa*

$$g^{-1} = \{(x,y) : (y,x) \in g\} = \{(x,y) : x = y^2\} = \{(x,y) : y = \pm\sqrt{x}\}$$

não é uma função. De fato, $(1,1),(1,-1) \in g^{-1}$ *pois* $1^2 = (-1)^2$. *Porém,* $1 \neq -1$.

Seguindo o definido quando estudamos relações, se $f : A \to B$ e $g : B \to C$, então a composição de f e g é a relação

$$\begin{aligned} g \circ f =& \{(x,z) : \text{para algum } y \in B, (x,y) \in f \text{ e } (y,z) \in g\} \\ =& \{(x,z) : \exists y \in B, f(x) = y \text{ e } g(y) = z\} \\ =& \{(x,z) : g(f(x)) = z\}. \end{aligned}$$

Assim, definimos $(g \circ f)(x) = g(f(x))$.

Exemplo 6.0.13. *Se* $f(x) = sen(x)$ *e* $g(x) = x^2 + 6x$, *então* $(f \circ g)(x) = f(g(x)) = sen(g(x)) = sen(x^2+6x)$ *e* $(g \circ f)(x) = g(f(x)) = sen^2(x) + 6sen(x)$. *Este exemplo mostra que a composição de funções não é uma operação comutativa, isto é,* $f \circ g \neq g \circ f$ *para algumas funções* f *e* g.

Observação 6.0.14. *A composição de funções é associativa, ou seja, se* $f : A \to B$, $g : B \to C$ *e* $h : C \to D$, *então* $(h \circ f) \circ g = h \circ (f \circ g)$. *Use a definição de composição para verificar que essas funções são iguais.*

Definição 6.0.15. *Seja* $f : A \to B$ *e seja* $D \subset A$. *A restrição de* f *a* D, *denotada por* $f|_D$, *é a função* $f|_D(x) = f(x)$ *para todo* $x \in D$.

Definição 6.0.16. *Uma função* $f : X \to Y$ *é dita ser* ***injetiva*** *(ou um a um) proposto que* f *aplique elementos distintos de* X *em elementos distintos de* Y, *isto é, se* $x \neq y$ *em* X, *então* $f(x) \neq f(y)$ *em* Y. *A função* f *é dita ser* ***sobrejetiva*** *(ou sobre) proposto que cada elemento de* Y *seja a imagem sob* f *de pelo menos um elemento de* X, *ou seja, para todo* $y \in Y$ *existe* $x \in X$ *tal que* $f(x) = y$.

Em outras palavras, uma função f é sobrejetiva se, e somente se, $Im(f) = Y$.

Exemplo 6.0.17. *(1) A função* $f : \mathbb{R}_+ - \{0\} \to \mathbb{R}$ *dada por* $f(x) = \frac{x+1}{x}$ *é injetiva, pois se* $f(x) = f(y)$, *então* $\frac{x+1}{x} = \frac{y+1}{y}$ *e daí* $(x+1)y = (y+1)x$. *Portanto,* $x = y$. *Observe que a forma mais prática de mostrar a injetividade de uma função* f *é usar a contrapositividade. Agora verifiquemos que a função* f *não é sobrejetiva. Se este fosse o caso, teríamos que para todo* $y \in \mathbb{R}$ *existiria pelo menos um* $x \in \mathbb{R}_+ - \{0\}$ *tal que* $f(x) = y$. *Ou seja,* $\frac{x+1}{x} = y$, *donde concluiríamos que* $x = \frac{1}{y-1}$. *Mas isso não vale para* $y = 1$!

(2) Seja $g : \mathbb{R} \to \mathbb{R}$ definida por $g(x) = x^2 + 1$. Então g não é sobrejetiva, pois existem elementos no contra-domínio que não tem pré-imagem no domínio. Por exemplo, para cada $y \leq 0$ não existe $x \in \mathbb{R}$ tal que $g(x) = y$ já que $g(x) = x^2 + 1 \geq 1$. A função g também não é injetiva, pois $g(1) = g(-1)$, porém $1 \neq -1$.

(3) A função $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por $f(x,y) = xy$ é sobrejetiva porque para todo $y \in \mathbb{Z}$ existe $(z,1) \in \mathbb{Z} \times \mathbb{Z}$ tal que $f(z,1) = z \cdot 1 = z$. Mas f não é injetiva pois $f(1,1) = f(-1,-1)$ com $(1,1) \neq (-1,-1)$.

(4) Seja $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $h(m,n) = 2^{m-1}(2n-1)$. Para mostrarmos que h é sobrejetiva, considere $s \in \mathbb{N}$. Devemos provar que existe $(m,n) \in \mathbb{N} \times \mathbb{N}$ tal que $h(m,n) = s$. Ora, se s é par, então podemos expressar s na forma $2^k t$, onde $k \geq 1$ e t é ímpar. Desde que t é ímpar, existe $n \in \mathbb{N}$ tal que $t = 2n-1$. Assim, para $m = k+1$ temos que $h(m,n) = 2^{m-1}(2n-1) = 2^k t = s$. Por outro lado, se s é ímpar, então $s = 2n-1$ para algum $n \in \mathbb{N}$ e daí, tomanto $m = 1$ segue que $h(m,n) = 2^{m-1}(2n-1) = s$. Agora, a função h também é injetiva. De fato, suponha $h(m,n) = h(r,s)$ e $m \geq r$ (o caso $m < r$ é tratado de forma semelhante). Então $2^{m-1}(2n-1) = 2^{r-1}(2s-1)$ e isso implica que $2^{m-r}(2n-1) = 2s-1$. Como o lado direito é ímpar, seque que $m - r = 0$, donde $m = r$. Logo, $2n-1 = 2s-1$ fornece $n = s$ e $(m,n) = (r,s)$.

Vimos então que funções podem aplicar elementos do domínio em elementos do contra-domínio de muitas maneiras. Uma função pode "atingir"cada elemento no contra-domínio ou ela pode "errar"alguns. Ela pode associar mais que um x a y ou pode associar exatamente um x a cada y. Quando uma função é simultaneamente injetiva e sobrejetiva, dizemos que ela é bijetiva.

Quinta Lista de Exercícios

1. Quais das seguintes relações são funções?

   (a) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x = sen(y)\}$;

   (b) $S = \{(x,y) \in \mathbb{N} \times \mathbb{N} : x \leq y\}$;

   (c) $T = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : y^2 = x\}$.

2. Para a função real f dada por $f(x) = x^2 - 1$ responda:

   (a) Qual a imagem de $x = 5$ sob f?

   (b) Qual é a pré-imagem de 15?

3. Explique porque as funções $f(x) = \frac{9-x^2}{x+3}$ e $g(x) = 3 - x$ não são iguais.

4. Para a aplicação canônica $f : \mathbb{Z} \to \mathbb{Z}_6$ encontre $f(3)$ e a pré-imagem de $[3]$.

5. Encontre $f \circ g$ e $g \circ f$ para cada par de funções f e g:

   (a) $f(x) = 2x + 5$ e $g(x) = 6 - 7x$;

(b) $f(x) = sen(x)$ e $g(x) = 2x^2 + 1$;

(c) $f(x) = x+1$, se $x \leq 0$ e $f(x) = 2x$, se $x > 0$, e $g(x) = 2x$, se $x \leq -1$ e $g(x) = -x$, se $x > -1$.

6. Para qual das seguintes funções f a relação inversa f^{-1} é uma função? Quando f^{-1} for uma função escreva uma expressão explícita para $f^{-1}(x)$.

(a) $f(x) = 5x+2$;

(b) $f(x) = \frac{x+1}{x+2}$;

(c) $f(x) = e^{x+3}$;

(d) $f(x) = sen(x)$.

7. Seja I um intervalo da reta real, e seja f uma função de valor real com $I \subset D(f)$. Dizemos que f é crescente sobre I se, e somente se, para todo $x, y \in I$, se $x < y$ então $f(x) < f(y)$. Dizemos que f é decrescente sobre I se, e somente se, para todo $x, y \in I$, se $x < y$ então $f(x) > f(y)$. Prove que:

(a) f é crescente sobre $\mathbb{R}$, onde $f(x) = 3x - 7$;

(b) f é crescente sobre $(-3, \infty)$, onde $f(x) = \frac{x-1}{x+3}$;

(c) g é decrescente sobre I, onde $g = h \circ f$, onde h é decrescente e f é crescente sobre I.

8. Quais das seguintes funções são sobrejetivas, injetivas ou bijetivas? No caso de uma bijeção, forneça f^{-1}:

(a) $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, $f(x) = (x, x)$;

(b) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$;

(c) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = cos(x)$;

(d) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2^x$;

(e) $f : [2, 3) \to [0, \infty)$, $f(x) = \frac{x-2}{3-x}$;

(f) $f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$, $f((x, y), (u, v)) = xu + yv$. Você reconhece essa função?

(g) $f : \mathscr{P}(X) \to \mathscr{P}(X)$, $f(A) = X - A$.

9. Mostre que $f : \mathbb{Z}_4 \to \mathbb{Z}_8$ dada por $f([x]_4) = [2x]_8$ é uma injeção, mas não é uma bijeçào.

10. Seja $f(x) = x^2 + 1$. Encontre $f([1, 3])$ e $f^{-1}([-1, 1])$.

11. Seja $f : \mathbb{R} - \{0\} \to \mathbb{R}$ dada por $f(x) = x + \frac{1}{x}$. Encontre $f(f^{-1}(\mathbb{R}))$.

12. Seja $f : A \to B$ uma função. Mostre que se $X \subset A$ e f é injetiva, então $f(A - X) = f(A) - f(X)$.

13. Seja $f : A \to B$ e seja R a relação sobre A definida por xRy se, e somente se, $f(x) = f(y)$. Mostre que R é uma relação de equivalência.

14. Para cada $r \in \mathbb{R}$ seja $A_r = \{(x,y,z)\mathbb{R}^3 : x^2 + y^2 + z^2 = r^2\}$. É isto uma partição de $\mathbb{R}^3$? Se sim, dê uma descrição geométrica dos conjuntos particionados.

15. Existe uma função injetiva do intervalo aberto $(0,2)$ no intervalo aberto $(0,1)$? Se sim, explicite-a.

16. Seja $f : \mathbb{R} \to (-1,1)$ definida por $f(x) = \frac{x}{1+|x|}$. Mostre que f é uma função bijetiva.

17. Seja $f : \mathbb{R}^2 \to \mathbb{R}$ definida por $f(x,y) = x + y$. Mostre que não existe função $g : \mathbb{R} \to \mathbb{R}^2$ tal que $g \circ f = id_{\mathbb{R}}$.

18. Dê um exemplo de uma função não-nula $f : \mathbb{R} \to \mathbb{R}$ tal que $(f \circ f)(x) = 0$ para todo $x \in \mathbb{R}^2$. Pode uma tal função ser injetiva? Sobrejetiva?

19. Sejam A, B, C e D conjuntos não-vazios. Sejam $f : A \to B$ e $g : C \to D$ funções. Mostre que se f e g são bijetivas, então $H : A \times C \to B \times D$ definida por $H(a,c) = (f(a), g(c))$ é uma função bijetiva.

20. Seja $f : A \to B$ uma função. Mostre que se f é sobrejetiva, então $\{f^{-1}(\{b\}) : b \in B\}$ particiona o conjunto A.

CAPÍTULO 7

Cardinalidade

Intuitivamente sabemos o que significa o tamanho de um conjunto finito, e, também intuitivamente, parece claro que conjuntos finitos possuem tamanhos diferentes. O que dizer sobre conjuntos infinitos? Faz sentido discutir o tamanho de um conjunto infinito? Galileo escreveu no século dezessete que conjuntos infinitos tem o mesmo tamanho. Um entendimento correto sobre o tamanho de conjuntos infinitos foi dado por Cantor que desenvolveu a teoria dos conjuntos.

Como determinar quando dois conjuntos têm o mesmo tamanho?

Definição 7.0.18. *Sejam A e B conjuntos. Os conjuntos A e B têm a mesma* ***cardinalidade****, denotado por $A \sim B$, se existe uma função bijetiva $f : A \to B$.*

Note que a definição apenas nos fala da comparação entre dois conjuntos, mas não diz nada sobre cada conjunto individualmente. É imediato verificar as seguinte propriedades para conjuntos A, B e C:

(1) $A \sim A$;

(2) Se $A \sim B$, então $B \sim A$;

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

Exemplo 7.0.19. *(1) O conjuntos dos números naturais $\mathbb{N} = \{1, 2, 3, \cdots\}$ e o conjuntos dos quadrados $S = \{1, 4, 9, \cdots\}$ têm a mesma cardinalidade pois existe uma função bijetiva $f : \mathbb{N} \to S$ definida por $f(n) = n^2$ para todo $n \in \mathbb{N}$ (verifique este fato! Quem é a inversa de f?).*

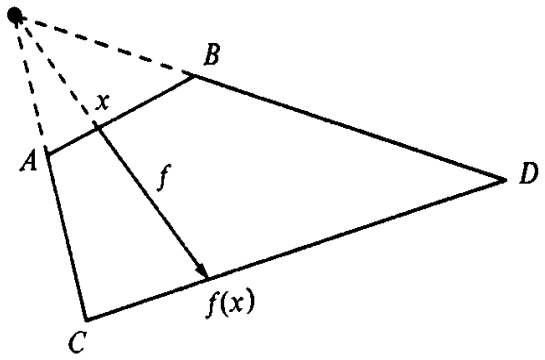
(2) O conjunto dos números naturais $\mathbb{N}$ e o conjunto dos números inteiros $\mathbb{Z}$ têm a mesma cardinalidade. Uma função bijetiva $g : \mathbb{N} \to \mathbb{Z}$ é definida por

$$g(n) = \begin{cases} \frac{n}{2}, & \text{se } n \text{ é par} \\ -\frac{n-1}{2}, & \text{se } n \text{ é ímpar.} \end{cases}$$

(3) Sejam $a, b, c, d \in \mathbb{R}$. Suponha que $a < b$ e $c < d$. Mostraremos que os intervalos $[a, b]$ e $[c, d]$ têm a mesma cardinalidade, independente dos tamanhos desses intervalos. Basta verificar que a função $h : [a, b] \to [c, d]$ definida por

$$h(x) = \frac{d-c}{b-a}(x-a) + c$$

para todo $x \in [a, b]$ é bijetiva. Um argumento análogo mostra que os intervalos (a, b) e (c, d) possuem a mesma cardinalidade.



(4) Estendemos o exemplo anterior para verificarmos que qualquer intervalo aberto (a,b) possui a mesma cardinalidade que toda a reta $\mathbb{R}$. De fato, vimos no item anterior que os intervalos (a,b) e $(-\frac{\pi}{2},\frac{\pi}{2})$ têm a mesma cardinalidade. Desde que a função $f : (-\frac{\pi}{2},\frac{\pi}{2}) \to \mathbb{R}$ dada por $f(x) = tan(x)$ é bijetiva, segue que $(a,b) \sim \mathbb{R}$.

Os exemplos revelam uma característica comum aos conjuntos infinitos (às vezes tomada como definição): eles possuem um subconjunto próprio com a mesma cardinalidade.

Definição 7.0.20. *Um conjunto é **finito** se ele é vazio ou tem a mesma cardinalidade que o conjunto $\{1,2,\cdots,n\}$, para algum $n \in \mathbb{N}$. Um conjunto é **infinito** se ele não é finito. Um conjunto é **enumerável** (ou contável) se ele é finito ou tem a mesma cardinalidade que $\mathbb{N}$. Um conjunto é **não-enumerável** (incontável) se ele não é enumerável.*

O que não é imediato nessa definição é a existência de conjuntos não-enumeráveis. Para isso faremos uso da cardinalidade do conjunto potência.

Teorema 7.0.21 (Cantor)**.** *Seja A um conjunto. Então A e $\mathscr{P}(A)$ não têm a mesma cardinalidade.*

Demonstração. Existem dois casos. Primeiro, se $A = \emptyset$, então $\mathscr{P}(A) = \{\emptyset\}$ e, assim, não pode existir uma função bijetiva entre o conjunto unitário $\mathscr{P}(A)$ e o conjunto vazio A. Logo, A e seu conjunto potencia não tem a mesma cardinalidade.

Segundo, se $A \neq \emptyset$, então suponha que A e $\mathscr{P}(A)$ tenham a mesma cardinalidade. Ou seja, existe uma função bijetiva $f : A \to \mathscr{P}(A)$ que associa cada elemento em A a um subconjunto de A. Seja $D = \{a \in A : a \notin f(a)\}$. Note que $D \subseteq A$ e, assim, $D \in \mathscr{P}(A)$. Desde que f é sobrejetiva, existe $d \in A$ tal que $f(d) = D$. Ora, $d \in D$ ou $d \notin D$ e em ambos os casos chegamos a uma contradição. De fato, se $d \in D$, então pela definição de D temos que $d \notin f(d) = D$. Por outro lado, se $d \notin D$, então $d \in f(d) = D$. □

Consequentemente, $\mathbb{N}$ e $\mathscr{P}(\mathbb{N})$ não tem a mesma cardinalidade. Além disso, $\mathscr{P}(\mathbb{N})$ não é finito, pois se esse fosse o caso, o subconjunto $T = \{\{n\} : n \in \mathbb{N}\} \subset \mathscr{P}(\mathbb{N})$ seria finito. Contudo, é evidente que T e $\mathbb{N}$ têm a mesma cardinalidade. Isto implicaria que $\mathbb{N}$ é finito, o

que é um absurdo. Concluímos então que o conjunto $\mathscr{P}(\mathbb{N})$ é não enumerável. Mas isto é um pouco abstrato. Como um exemplo mais palpável, mostraremos mais à frente que o conjunto dos números reais $\mathbb{R}$ é não enumerável.

Para mostrarmos que um conjunto é enumerável é necessário mostrar que ele é finito ou tem a mesma cardinalidade que $\mathbb{N}$. Unificaremos estes dois casos no teorema seguinte, com a vantagem que agora basta mostrar que uma determinada função é injetiva ou sobrejetiva, não ambas, para verificarmos enumerabilidade.

Teorema 7.0.22. *Seja A um conjunto não vazio. As seguintes afirmações são equivalentes:*

(a) O conjunto A é enumerável;

(b) Existe uma função injetiva $f : A \to \mathbb{N}$;

(c) Existe uma função sobrejetiva $g : \mathbb{N} \to A$.

Demonstração. $(a) \Rightarrow (b)$. Suponha que A é enumerável. Existem dois casos, dependendo de quando A é finito ou tem a mesma cardinalidade de $\mathbb{N}$. Se A é finito, existe uma função bijetiva $f : A \to \{1, \cdots, n\}$ para algum $n \in \mathbb{N}$, e assim existe uma função injetiva $f^* : A \to \mathbb{N}$, porque $\{1, \cdots, n\} \subset \mathbb{N}$. Agora, se A tem a mesma cardinalidade que $\mathbb{N}$, então existe uma bijeção $h : A \to \mathbb{N}$ e, consequentemente, uma injeção.

$(b) \Rightarrow (a)$. Suponha que existe uma função injetiva $f : A \to \mathbb{N}$. □

São uniões, interseções e produtos de conjuntos enumeráveis sempre enumerável? A resposta é sim para interseções, mas nem sempre para uniões e produtos.

Teorema 7.0.23. *Suponha que A e B são conjuntos enumeráveis. Então $A \cup B$ é um conjunto enumerável.*

Demonstração. Se $A \subset B$ ou $B \subset A$, o resultado é claro. Então suponha que $A - B$ e $B - A$ são ambos não vazios. Agora note que $A \cup B = A \cup (B - A)$ e $A \cap (B - A) = \emptyset$. Desde que $B - A \subset B$, segue que $B - A$ é enumerável. Além disso, A e $B - A$ enumeráveis implica a existência de funções bijetivas $f : A \to \mathbb{N}$ e $g : B - A \to \mathbb{N}$. Defina $H : A \cup B \to \mathbb{N}$ por

$$H(x) = \begin{cases} 2f(x), & \text{se } x \in A \\ 2g(x) + 1, & \text{se } x \in B - A. \end{cases}$$

Você pode checar que a função H está bem definida e é injetiva. Logo, $A \cup B$ é enumerável. □

Observação 7.0.24. *O teorema acima pode ser generalizado, de forma que, se I é um conjunto de índices enumerável e $\{A_i\}_{i \in I}$ é uma família de conjuntos enumeráveis indexada por I, então $\bigcup_{i \in I} A_i$ é enumerável.*

No próximo teorema, queremos mostrar que $\mathbb{N} \times \mathbb{N}$ é equivalente a $\mathbb{N}$. Isto é algo surpreendente, uma vez que $\mathbb{N} \times \mathbb{N}$ parece ser muito maior que $\mathbb{N}$.

Teorema 7.0.25. *O conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável.*

Demonstração. Mostramos que $\mathbb{N} \times \mathbb{N}$ é enumerável por definir uma função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ explicitamente. Então definimos $f(n,m) = 2^n 3^m$, para todo $(n,m) \in \mathbb{N} \times \mathbb{N}$. (Note que esta função não é sobrejetiva, pois um número como 7 não está na imagem. Assim, não tentamos mostrar que f é uma bijeção entre $\mathbb{N} \times \mathbb{N}$ e $\mathbb{N}$). Como a fatorização prima de um número natural é única, a função é injetiva. Assim, temos uma aplicação injetiva $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ o que permite concluirmos que $\mathbb{N} \times \mathbb{N}$ é enumerável. □

Usamos o resultado acima para obtermos algo mais geral, no sentido que se A e B são conjuntos enumeráveis, então $A \times B$ é enumerável. De fato, desde que existem funções $f : A \to \mathbb{N}$ e $g : B \to \mathbb{N}$ injetivas, podemos definir uma função $h : A \times B \to \mathbb{N} \times \mathbb{N}$ por

$$h(x,y) = (f(x), g(y))$$

que é injetiva (verifique isso!).

Como cada sistema de números contém o conjunto dos números naturais, todos eles são infinitos. A questão é então determinar quais são enumeráveis e quais não são. Já vimos que $\mathbb{Z}$ é enumerável. Em relação aos números racionais, veremos mais uma vez que nossa intuição é falha, pois existem tantos números racionais quanto números naturais.

Teorema 7.0.26. *O conjunto dos números racionais $\mathbb{Q}$ é enumerável.*

Demonstração. fbfbfb □

O teorema nos diz que em princípio os elementos de $\mathbb{Q}$ podem ser alinhados em alguma ordem, de forma que $\mathbb{Q}$ tem um primeiro elemento, um segundo elemento, e assim por diante, embora este alinhamento não necessariamente esteja numa ordem crescente de tamanho. Na figura abaixo vemos um diagrama, devido a Cantor, que sumariza um modo bem conhecido de alinhar os números racionais positivos.

Até aqui parece que o mundo é enumerável! Está na hora de dar um exemplo de um conjunto não-enumerável. O próximo teorema mostra que o conjunto dos números reais é não-enumerável.

Teorema 7.0.27. *O conjunto $\mathbb{R}$ é não-enumerável.*

Demonstração. jgjgjgj □

Referências Bibliográficas

[1] Bloch, E. D., **Proofs and Fundamentals** - a first course in abstract mathematics, Springer (2011), New York.

[2] Chartrand G., Polimeni A. D. and Zhang P., **Mathematical Proofs**: a transition to advanced mathematics, 2 edition, Pearson Education (2008).

[3] Cunningham, D. W., **A Logical Introduction to Proof**, Springer (2012), New York.

[4] Daepp, U. e Gorkin, P., **Reading, Writing and Proving** - a closer look at mathematics, Springer (2011), New York.

[5] Garnier, R., **100% Mathematical Proof**, John-Wiley & Sons (1996), New York.

[6] Houston, K., **How to Think Like a Mathematician**, Cambridge University Press (2009), New York.

[7] Kenneth, R., **Matemática Discreta e suas Aplicações**, Mc-Graw Hill, Tradução da 6a. edição em inglês, 2009.

[8] Morais, D. C., **Um Convite à Matemática**, SBM (2012), Rio de Janeiro.

[9] Mortari, C. A., **Introdução à Lógica**, Editora Unesp (2001), São Paulo.

[10] Smith, D.; Eggen, M. e Andre, R., **A Transition to Advanced Mathematics**, Cengage Learning (2011), Boston.