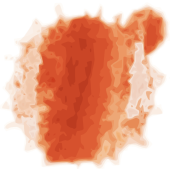


Notas de aula

Matemática Discreta

por

Jair Donadelli

2021.2

Esse documento é melhor vizualizado se acompanhado de café

Sumário

1 A linguagem matemática **2**
1.1 Noções de lógica e teoria dos conjuntos . . . 2
1.1.1 Sentenças, conectivos e operadores lógicos . . . 3
1.1.2 A implicação lógica . . . 9
Exercícios . . . 14
1.2 A teoria dos conjuntos de Zermelo–Fraenkel . . . 18
1.2.1 Abordagem intuitiva da teoria dos conjuntos . . . 18
1.2.2 Abordagem axiomática (mas ainda intuitiva) da teoria dos conjuntos . . . 21
1.2.3 Par ordenado e Produto cartesiano . . . 23
1.2.4 Relações e Funções . . . 24
Exercícios . . . 25
Complemento: Conjuntos numéricos . . . 27

2 Demonstrações **30**
2.1 Demonstrações . . . 30
2.1.1 Considerações iniciais . . . 30
2.1.2 Demonstração direta de implicação . . . 32
2.1.3 Demonstração de equivalências . . . 34
2.1.4 Demonstração indireta de implicação . . . 35
2.1.5 Demonstração por vacuidade e prova trivial . . . 38
2.1.6 Demonstração por casos . . . 38
2.1.7 Demonstrações existenciais . . . 39
2.1.8 Mais exemplos — uso do PBO . . . 40
2.1.9 Considerações finais . . . 42
Exercícios . . . 43
Complemento: O método probabilístico . . . 46

3 Princípios de Indução Finita e demonstrações por indução **48**
3.1 Princípios de indução . . . 48
3.1.1 Indução em subconjuntos dos inteiros limitados inferiormente . . . 49
3.1.2 Mais duas variantes . . . 50
3.1.3 Equivalência entre os princípios . . . 50
3.2 Demonstrações por indução . . . 50
3.2.1 A base é importante . . . 52
3.2.2 O passo é importante . . . 52
3.2.3 Outro exemplo de prova errada . . . 53
3.2.4 Desigualdade das médias aritmética e geométrica . . . 53
3.3 Definições recursivas . . . 54
Exercícios . . . 57

4 Relações **60**
4.1 Relação de equivalência . . . 61
Exercícios . . . 63
Complemento: Construção dos Inteiros . . . 64
4.2 Relação de ordem . . . 64
4.2.1 Boa ordem e Indução . . . 67

4.2.2 (opcional) O teorema de Dilworth . . . 69
Exercícios . . . 69
Complemento: Números naturais e ordinais . . . 72
4.3 Relações bem fundadas . . . 73
4.3.1 Indução bem fundada . . . 74
Exercícios . . . 78
Complemento: Lema de Zorn e teorema da boa ordem . . . 79

5 Contagem **81**
5.1 Princípios de contagem . . . 81
5.1.1 Bijeções . . . 81
5.1.2 Conjuntos finitos . . . 84
5.1.3 Conjuntos enumeráveis . . . 86
5.1.4 Conjuntos infinitos . . . 86
5.1.5 Princípio das gavetas . . . 87
5.1.6 Demonstração do Teorema de Cantor–Schröder–Bernstein . . . 89
Exercícios . . . 90
Complemento: O problema de Hadwiger–Nelson (1950) . . . 92
5.2 Combinatória . . . 93
5.2.1 Arranjo . . . 94
5.2.2 Combinação . . . 95
5.2.3 Relações de equivalência e contagem . . . 101
Exercícios . . . 105
Complemento: Aproximação de Stirling . . . 109
5.3 Funções geradoras . . . 110
5.3.1 Série formal de potências . . . 111
5.3.2 Expansão de funções de geradoras . . . 115
Exercícios . . . 117
Complemento: Série analítica de potências . . . 119
Complemento: Teorema binomial estendido . . . 121

Capítulo 1

A linguagem matemática

1.1 Noções de lógica e teoria dos conjuntos

Uma parte do trabalho dos matemáticos, de um modo geral, é descobrir e comunicar "verdades matemáticas" e uma demonstração é um argumento cujo objetivo é convencer outras pessoas de que algo é verdade. As demonstrações que aparecem nos textos, desde livros didáticos até artigos publicados em periódicos de matemática, diferem enormemente quanto ao estilo porém encerram construções que estão em, ou formam, em certo sentido, um senso comum quanto aos seus significados. O estilo é em grande parte influenciado pelo público a que se destina o texto e considera, entre outras coisas, o conhecimento esperado da audiência a que se destina.

A linguagem usada nas demostrações é uma linguagem natural, como o português, o inglês e o francês, porém tais linguagens podem levar a ambiguidades e paradoxos. Um desses paradoxos é o famoso paradoxo de Russell, de 1901, que levou a uma contradição no sistema que formalizava a teoria dos conjuntos na época:

> "Seja U o conjunto formado pelos conjuntos que não pertencem a eles mesmos. O conjunto U pertence a ele mesmo?"

No início do século 20, esse e outros problemas culminaram no que ficou conhecido como a crise dos fundamentos da matemática. Para tentar evitar ambiguidades, na matemática usamos palavras como "ou", "se…então" e outras com um significado muito específico e que nem sempre é o significado coloquial. Além disso, há uma certa "gramática" subjacente, algumas construções baseadas em princípios lógicos estão presentes nas demonstrações. Enfim, se corretamente apresentada, uma demonstração não deixa dúvidas quanto a sua correção o que dá a linguagem matemática a propriedade notável da sua precisão.

O estudo formal das deduções logicamente válidas é um dos objetos de estudo da Lógica Matemática. Os lógicos constroem linguagens formais, rigorosas, livres de ambiguidades e de contexto e que são adequadas para lidar com a relação de dedução. Essas linguagens possuem uma dimensão *sintática*, que define os símbolos da linguagem e as regras de combinação às quais estão sujeitos para a construção dos termos e fórmulas, e uma dimensão *semântica* que define precisamente o significado delas. Além disso, um sistema formal especifica os axiomas e as regras de inferência que independem da semântica e são usados para deduzir os teoremas lógicos. As teorias (axiomáticas) são estudadas acrescentando ao sistema lógico seus símbolos e axiomas, desse último deduzimos os teoremas que compõem a teoria.

A teoria dos conjuntos é um sistema adequado para descrever e explicar as estruturas matemáticas. A linguagem da lógica de predicados juntamente com a linguagem da teoria de conjuntos compõem um sistema dedutivo formal capaz de expressar praticamente toda a matemática sem ambiguidades. Para conjuntos, uma teoria axiomática bem aceita foi apresentada por Ernest Zermelo e Abraham Fraenkel no início do século 20, a teoria de conjuntos de Zermelo–Fraenkel (ZF) é um dos vários sistemas axiomáticos propostos para formular uma teoria de conjuntos livre de paradoxos como o paradoxo de Russell por exemplo. Acrescentando aos axiomas de ZF o axioma da escolha, a teoria é conhecida pela sigla ZFC e é o tratamento axiomático mais comum da teoria dos conjuntos na matemática e amplamente aceita entre os matemáticos como o ponto de partida para fundamentar a matemática de maneira estritamente formal.

Nós não utilizamos essa linguagem formal no dia-a-dia em Matemática, isso deixaria tudo muito árido mas, como já dissemos, existe uma convenção linguística quase universal na escrita em linguagem natural nas proposições matemáticas que nos faz aceitar as formas como rigorosas e não ambíguas. Neste capítulo abordamos tal linguagem informal[1] da matemática. Adotaremos aqui uma abordagem intuitiva para a teoria dos conjunto e discutiremos brevemente e informalmente a abordagem axiomática Zermelo–Fraenkel.

[1] Em oposição ao formal das linguagens lógicas.

1.1.1 Sentenças, conectivos e operadores lógicos

As afirmações matemáticas são sentenças que podem ser verdadeiras ou falsas, mas não ambas.

Uma **sentença**, é uma frase declarativa de um juízo com verbo no indicativo e que assume um, e só um, de dois valores: VERDADEIRO que passamos a denotar por **V** ou FALSO que passamos a denotar por **F**. O valor de uma sentença é chamado **valor-lógico** da sentença.

Por exemplo, são sentenças:

1. O time joga bem.
2. O céu está limpo.
3. A grama é verde.
4. Os torcedores estão felizes.

Do ponto de vista da linguagem natural é bastante restritivo considerarmos apenas sentenças declarativas, porém estamos interessado nos enunciados matemáticos:

5. $1+1=2$.
6. $3>5$.
7. Uma sequência limitada de de números reias é convergente.
8. 27 é um quadrado perfeito.
9. O conjunto vazio é único.

Para tal efeito, essas sentaças são satisfatórias. Notemos que são sentenças enunciadas como

10. x^2 é positivo;
11. x é a soma de quatro quadrados perfeitos;
12. essa frase é falsa;

pois não podemos atribuir a elas um valor lógico.

Toda linguagem permite construir sentenças mais complexas a partir de outras sentenças.

Uma sentença é dita **atômica** se a ela corresponde, individualmente, um desses valores-verdade. **Sentenças compostas** são construídas com os conectivos "**não**", "**e**", "**ou**", "**se,... então**", "**se, e somente se,**" que chamamos **conectivos lógicos**.

São sentenças atômicas "O time ganhou o campeonato" assim como "O técnico é culpado", mas não é o caso de "O time ganhou o campeonato ou o técnico é o culpado", essa última é composta. Vejamos mais alguns exemplos:

1. Os torcedores estão felizes **e** o técnico foi demitido.
2. Samuel virá para a festa **e** Maximiliano não virá, **ou** Samuel não virá para a festa **e** Maximiliano vai se divertir.
3. **Se** o time joga bem, **então** o time ganha o campeonato.
4. **Se** o time **não** joga bem, **então** o técnico é o culpado.
5. 27 **não** é um quadrado perfeito.
6. O conjunto vazio **não** é único.

O valor lógico de uma sentença composta depende do valor lógico das sentenças atômicas que a compõem e da maneira como elas são combinadas usando os conectivos. A cada conectivo lógico corresponde um operador lógico que determina um valor lógico de acordo com as regras abaixo.

As letras A e B denotam sentenças. A **negação** de A é a sentença "não A" cujo valor lógico é $\neg A$ dado pela tabela 1.1.

A **disjunção** de A e B é a sentença "A ou B" cujo valor lógico é $A \vee B$ dado pela tabela 1.2. A **conjunção** é a sentença "A e B" cujo valor lógico é $A \wedge B$ também dado na tabela 1.2. A **condicional** é a sentença "se A então B" cujo valor lógico é $A \to B$ é dado na tabela 1.2. Finalmente, a **bicondicional** é a sentença "A se, e somente se B" cujo valor lógico é $A \leftrightarrow B$ dado na tabela 1.2.

A	$\neg A$
V	**F**
F	**V**

Tabela 1.1: operador negação.

A	B	$A \vee B$	$A \wedge B$	$A \to B$	$A \leftrightarrow B$
V	**V**	**V**	**V**	**V**	**V**
V	**F**	**V**	**F**	**F**	**F**
F	**V**	**V**	**F**	**V**	**F**
F	**F**	**F**	**F**	**V**	**V**

Tabela 1.2: operadores conjunção, disjunção, condicional e bicondicional.

Esse é o modo como interpretamos essas palavras chaves e essa interpretação as vezes entra em conflito com interpretações coloquiais. O "e", em geral, não causa confusão exceto, possivelmente, pelo estilo de escrita. As vezes pode ocorrer uma confusão por abreviações na escrita. Por exemplo, quando dizemos que "5 é um natural primo e ímpar" significa que 5 tem as duas propriedades, porém o conectivo "e" com sentido lógico conecta sentenças (não objetos ou propriedades deles) de modo que tal sentença expressa "5 é um natural primo e 5 é um natural ímpar". A sentença a "se 7 é primo e divide $28 \cdot 9$, então 7 divide 28 ou divide 9" fica melhor exprimida por "se 7 é primo e 7 divide $28 \cdot 9$, então 7 divide 28 ou 7 divide 9".

No caso do "ou" o equivoco comum é considerar o "ou exclusivo" no sentido de que a disjunção é verdadeira quando ou uma ou a outra sentença é verdadeira, não ambas.

O "não", por sua vez, é mal interpretado quando mudamos o significado na negação. Por exemplo, a rigor, a negação de "o natural 5 é par" é "o natural 5 não é par" que não pode, em princípio, ser tomada como "o natural 5 é ímpar", essa equivalência só vale como consequência do teorema da divisão que garante que se um natural não é da forma $2k$ (o que o caracteriza como par), então é da forma $2k+1$ (o que o caracteriza como ímpar). A negação de m é o maior elemento do conjunto (finito) de números A, não é dizer que m é o menor elemento de A, simplesmente diz que m não é o maior elemento de A.

Veremos que "o oconjunto A está contido no conjunto B" significa que "todo elemento do conjunto A é elemento do conjunto B" cuja negação não é "nenhum elemento de A é elemento de B"! A sentença negada é "o oconjunto A não está contido no oconjunto B" e significa que "nem todo elemento do conjunto A é elemento do conjunto B" ou "algum elemento do conjunto A não é elemento do conjunto B".

Esse último caso tem a ver com a negação de uma condicional. A condicional é, provavelmente, o conectivo com mais chance de confusão entre a interpretação coloquial e a intencionada na matemática.

O condicional

É no condicional que se dá a maior diferença entre os significados em matemática e na linguagem coloquial. Se os pais dizem ao seu filho

se não comer toda a refeição, então não ganha a sobremesa

a única situação em que os pais ficam desmoralizados é quando o filho não come toda a refeição e ganha a sobremesa. A confusão aqui normalmente se dá quando "se não comer toda a refeição, então não ganha a sobremesa" é interpretado também como "se comer toda a refeição, então ganha a sobremesa" o que a rigor, no sentido matemático, não está dito; tal sentença valeria se a sentença original fosse uma bicondicional.

Ocorre que não foi estabelecido o que acontece quando o filho come toda a refeição de modo que se ele ganha a sobremesa, está tudo correto, os pais estão sendo verdadeiros e se ele não ganha a sobremesa também está tudo correto. Certamente, se o filho não comer toda a refeição e não ganhar a sobremesa também os pais foram verdadeiros.

Outro problema que ocorre frequentemente é quando interpretamos a condicional como uma consequência, uma relação de causa-efeito entre as sentenças, que não é o caso.

Todos concordamos que é verdadeira a sentença[2]

para todo número natural n, se n primo então n é maior ou igual a dois.

pois decorre da definição de número primo. Dito isso, as particularizações de "se n primo então n é maior ou igual a dois" devem ser verdadeiras, ou seja,

se 1 primo então 1 é maior ou igual a dois

[2] Augusto Oliveira, *Lógica& Aritmética*, Ed. Gradiva, 2010.

é verdadeira ("se **F**, então **F**" é verdadeiro), assim como

se 4 primo então 4 é maior ou igual a dois

é verdadeira ("se **F**, então **V**" é verdadeiro).

Exercício 1. Qual é a única sentença falsa dentre as quatro condicionais a seguir?

se $\sqrt{2}$ é racional, então 2 é par.

se $\sqrt{2}$ é racional, então 2 é ímpar.

se $\sqrt{2}$ não é racional, então 2 é par.

se $\sqrt{2}$ não é racional, então 2 é ímpar.

Em $A \to B$ chamamos A de **antecedente** e B de **consequente** da condicional. A **recíproca** de $A \to B$ é $B \to A$. Observe que que há casos em que $A \to B$ tem valor lógico diferente de $B \to A$. A **contrapositiva** de $A \to B$ é $(\neg B) \to (\neg A)$. Pode-se verificar que contrapositiva tem sempre o mesmo valor lógico que a sentença que a originou.

Em português a sentença "se A então B" pode ser expressa de muitas formas. Algumas delas estão descritos abaixo.

- B sempre que A.
- B se A.
- A é suficiente para B.
- B é necessário para A.

O "se e somente se" também pode ser expresso de várias maneiras, dentre elas

- A é condição necessária e suficiente para B.
- A e B são equivalentes.
- se A então B, e se B então A.

Neste texto usamos a abreviação "A **sse** B".

Tautologia e Contradição

Tautologia e contradição é como chamamos as sentenças compostas com valor-lógico constante.

Uma **tautologia** é uma sentença composta que é sempre verdadeira. Uma **contradição** é uma sentença composta que é sempre falsa.

Por exemplo $A \vee (\neg A)$ é uma tautologia e $(A \to B) \leftrightarrow ((\neg A) \vee B)$ é uma tautologia, enquanto que $A \wedge \neg A$ é uma contradição. Por abuso de notação representamos uma tautologia qualquer, genérica, por **V** e uma contradição qualquer, genérica, por **F**.

Variáveis

Usualmente, uma variável é um símbolo que funciona como um espaço reservado para um objeto matemático de algum universo (do discurso). Exceto quando tratamos de sintaxe linguagens formais, como a teoria (formal) de conjuntos, o que não é feito neste texto, as variáveis devem estar associadas a domínios. Em geral, o simbolo usado é uma letra. É possível que variáveis desempenhem papéis diferentes na mesma expressão. Por exemplo, como na forma geral de um polinômio de grau no máximo dois, $ax^2 + bx + c$, onde a, b, c são considerados números, são chamadas de parâmetros ou coeficientes (muitas vezes são chamadas, inapropriadamente, de constantes) e x é a incógnita, ou indeterminada.

Com funções, o termo variável se refere aos argumentos das funções, em $f(x)$ a letra f é uma função da variável x. Em algumas situações como essa x também é chamado de parâmetro, um objeto ou quantidade de um problema que permanece constante durante toda a solução, ou cálculo, desse problema. Por exemplo, em termodinâmica a pressão e a temperatura são parâmetros para o estudo de gases. Todas essas denominações de variáveis são de natureza semântica.

Em disciplinas como a matemática e a ciênca da computação, uma **variável livre** é um símbolo que especifica posições em uma expressão onde uma substituição pode eventualmente ocorrer. Por exemplo, esse é o caso de x mas não é o caso de h em

$$\lim_{h \to 0} \frac{(x+h)^2 - x^2}{h} = 2x. \tag{1.1}$$

Uma **variável muda**, as vezes chamada de variável ligada ou variável vinculada, é uma variável associada a um valor específico ou conjunto de valores, como é o h acima. A expressão (1.1) expressa alguma informação a respeito de x, mas não expressa nada a respeito de h, ela poderia ter sido escrita como $\lim_{t\to 0}((x+t)^2 - x^2)/t$.

A sentença "$n = 2 \cdot k$ para natural k" expressa algo a respeito de n, a saber, que é um número par, porém não expressa nada a respeito de k, poderíamos ter escrito "$n = 2 \cdot j$ para natural j" que transmitiríamos a mesma informação. A variável livre nessa expressão se torna muda quando escrevemos "para todo natural n, $n = 2 \cdot k$ para natural k". Agora não se expressa mais um fato a respeito de n, pois se exprime que "todo número natural é par".

A expressão

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

afirma algo a respeito da variável n, essa variável é livre, A variável k, por seu lado, é muda. Ela está associada aos números inteiros de 1 a n pois o símbolo $\sum$ a esquerda da igualdade nos indica a soma de todos os valores que k assume nesse intervalo, desde quando $k = 1$ até $k = n$. Notemos que é indiferente usarmos k, ℓ ou i para esse fim. Em

$$\sum_{k=0}^{\infty} \frac{x^k}{k!}$$

x é livre e k é muda. Nesse caso, temos uma expressão aritmética cujo valor depende da variável x, mas não da variável k, de fato essa "soma infinita" é a função e^x se considerarmos $x \in \mathbb{R}$. Assim, $\mathrm{e}^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ é uma expressão a cerca da variável (livre) x de modo que se dissermos "para todo $x \in \mathbb{R}$, $\mathrm{e}^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$" então x agora é muda e essa sentença, que não apresenta variável livre, é verdadeira.

No exemplo,

$$\int_0^t x^n \mathrm{e}^{-x}\,\mathrm{d}x$$

a variável x é muda, enquanto que t e n são livres, o valor dessa expressão também não depende de x, só de t e de n, de modo que podemos dizer que temos uma função f (com domínio e contradomínio que devem ser especificados) dada por $f(t,n) = \int_0^t x^n \mathrm{e}^{-x}\,\mathrm{d}x$ que, por sua vez é avaliada da mesma forma que $\int_0^t z^n \mathrm{e}^{-z}\,\mathrm{d}z$.

Predicados

Uma **sentença aberta** é uma sentença parametrizada por uma ou mais variáveis, ela nos diz algo (um predicado) de uma ou mais variáveis. Uma sentença aberta não tem valor lógico, porém quando se atribui um elementos de um conjunto (o domínio) para as variáveis a sentença deixa de ser aberta e passa a ser um sentença com valor lógico. O processo de trocar as ocorrências de uma variável por um elemento de um domínio chamamos de **instanciação** da variável.

Entendemos por predicado uma declaração a respeito de uma ou mais variáveis. Por exemplo, "x é primo", "x é maior que 0", "x é menor ou igual a y", "x, y, z são vértices de um triângulo", "$x < 1$" são predicados. Observemos que "$x + 1$" não é predicado, essa expressão não diz algo a respeito de x.

Algumas poucas vezes, por conveniência, usamos a notação funcional para sentenças predicativas, letras minúsculas $x, y, z, \ldots$ denotam variáveis e letras maiúsculas $P, Q, R, \ldots$ os predicados, os quais são seguidas por uma lista de variáveis distintas entre parênteses, usados para denotar sentenças abertas que dependem dessas variáveis, por exemplo

$O(x)$**:** representa a sentença aberta $x \leqslant x^2$.

$P(x)$**:** representa a sentença aberta x é primo.

$Q(x,y)$**:** representa a sentença aberta $x \leqslant y^2$.

$S(n)$**:** representa a sentença aberta $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Nesse casos, uma instanciação de uma variável troca todo ocorrência daquela variável pela instância. Usando os exemplos acima temos: $O(1)$ é "$1 \leqslant 1^2$", $P(4)$ é "4 é primo" e $Q(1,2)$ e "$1 \leqslant 2^2$". A senteça $Q(1,y)$ é "$1 \leqslant y^2$", portanto aberta. Se instanciamos todas as variáveis de uma sentença aberta ela deixa de ser aberta e passa a ter valor lógico, por exemplo, $R(x,y)$ dada por $x > y$ é uma sentença verdadeira se os valores de x e y forem 7 e 4, ou seja $R(4,7)$ é verdadeiro. Mas tal sentença é falsa se os valores forem $x = 1$ e $y = 2$, ou seja, $R(1,2)$ é falso.

De um modo geral, dado um predicado $P(x_1, x_2, \ldots, x_n)$, usamos a notação $P(v_1, v_2, \ldots, v_n)$ para indicar a **substituição** de todas as ocorrências da variável x_i pelo valor v_i, para todo $i = 1, 2, \ldots, n$.

Podemos combinar predicados usando os conectivos lógicos para formar outros predicados.

Quantificadores

A substituição de variáveis por valores do domínio não é a única maneira de transformar uma sentença aberta em uma sentença. Outra maneira é a **quantificação** da variável. A quantificação permite expressar conceitos como "todos os elementos do domínio" ou "alguns elementos do domínio". O primeiro é chamado quantificação universal e segundo de quantificação existencial.

A **quantificação universal** de $P(x)$ é a sentença

$$\text{para todo } x \in D,\ P(x) \tag{1.2}$$

que é verdadeira se $P(x)$ é verdadeiro para toda instanciação de x com valores de um domínio $D \neq \varnothing$. Caso $P(x)$ seja falsa para um ou mais valores atribuídos a x então a sentença (1.2) é falsa. A sentença (1.2) é, simbolicamente, escrita como

$$\forall x \in D,\ P(x).$$

Um elemento de D para o qual P é falso um **contraexemplo** para (1.2)

Por exemplo, "para todo $x \in \mathbb{Z},\ x < x+1$" é verdadeira enquanto que "para todo $x \in \mathbb{N},\ x$ é primo" é falsa pois, por exemplo, $4 \in \mathbb{N}$ e 4 não é primo. Nesse caso, dizemos que 4 é um contraexemplo para "para todo $x \in \mathbb{N},\ x$ é primo".

A **quantificação existencial** da sentença aberta $P(x)$ é a sentença

$$\text{existe } x \in D,\ P(x) \tag{1.3}$$

que é verdadeira se $P(x)$ é verdadeiro para pelo menos uma instanciação de x com valores de $D \neq \varnothing$. Caso $P(x)$ seja falsa para todos os valores de D atribuídos a x então a sentença existe $x \in D,\ P(x)$ é falsa. Simbolicamente, usamos

$$\exists x \in D,\ P(x)$$

para expressar (1.3).

Por exemplo, "existe $x \in \mathbb{Z},\ x = x+1$" é falsa enquanto que "existe $x \in \mathbb{N},\ x$ é primo" é verdadeira.

Exemplo 2. São exemplos de sentenças quantificadas:

1. "Todo o número inteiro que não é ímpar é par". Essa sentença fica melhor, no sentido de explicitar seus componentes lógicos, se a escrevemos como"para todo $n \in \mathbb{Z}$, se n não é impar então n é par". Em símbolos poderíamos escrevê-la como $\forall n \in \mathbb{Z}(\neg\exists k \in \mathbb{Z}, n = 2k+1 \rightarrow \exists k \in \mathbb{N}, n = 2k)$.
2. "Para cada número real x, existe um número real y para o qual $y^3 = x$", ou em símbolos $\forall x \in \mathbb{R}, \exists y \in \mathbb{R},\ y^3 = x$.
3. "Dado qualquer dois números racionais a e b, segue-se que ab é racional", ou seja, "para todo $a \in \mathbb{Q}$, para todo $b \in \mathbb{Q}$, $a \cdot b \in \mathbb{Q}$".

Exemplo 3. As sentenças

1. para todo $x \in \mathbb{R}$, se $x \geq 0$ então $x^2 \geq 0$
2. existe $x \in \mathbb{R}$, se $x \geq 0$ então $x^2 \geq 0$

são verdadeiras. Agora,

- para todo $x \in \mathbb{R}$, se $x \geq 0$ então $x^2 > 3$

é falsa e para mostrar isso basta exibirmos um contraexemplo. Nesse caso, um contraexemplo é um valor a do domínio para o qual "se $a \geq 0$ então $a^2 > 3$" é falso, como o número 0.

Negação e domínio vazio Deve ficar claro que da exposição acima podemos concluir que a negação de "para todo $x \in D,\ P(x)$" é "existe $x \in D$, não $P(x)$".

Exercício 4. Qual é a negação de "existe $x \in D$, $P(x)$"?

No caso de domínio vazio, convencionamos que "para todo $x \in D$, $P(x)$" é verdadeiro. Isso corrobora o fato da negação dessa sentença ser falsa, isto é, "existe $x \in D$, não $P(x)$" é falso independentemente de P pois $D = \varnothing$. Analogamente, "existe $x \in D$, $P(x)$" é falso.

Omissão de quantificadores As vezes, infelizmente, ocorre em textos que lemos a omissão de quantificadores que deveriam estar presentes para que expressões tenham seu significado explicitado. Nesses casos, os quantificadores estão implícitos, como nos seguintes exemplos.

No domínio do reais a afirmação "*se x é inteiro, então x é racional*" é uma sentença implicitamente quantificada universalmente que, simbolicamente, pode ser escrita como

$$\text{para todo } x \in \mathbb{R}, \text{ se } \in \mathbb{Z}, \text{ então } x \in \mathbb{Q}$$

assim como a identidade trigonométrica $\sin^2(x) + \cos^2(x) = 1$ que é completamete expressa como

$$\text{para todo } x \in \mathbb{R}, \ \sin^2(x) + \cos^2(x) = 1.$$

Múltiplos quantificadores Se uma sentença aberta menciona mais de uma variável, é preciso um quantificador para cada variável distinta para transformá-la numa sentença fechada. Por exemplo, no domínio dos inteiros há oito maneiras de transformar a sentença aberta $x + y = y + x$ em uma sentença fechada:

1. $\forall x \in \mathbb{Z}, \ \forall y \in \mathbb{Z}(x + y = y + x)$
2. $\forall x \in \mathbb{Z}, \ \exists y \in \mathbb{Z}(x + y = y + x)$
3. $\exists x \in \mathbb{Z}, \ \forall y \in \mathbb{Z}(x + y = y + x)$
4. $\exists x \in \mathbb{Z}, \ \exists y \in \mathbb{Z}(x + y = y + x)$
5. $\forall y \in \mathbb{Z}, \ \forall x \in \mathbb{Z}(x + y = y + x)$
6. $\forall y \in \mathbb{Z}, \ \exists x \in \mathbb{Z}(x + y = y + x)$
7. $\exists y \in \mathbb{Z}, \ \forall x \in \mathbb{Z}(x + y = y + x)$
8. $\exists y \in \mathbb{Z}, \ \exists x \in \mathbb{Z}(x + y = y + x)$

Em sentenças com mais de uma variável *a ordem em que os quantificadores aparece é importante.* Por exemplo, se x e y são inteiros

$$\text{para todo } x \in \mathbb{Z}, \text{ existe } y \in \mathbb{Z}, \ x + y = 0 \tag{1.4}$$

não é logicamente equivalente a

$$\text{existe } y \in \mathbb{Z}, \text{ para todo } x \in \mathbb{Z}, \ x + y = 0 \tag{1.5}$$

pois (1.4) é verdadeiro enquanto que (1.5) é falso. Entretanto, em alguns casos vale a equivalência. Por exemplo,

$$\text{para todo } x \in \mathbb{N}, \text{ existe } y \in \mathbb{N}, \ x \text{ divide } y$$

é verdadeira, assim como

$$\text{existe } y \in \mathbb{N}, \text{ para todo } x \in \mathbb{N}, \ x \text{ divide } y$$

pois, no segundo caso todo $x \in \mathbb{N}$ divide o 0.

Ao escrever (e ler) demonstrações de teoremas nós devemos estar sempre atentos à estrutura lógica e ao significados das sentenças. Às vezes é útil escrevê-las em expressões que envolvem símbolos lógicos. Isso pode ser feito mentalmente ou em papel de rascunho, ou ocasionalmente, mesmo explicitamente dentro do corpo de uma prova. Entretanto, deve-se ter em mente que simbolizar uma sentença não a torna mais formal ou mais correta.

Exercício 5. Escreva a seguintes sentenças em português e diga se são verdadeiras ou falsas.

1. $\forall x \in \mathbb{R}, \ x^2 > 0$.
2. $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, \ xn \geqslant 0$
3. $\exists a \in \mathbb{R}, \forall x \in \mathbb{R}, \ ax = x$.
4. $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, \ m + n = 5$.
5. $\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, \ m + n = 5$.

1.1.2 A implicação lógica

Quando lemos um teorema em um livro, como *se a função f é diferenciável em a então a função f é contínua em a* em um livro de análise real, por exemplo, entendemos que tal sentença é verdadeira e seguirá uma demonstração de tal fato.

Esse entendimento de que a sentença do teorema é verdadeira significa formularmos uma outra sentença que afirma que algo sobre a primeira sentença, a saber, formulamos que "a sentença *se a função f é diferenciável em a então a função f é contínua em a* é verdadeira". Dizemos que essa última é uma *metassentença*, uma sentença que diz algo respeito de sentenças.

Ademais, a demonstração de tal teorema estabelece uma relação entre a sentença *a função f é diferenciável em a* e a sentença *a função f é contínua em a*, a saber, que a segunda é verdadeira sempre que a primeira é verdadeira.

A ideia intuitiva de implicação lógica é que a sentença A implica na declaração B se *B é verdadeiro sempre que A é verdadeiro*. Em outras palavras, nunca pode ser o caso em que A é verdadeiro e B é falso.

O valor verdadeiro da condicional $A \to B$ não deve ser circunstancial, devido ao valor verdade das sentenças A e B. A implicação lógica não deve depender dos valores lógicos particulares das sentenças atômicas que a compõem pois elas estão de tal forma relacionadas nas fórmulas que resultado final é sempre uma condicional tautológica, como no seguinte exemplo trivial: $A \to A$, não importa o valor lógico de A, a condicional é sempre verdadeira. O mesmo ocorre com (A e ($A \to B$)) $\to B$, o segundo condicional é sempre verdadeiro, independentemente dos valores lógicos de a e B.

Dizemos que A **implica logicamente** B, ou simplesmente A **implica** B, se a sentença condicional "se A então B" (em símbolos $A \to B$) é uma tautologia.

Nós abreviamos a expressão "A implica B" por $A \Rightarrow B$. É importante notarmos a diferença entre as notações $A \to B$ e $A \Rightarrow B$. Na prática, do ponto de vista informal que adotamos, a distinção é simples

$A \to B$ é uma sentença composta construída a partir de A e B que lemos "se A então B".

$A \Rightarrow B$ é uma (meta)sentença que significa que $A \to B$ é uma tautologia, ou seja, verdadeiro independentemente dos valores lógicos de A e de B, e que lemos "'se A então B' é verdadeiro" ou "se A é verdadeiro então B é verdadeiro".

Veremos adiante que as implicações são extremamente úteis na construção de argumentos válidos.

Mais geralmente, sejam $A_1, A_2, \ldots, A_n$ e B sentenças. Dizemos que essas sentenças $A_1, A_2, \ldots, A_n$ **implicam logicamente** B se $A_1 \wedge A_2 \wedge \cdots \wedge A_n \to B$ é uma tautologia e escrevemos $A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow B$.

Por exemplo, dado que $A \to B$ é verdadeira, temos que sua conclusão B pode ser verdadeira ou falsa, mas se nos é dado que a hipótese A também é verdadeiras, então a conclusão B deve ser, obrigatoriamente, verdadeira, isto é

$$A \wedge (A \to B) \Rightarrow B$$

Essa implicação lógica é conhecida por ***modus ponens***.

Exemplo 6. Considere as sentenças A dada por "Mané estuda"; B por "Mané joga futebol" e C dada por "Mané passa em discreta". Então $A \to C$, $(\neg B) \to A$, $(\neg C)$ têm como consequência lógica B.

A tabela 1.3 lista algumas consequências lógicas notáveis. As letras A, B, C denotam sentenças e A e B predicados.

Adição	$A \Rightarrow A \to B$
Simplificação	$A \wedge B \Rightarrow A$ $A \wedge B \Rightarrow B$
Modus ponens	$A \wedge (A \to B) \Rightarrow B$
Modus tollens	$(A \to B) \wedge (\neg B) \Rightarrow \neg A$
Silogismos	$(A \to B) \wedge (B \to C) \Rightarrow A \to C$ $(A \vee B) \wedge (\neg A) \Rightarrow B$
Contradição	$A \to \mathbf{F} \Rightarrow \neg A$
Distributiva para quantificadores	$(\forall x P(x)) \vee (\forall x Q(x)) \Rightarrow \forall x\,(P(x) \vee Q(x))$ $\exists x\,(P(x) \wedge Q(x)) \Rightarrow (\exists x P(x)) \wedge (\exists x Q(x))$

Tabela 1.3: Consequências lógicas notáveis.

Do exemplo 6 acima tiramos

1.	$A \to C$	premissa
2.	$\neg C$	premissa
3.	$\neg B \to A$	premissa
4.	$\neg C \to \neg A$	contrapositiva de 1
5.	$\neg A$	Modus ponens de 2 e 4
6.	$\neg A \to \neg(\neg B)$	contrapositiva de 3
7.	$\neg(\neg B)$	modus ponens de 5 e 6
8.	B	dupla negação

em que cada linha a partir da linha 4 é consequência lógica das linhas anteriores, portanto, B é consequência lógica das premissas.

Equivalência lógica

Há sentenças que são diferentes mas transmitem a mesma informação como "não é o caso de eu não perder o guarda-chuva" ser equivalente a "eu vou perder o guarda-chuva". O que nos interessa são declarações logicamente equivalentes, ou seja, sentenças diferentes como mesmo valor lógico como, por exemplo, A e $\neg\neg A$.

Duas sentenças A e B são **logicamente equivalentes** se assumem o mesmo valor lógico, isto é, $A \leftrightarrow B$ é uma tautologia. A notação é $A \Leftrightarrow B$. As sentenças abertas $P(x)$ e $Q(x)$ são **logicamente equivalentes** se $P(a) \leftrightarrow Q(a)$ é tautologia para todo $a \in D$, e escrevemos $\forall x \in D(P(x) \Leftrightarrow Q(x))$.

Por exemplo $(A \to B) \Leftrightarrow (\neg A \vee B)$ e $(A \leftrightarrow B) \Leftrightarrow (A \to B) \wedge (B \to A)$.

Observamos que $\leftrightarrow$ é um conectivo, ele "conecta" sentenças enquanto que $\Leftrightarrow$ é uma abreviação de uma metassentença.

As leis de equivalências dadas na tabela 1.4 são notórias e a seguir são usadas para deduzir outras.

Identidade	$A \wedge \mathbf{V} \Leftrightarrow A$ $A \vee \mathbf{F} \Leftrightarrow A$
Idempotência	$A \vee A \Leftrightarrow A$ $A \wedge A \Leftrightarrow A$
Distributiva	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
Comutativa	$A \vee B \Leftrightarrow B \vee A$ $A \wedge B \Leftrightarrow B \wedge A$
Associativa	$A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$ $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$
Absorção	$A \vee (A \wedge B) \Leftrightarrow A$ $A \wedge (A \vee B) \Leftrightarrow A$
De Morgan	$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
Dominação	$A \vee \mathbf{V} \Leftrightarrow \mathbf{V}$ $A \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$
Inversas	$A \vee (\neg A) \Leftrightarrow \mathbf{V}$ $A \wedge (\neg A) \Leftrightarrow \mathbf{F}$
Dupla negação	$\neg(\neg(A)) \Leftrightarrow A$
Contrapositiva	$A \to B \Leftrightarrow (\neg B) \to (\neg A)$
Contradição	$A \to B \Leftrightarrow (A \wedge (\neg B)) \to \mathbf{F}$
Distributiva para quantificadores	$\forall x\,(P(x) \wedge Q(x)) \Leftrightarrow (\forall x P(x)) \wedge (\forall x Q(x))$ $\exists x\,(P(x) \vee Q(x)) \Leftrightarrow (\exists x P(x)) \vee (\exists x Q(x))$
Negação	$\neg(\forall x,\, P(x)) \Leftrightarrow \exists x,\, \neg(P(x))$ $\neg(\exists x,\, P(x)) \Leftrightarrow \forall x,\, \neg(P(x))$

Tabela 1.4: Equivalências lógicas notáveis.

Exercício 7. Verifique usando as leis da tabela 1.4 que $(A \vee B) \wedge \neg(\neg(A) \wedge B)$ é logicamente equivalente a A.

Resolução.

$$
\begin{array}{rcl}
 & (A \vee B) \wedge \neg(\neg(A) \wedge B) & \\
\Leftrightarrow & (A \vee B) \wedge (\neg\neg(A) \vee \neg(B)) & \text{por De Morgan} \\
\Leftrightarrow & (A \vee B) \wedge (A \vee \neg(B)) & \text{por dupla negação} \\
\Leftrightarrow & (A \vee (B \wedge \neg(B)) & \text{por distributiva} \\
\Leftrightarrow & (A \vee \mathbf{F}) & \text{por inversa} \\
\Leftrightarrow & A & \text{por identidade}
\end{array}
$$

□

Exercício 8. Verifique que $\neg(A \to B) \Leftrightarrow A \wedge \neg(B)$.

Regras de Inferência e Argumentos válidos

Um **argumento** é uma sequência $A_1, A_2, \ldots, A_n$ de sentenças, ditas **premissas** que terminam com uma sentença dita **conclusão** B (o que indicamos pelo símbolo $\therefore$ lido como "portanto")

$$
\begin{array}{l}
A_1 \\
A_2 \\
\vdots \\
A_n \\
\hline
\therefore B
\end{array}
$$

O argumento é **válido** se, e só se, $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \Rightarrow B$, isto é, se a conclusão B é verdadeira sempre as premissas forem verdadeiras.

Regras de inferência são esquemas de argumentos válidos simples que usamos para para construir argumentos válidos mais complexos.

Por exemplo,

$$
\begin{array}{l}
\text{Se você tem uma senha, então você pode entrar no moodle.} \\
\text{Você tem uma senha.} \\
\hline
\text{Portanto, você pode entrar no moodle.}
\end{array}
$$

é um argumento válido porque se encaixa na lei de *modus ponens* dada na tabela 1.3, o argumento

$$
\begin{array}{l}
A \to B \\
A \\
\hline
\therefore B
\end{array}
$$

é uma regra de inferência chamada ***Modus Ponens***. Cada lei dada na tabela 1.3 nos dá uma regra de inferência:

1. **Regra da Adição** Se A é uma premissa, podemos deduzir $A \vee B$

$$
\begin{array}{l}
A \\
\hline
\therefore A \vee B
\end{array}
$$

2. **Regra da Simplificação** Se $A \wedge B$ é uma premissa, podemos deduzir A

$$
\begin{array}{l}
A \wedge B \\
\hline
\therefore A
\end{array}
$$

3. ***Modus ponens***

$$
\begin{array}{l}
A \to B \\
A \\
\hline
\therefore B
\end{array}
$$

4. ***Modus tollens*** Se $A \to B$ e $\neg B$ são duas premissas, podemos usar o *modus tollens* para deduzir $\neg A$

$$\begin{array}{l} A \to B \\ \neg B \\ \hline \therefore \neg A \end{array}$$

Por exemplo

Se você tem uma senha, então você pode entrar no moodle.
Você não pode entrar no moodle.
Portanto, você não tem uma senha.

5. **Regra do silogismo hipotético** Se $A \to B$ e $B \to C$ são duas premissas, podemos usar o silogismo hipotético para deduzir $A \to C$

$$\begin{array}{l} A \to B \\ B \to C \\ \hline \therefore A \to C \end{array}$$

6. **Regra do silogismo disjuntivo** Se $\neg A$ e $A \vee B$ são premissas, podemos usar o silogismo disjuntivo para deduzir B

$$\begin{array}{l} A \vee B \\ \neg A \\ \hline \therefore B \end{array}$$

7. **Regra da contradição** Se $\neg A \to \mathbf{F}$ é verdadeiro então A é verdadeiro

$$\begin{array}{l} \neg A \to \mathbf{F} \\ \hline \therefore A \end{array}$$

8. **Regra da conjunção** Se temos A e temos B então deduzimos $A \wedge B$

$$\begin{array}{l} A \\ B \\ \hline \therefore A \wedge B \end{array}$$

Podemos usar essa regras para escrever outras regras, ou argumentos válidos. O seguinte é um argumento válido

$$\begin{array}{l} \neg A \to B \\ B \to S \\ A \to C \\ \hline \therefore \neg C \to S \end{array}$$

Resolução. Vejamos

passo	*proposição*	*justificativa*
1.	$\neg A \to B$	premissa
2.	$B \to S$	premissa
3.	$A \to C$	premissa
4.	$\neg C \to \neg A$	contrapositiva de 3
5.	$\neg C \to B$	Silogismo hipotético de 4 e 1
6.	$\neg C \to S$	Silogismo hipotético de 5 e 2

□

Exercício 9. Preste atenção nesse caso:

$$\begin{array}{l} \text{se } \sqrt{2} > 3/2 \text{ então } 2 > 9/4 \\ \sqrt{2} > 3/2 \\ \hline \therefore 2 > 9/4 \end{array}$$

o argumento é válido?

Exercício 10. Verifique a validade das seguintes regras de inferência:

9. **Resolução** $\dfrac{A \vee B \quad \neg A \vee C}{\therefore B \vee C}$

10. **Prova por casos** $\dfrac{A \to B \quad C \to B \quad A \vee C}{\therefore B}$

Regras de inferência para quantificadores

11. **Instanciação universal** Se $\forall x \in D,\ P(x)$ é uma premissa, então deduzimos $P(c)$ para qualquer que seja c elemento do domínio D

$$\frac{\forall x \in D, P(x)}{\therefore P(c)}$$

12. **Generalização universal** Se $P(c)$ para um elemento *c arbitrário* do domínio D é premissa, então deduzimos $\forall x \in D,\ P(x)$

$$\frac{P(c) \text{ para } c \text{ arbitrário}}{\therefore \forall x \in D, P(x)}$$

Exemplo 11. Consideremos a sentença aberta $n^2 = n$. Usando a generalização universal para $c = 0$

$$\frac{0^2 = 0}{\therefore \forall n \in \mathbb{N},\ n^2 = n}$$

o que não é válido porque 0 não é um elemento *arbitrário*.

13. **Instanciação existencial** Se $\exists x \in D,\ P(x)$ é premissa, então deduzimos $P(c)$ para algum elemento c do domínio D

$$\frac{\exists x \in D, P(x)}{\therefore P(c)}$$

14. **Generalização existencial** Se $P(c)$ para algum c particular em D é premissa, então deduzimos $\exists x \in D,\ P(x)$

$$\frac{P(c) \text{ para algum } c \text{ particular}}{\therefore \exists x \in D,\ P(x)}.$$

Por exemplo, o seguinte argumento é válido

$$\frac{\forall x(P(x) \to Q(x)) \quad \forall x(Q(x) \to R(x))}{\therefore \forall x(P(x) \to R(x))}$$

Vejamos

passo	*proposição*	*justificativa*
1.	$\forall x(P(x) \to Q(x))$	premissa
2.	$\forall x(Q(x) \to R(x))$	premissa
3.	$P(c) \to Q(c)$	instanciação universal de 1
4.	$Q(c) \to R(c)$	instanciação universal de 2
5.	$P(c) \to R(c)$	Silogismo hipotético de 3 e 4
6.	$\forall x(P(x) \to R(x))$	generalização universal.

Da regra da conjunção podemos mostrar que

$$\exists x \in D, (P(x) \wedge Q(x)) \Rightarrow (\exists x \in D, P(x)) \wedge (\exists x \in D, Q(x)).$$

Vejamos

passo	*proposição*	*justificativa*
1.	$\exists x, (P(x) \wedge Q(x))$	premissa
2.	$P(c) \wedge Q(c)$	instanciação existencial de 1
3.	$P(c)$	simplificação de 2
4.	$Q(c)$	simplificação de 2
5.	$\exists x, P(x)$	generalização existencial de 3
6.	$\exists x, Q(x)$	generalização existencial de 4
7.	$(\exists x, P(x)) \wedge (\exists x, Q(x))$	conjunção.

No próximo exercício suponha que há um domínio associado sem se preocupar com o que de fato é tal conjunto (pode ser o conjunto de todos os animais conhecidos, por exemplo).

Exercício 12 (Lewis Carrol). Verfique se o seguinte argumento é válido:

Todos os leões são selvagens.
Alguns leões não bebem café.

Portanto, alguma criatura selvagem não bebe café.

Solução. Consideremos Matata um elemento do domínio.

passo	*proposição*	*justificativa*
1.	$\forall x, (L(x) \to S(x))$	premissa
2.	$\exists x, (L(x) \wedge \neg C(x))$	premissa
3.	$L(\text{Matata}) \wedge \neg C(\text{Matata}))$	instanciação universal de 2
4.	$L(\text{Matata})$	simplificação de 3
5.	$\neg C(\text{Matata})$	simplificação de 3
6.	$(L(\text{Matata}) \to S(\text{Matata}))$	instanciação universal de 1
7.	$S(\text{Matata})$	Modus Ponens de 4 e 6
8.	$S(\text{Matata}) \wedge \neg C(\text{Matata})$	conjunção de 5 e 7
9.	$\exists x(S(x) \wedge \neg C(x))$	generalização existencial

□

Exercício 13 (*Modus ponens* universal). Verifique se o seguinte argumento que combina instanciação universal com *Modus Ponens* é válido:

$$\begin{array}{l} \forall x(P(x) \to Q(x)) \\ P(a) \\ \hline \therefore Q(a) \end{array}$$

Exercícios

1. Sejam P e Q as sentenças "a eleição foi decidida" e "os votos foram contados", respectivamente. Expresse cada uma das sentenças simbólicas abaixo como uma sentença em português
   (a) $\neg P$
   (b) $\neg(P) \wedge Q$
   (c) $(\neg P) \to (\neg Q)$
   (d) $(\neg Q) \vee ((\neg P) \wedge Q)$
2. Considere que P, $\neg Q$ e R sejam sentenças verdadeiras. Verifique quais das afirmações são verdadeiras.
   (a) $P \to Q$
   (b) $Q \to P$
   (c) $P \to (Q \vee R)$
   (d) $P \leftrightarrow Q$
   (e) $P \leftrightarrow R$
   (f) $(P \vee Q) \to P$
3. Verifique que

(a) há casos em que $P \to Q$ é verdadeira, mas sua *recíproca* $Q \to P$ é falsa; e vice-versa;

(b) há casos em que $P \to Q$ é verdadeira, mas sua *inversa* $(\neg P) \to (\neg Q)$ é falsa;

(c) a sentença $P \to Q$ e sua *contrapositiva* $(\neg Q) \to (\neg P)$ têm sempre o mesmo valor lógico.

4. A sentença $(A \to B) \wedge (A \to \neg B)$ é uma contradição?

5. Escreva as afirmações abaixo na forma simbólica, definindo e atribuindo símbolos aos predicados e definido os domínios dos quantificadores.

(a) Todos os estudantes gostam de lógica.

(b) Alguns estudantes não gostam de lógica.

(c) Cada pessoa tem uma mãe.

(d) Entre todos os inteiros exitem alguns que são primos.

(e) Um dia do próximo mês é domingo.

(f) Alguns inteiros são pares e divisíveis por 3.

(g) Alguns inteiros são pares ou divisíveis por 3.

(h) $x^2 - 14 = 0$ tem uma solução positiva.

(i) Toda solução de $x^2 - 14 = 0$ é positiva.

(j) Nenhuma solução de $x^2 - 14 = 0$ é positiva.

(k) Existe algum estudante de direito que não é brasileiro.

(l) Todo estudante de direito tem um celular.

(m) Ninguém é perfeito.

(n) Alguém é perfeito.

(o) Todos os nossos amigos são perfeitos.

(p) Algum de nossos amigos é perfeito.

(q) Todos são nossos amigos e são perfeitos.

(r) Ninguém é nosso amigo ou alguém não é perfeito.

6. Sejam $\mathbb{N}$ o conjunto dos números naturais, e suponha que $P(x)$ significa " x é par", $Q(x)$ significa "x e divisível por 3", $R(x)$ significa "x e divisível por 4" e $S(x, y)$ é "x + 2 > y". Escreva em português cada uma das sentenças a seguir, e determine seu valor lógico:

(a) $(\forall x \in \mathbb{N}) P(x)$.

(b) $(\forall x \in \mathbb{N})(P(x) \vee Q(x))$.

(c) $(\forall x \in \mathbb{N})(P(x) \to Q(x))$.

(d) $(\forall x \in \mathbb{N})(P(x) \vee R(x))$.

(e) $(\forall x \in \mathbb{N})(P(x) \wedge R(x))$.

(f) $(\forall x \in \mathbb{N})(R(x) \to P(x))$.

(g) $(\forall x \in \mathbb{N})(P(x) \to \neg Q(x))$.

(h) $(\forall x \in \mathbb{N})(P(x) \to P(x+2))$.

(i) $(\forall x \in \mathbb{N})(R(x) \to R(x+4))$.

(j) $(\forall x \in \mathbb{N})(Q(x) \to Q(x+1))$.

(k) $(\exists x \in \mathbb{N}) R(x)$

(l) $(\exists x \in \mathbb{N})(P(x) \vee Q(x))$.

(m) $(\exists x \in \mathbb{N})(P(x) \to Q(x))$.

(n) $(\exists x \in \mathbb{N})(Q(x) \to Q(x+1))$.

(o) $(\exists x \in \mathbb{N})(P(x) \to Q(x+1))$.

(p) $(\exists x \in \mathbb{N})(\forall y \in \mathbb{N}) S(x, y)$.

(q) $(\exists x \in \mathbb{N})(\exists y \in \mathbb{N})S(x,y)$.

(r) $(\exists y \in \mathbb{N})(\forall x \in \mathbb{N})S(x,y)$.

7. Verifique as equivalências e implicações lógicas notáveis, dadas nas tabelas 1.4 (página 10) e 1.3 (página 9).

8. Verifique as seguintes equivalência lógicas, para provas por contradição.

$$\begin{aligned}(P \to Q) &\Leftrightarrow ((P \wedge \neg Q) \to (R \wedge \neg R))\\ (P \to Q) &\Leftrightarrow ((P \wedge \neg Q) \to \neg P)\\ (P \to Q) &\Leftrightarrow ((P \wedge \neg Q) \to Q)\end{aligned}$$

9. Para cada sentença determine o valor verdade e a negação. Na negação, expresse em símbolos a sentença usando as equivalências lógicas para a negação de quantificadores.

(a) $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 < m)$.

(b) $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n < m^2)$.

(c) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x = y^2)$.

(d) $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 0)$.

(e) $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 + m^2 = 25)$.

(f) $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 4 \wedge n - m = 2)$.

(g) $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(\exists p \in \mathbb{N})(p = \frac{n+m}{2})$.

(h) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(xy = 0)$

(i) $(\forall x \in \mathbb{R})(x \neq 0) \to (\exists y \in \mathbb{R})(xy = 1)$.

(j) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(y \neq 0 \to (xy = 1))$.

(k) $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(x + 2y = 2 \wedge 2x + 4y = 5)$.

(l) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 2 \wedge 2x - y = 1)$.

10. Considere $G(x,y)$ como "x gosta de y". Expresse em símbolos as sentenças

(a) todo mundo gosta de todo mundo

(b) todo mundo gosta de alguém

(c) alguém gosta de todo mundo

(d) alguém gosta de alguém

11. A sentença $\forall x \in X,\ A(x)$ é falsa se e somente se $\exists x \in X,\ \neg A(x)$ é verdadeira, ou seja, a sentença $\forall x \in X,\ A(x)$ é falsa se e somente se podemos encontrar um $x_0 \in X$ tal que $A(x_0)$ é uma sentença falsa. Tal x_0 é chamado de contraexemplo para $\forall x \in X,\ A(x)$. Determine um contraexemplo para:

(a) $\forall x \in \mathbb{R},\ |x| \neq 0$;

(b) $\forall x \in \mathbb{R},\ x^2 > x$;

(c) $\forall x \in \mathbb{N},\ x^2 \geqslant x$;

(d) $\forall x \in \{3,5,7,9\},\ x + 3 \geqslant 7$;

(e) $\forall x \in \{3,5,7,9\},\ x$ é primo.

12. Verifique se cada argumento abaixo é um argumento válido.

(a)
$$\frac{\begin{array}{c}A \to B\\ A \to C\end{array}}{\therefore A \to (B \wedge C)}$$

(b)
$$\frac{\begin{array}{l}\neg R(c)\\ \forall t \in D(P(t) \to Q(t))\\ \forall t \in D(Q(t) \to R(t))\end{array}}{\therefore \neg P(c)}$$

13. Dê a justifcativa para cada passo dos argumentos abaixo para que seja válido.

    (a) $(P \wedge (P \to Q) \wedge (S \vee R) \wedge (R \to \neg Q)) \Rightarrow (S \vee T)$

    (b) $((P \to Q) \wedge (\neg R \vee S) \wedge (P \vee R)) \Rightarrow (\neg Q \to S)$

    (c)

passo	*justificativa*
1) P	
2) $P \to Q$	
3) Q	
4) $R \to \neg Q$	
5) $Q \to \neg R$	
6) $\neg R$	
7) $S \vee R$	
8) S	
9) $S \vee T$	

    (d)

passo	*justificativa*
1) $\neg(\neg Q \to S)$	
2) $\neg Q \wedge \neg S$	
3) $\neg S$	
4) $\neg R \vee S$	
5) $\neg R$	
6) $P \to Q$	
7) $\neg Q$	
8) $\neg P$	
9) $P \vee R$	
10) R	
11) $\neg R \wedge R$	
12) $\neg Q \to S$	

14. Uma argumento não é válido se é possível que as premissas sejam verdadeiras e a conclusão falsa. Mostre que os seguintes argumentos não são válidos exibindo valores-lógicos para as sentenças P, Q, R, S de modo que as premissas são verdadeiras mas a conclusão é falsa.

    (a)
    $$\begin{array}{ll} & P \leftrightarrow Q \\ & Q \to R \\ & R \vee \neg S \\ & \neg(S) \to Q \\ \hline \therefore & S \end{array}$$

    (b)
    $$\begin{array}{ll} & P \\ & P \to R \\ & P \to (Q \vee \neg R) \\ & \neg(Q) \vee \neg(S) \\ \hline \therefore & S \end{array}$$

15. Verifique que valem as equivalências e consequências lógicas abaixo.

    (a) $\forall x \in D(P(x) \wedge Q(x)) \Leftrightarrow (\forall x \in D, P(x)) \wedge (\forall x \in D, Q(x))$.

    (b) $(\forall x \in D, P(x)) \vee (\forall x \in D, Q(x)) \Rightarrow \forall x \in D(P(x) \vee Q(x))$.

    (c) $\exists x \in D, (P(x) \vee Q(x)) \Leftrightarrow (\exists x \in D, P(x)) \vee (\exists x \in D, Q(x))$.

    (d) $\exists x \in D, (P(x) \wedge Q(x)) \Rightarrow (\exists x \in D, P(x)) \wedge (\exists x \in D, Q(x))$.

16. Escreva os seguinte argumentos na forma simbólica, estabeleça sua validade ou dê um contraexemplo para mostrar que é inválido.

    (a) "Se Raquel consegue posto de supervisor e trabalha duro, ela ganhará um aumento. Se ela receber o aumento, então ela vai comprar um carro novo. Ela não comprou um carro novo. Portanto, ou Raquel não conseguiu o posto de supervisor ou ela não trabalhou duro."

(b) "Se Dominic for para a pista, Helen ficará louca. Se Ralph jogar cartas a noite toda, então Carmela ficará louca. Se Helen ou Carmela ficarem loucas, então Veronica (a advogada delas) será notificada. Verônica não teve notícias de nenhum desses dois clientes. Portanto, Dominic não chegou à pista e Ralph não jogou cartas a noite toda."

(c) "Se há uma possibilidade de chuva ou sua camisa vermelho está lavando, Luiz não cortará sua grama. Sempre que a temperatura é superior a 25ºC, não há chance de chuva. Hoje a temperatura é de 30ºC e Luiz está usando sua camisa vermelha. Portanto, hoje Luiz cortará a grama."

1.2 A teoria dos conjuntos de Zermelo–Fraenkel

A elegante teoria dos conjuntos desenvolvida por Ernest Zermelo (1871–1953) e Abraham Fraenkel (1891–1965) e que teve importantes contribuições de outros outros, conquistou a matemática moderna que fez dela um dos seus pilares fundamentais. A ideia por trás dessa fundamentação é considerar que todos os objetos é estruturas ma temáticas são definíveis como conjuntos, números, conjuntos, elementos dos conjuntos, tudo é conjunto. A teoria foi batizada como sistema ZFC em homenagem a Zermelo e Fraenkel, a letra C vem do inglês *choice* em referência ao axioma da escolha, que levanta polêmica entre alguns matemáticos.

1.2.1 Abordagem intuitiva da teoria dos conjuntos

Conjunto é informalmente entendido como uma *coleção* de entidades, ou objetos, chamados de **elementos** do conjunto e eles mesmos podem ser conjuntos. Um elemento x **pertence** ao conjunto A se x é um elemento de A o que é denotado por

$$x \in A$$

e escrevemos a negação como $x \notin A$.

Essa sentença não define conjunto, ela é circular pois usa o termo *coleção* que é sinônimo de conjunto e não esclarece o que são objetos. Não definimos conjunto e assumimos que todos têm alguma noção, mesmo que possivelmente errada, da concepção de conjuntos.

Axiomas e termos indefinidos são inevitáveis em um tratamento rigoroso da matemática. A abordagem moderna em matemática aceita a existência de termos indefinidos, desde que sejam usados adequadamente. Em última análise, objetos indefinidos não nos incomodam, porque tais objetos não existem em si mesmos, pois são determinados pelas propriedades axiomáticas hipotetizadas para eles, e são essas propriedades que usamos nas provas.

Convencionamos usar letras maiúsculas para conjuntos e minúsculas para elementos. Entretanto, um conjunto pode ser elemento de outro conjunto assim, um conjunto representado por uma letra minúscula deve ser entendido como um elemento de algum outro conjunto.

Igualdade de conjuntos *Dois conjuntos são iguais se, e somente se, têm os mesmos elementos.* Ou seja, a única propriedade distintiva de um conjunto é sua lista de membros.

Conjunto vazio *Há um (único) conjunto sem elementos, denotado por $\varnothing$ e chamado de conjunto vazio.*

Especificação de conjuntos Da igualdade de conjuntos podemos inferir que especificar todos os elementos de um conjunto é suficiente para defini-lo, podemos fazer isso de diversas formas.

Se um conjunto tem poucos elementos, podemos listá-los entre chaves "{}" separados por vírgulas. Por exemplo, o conjunto dos algarismos primos é formado pelos números inteiros 2, 3, 5 e 7 e escrevemos $\{2,3,5,7\}$. O conjunto dos algarismos indo-arábicos é $\{0,1,2,3,4,5,6,7,8,9\}$.

Quando os conjuntos têm muitos elementos não é viável escrever todos seus elementos e uma solução comum, mas que só usamos quando o contexto não dá margem a ambiguidade sobre seu significado, é o uso de reticências (...). Por exemplo, o conjunto dos naturais menores que 2.017 é descrito por $\{0,1,\ldots,2.016\}$; o conjunto das letras do alfabeto $\{a,b,c,\ldots,z\}$; o conjunto dos naturais pares $\{0,2,4,6,\ldots\}$. No geral é preciso muito cuidado e a recomendação é que essa solução deve ser evitada pois, por exemplo, o que é o conjunto $\{3,5,7,\ldots\}$?

Exercício 14. Encontre duas respostas factíveis para a pergunta acima.

Além de listar os elementos de um conjunto explicitamente, também podemos definir conjunto por *especificação* (também chamado de *seleção*), onde damos uma regra de como gerar todos os seus elementos. Podemos especificar um conjunto através de uma ou mais propriedade de seus elementos e, nesse caso, usamos a notação como

$$A = \{\, x \in D \colon P(x) \,\}$$

em que P é um predicado (sentença aberta). Assim, $a \in A$ é verdadeiro se, e só se, a é um elemento do domínio D para o qual $P(a)$ é verdadeiro. Por exemplo, $\{x \in \mathbb{R}\colon x^2 \leq 2\}$ corresponde ao intervalo fechado da reta real composto pelo números cujo quadrado é no máximo 2, ou ainda,o intervalo $[-\sqrt{2}, \sqrt{2}]$; o conjunto dos números naturais primos é o conjunto dos números naturais maiores que 1 que não têm divisores além do 1 e do próprio número. Essa sentença pode ser escrita como "se $x = yz$ então $y = 1$ ou $z = 1$ de modo que o conjunto dos números primos é especificado por

$$\big\{x \in \mathbb{N}\colon x > 1 \text{ e para todo } y \text{ e todo } z \text{ naturais, se } yz = x \text{ então } y = 1 \text{ ou } z = 1)\big\}.$$

ou, em símbolos, $\big\{x \in \mathbb{N}\colon \text{ e } x > 1 \text{ e } \forall y \in \mathbb{N}, \forall z \in \mathbb{N}(yz = x \to y = 1 \text{ ou } z = 1)\big\}$.

Há ainda um esquema de substituição, uma descrição parametrizada usada para os elementos de um conjunto. Nesse caso, se f é uma função com um domínio que inclui o conjunto D então formamos o conjunto dos $f(x)$ tal que $x \in D$. Por exemplo, o conjunto dos inteiros ímpares é dado por

$$\{2k+1\colon k \in \mathbb{Z}\}.$$

Observamos que $\{2,3,5,7\}$ pode ser especificado. Observamos também que os elementos de um conjunto podem, eles mesmos, serem conjuntos

$$X = \{\{a\},\{b\},\{c\}\}.$$

Observamos, ainda, que conjuntos não contêm elementos repetidos e não existe ordem na descrição dos elementos.

$$\begin{aligned}\{1,1,1\} &= \{1\}\\ \{1,2,1,1\} &= \{1,2\}\\ \{1,2,3\} &= \{1,3,2\} = \{2,3,1\} = \{2,1,3\} = \ldots\end{aligned}$$

Paradoxo de Russell A definição de um conjunto pode usar outros conjuntos e, nesse caso, deve-se tomar cuidado para evitar definições autorreferentes, ou circulares, que podem não ter sentido. Um exemplo clássico: *o que é o conjunto* $S = \{x : x \notin x\}$*?,* $S \in S$*?* Conhecido pelo nome Paradoxo de Russell, teve um papel muito importante no desenvolvimento da teoria de conjuntos.

Inclusão e conjunto das partes

O conjunto A é **subconjunto** de um conjunto B, fato denotado por $A \subset B$ se, e só se, é verdadeira a sentença "todo elemento de A é elemento de B", ou seja, para todo x

$$x \in A \Rightarrow x \in B.$$

Usamos $A \subseteq B$ para expressar $A \subset B$ e usamos $A \subsetneq B$ para expressar $A \subset B$ e $A \neq B$, nesse caso dizemos que é **subconjunto próprio** de B. A negação de $A \subset B$, *A não é subconjunto* de B, é escrita como $A \not\subset B$.

Observemos que

$$\begin{aligned}A \not\subset B \quad &\Leftrightarrow \quad \text{não}\big(\text{ para todo } x\,(x \in A \to x \in B)\big)\\ &\Leftrightarrow \quad \text{existe } x, \text{ não}(x \in A \to x \in B)\\ &\Leftrightarrow \quad \text{existe } x\,(x \in A \text{ e } x \notin B),\end{aligned}$$

ou seja, $A \not\subset B$ se e somente se há um elemento de A que não pertence a B. Também, é verdade que $A = B$ e e somente se $A \subset B$ e $B \subset A$ e, assim, $A \neq B$ se e somente se $A \not\subset B$ ou $B \not\subset A$.

O nosso primeiro resultado sobre conjuntos é o seguinte.

Teorema 15 *Para qualquer conjunto A, $\varnothing \subset A$.*

Demonstração. Seja A um conjunto qualquer. A condicional

$$\text{se } x \in \varnothing \text{ então } x \in A$$

é verdadeira para todo x pois $x \in \varnothing$ é falso. Como A é arbitrário, $\varnothing \subset A$ para todo A. □

Exercício 16. Verifique se é verdadeiro ou não: se $A \subset B$ e $B \subset C$, então $A \subset C$, para quaisquer conjuntos A, B e C.

O **conjunto das partes de** A, isto é, conjunto formado por todos os subconjuntos de A. Algumas referências usam $\wp(A)$ (ou $\mathscr{P}(A)$) para denotá-lo. Aqui usaremos, preferencialmente, 2^A.

Exercício 17. Descreva o conjunto das partes do conjunto vazio. Descreva o conjunto das partes do conjunto $\{a\}$.

Operações sobre conjuntos

As operações sobre conjuntos definem novos conjuntos. A seguir descrevemos as quatro operações mais usuais e suas propriedades.

União $A \cup B$ denota a união dos conjuntos A e B que é o conjunto dos elementos que pertencem a A ou a B

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

Intersecção $A \cap B$ denota a intersecção dos conjuntos A e B que é o conjunto dos elementos que pertencem a A e a B

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

Diferença $A \setminus B$ denota o conjunto dos elementos pertencem a A e não a B

$$A \setminus B = \{x\colon\ x \in A \text{ e } x \notin B\}.$$

Diferença simétrica $A \triangle B$ denota o conjunto dos elementos que pertencem exclusivamente a A ou a B mas não a ambos

$$A \triangle B = \{x\colon\ x \in A \cup B \text{ e } x \notin A \cap B\}.$$

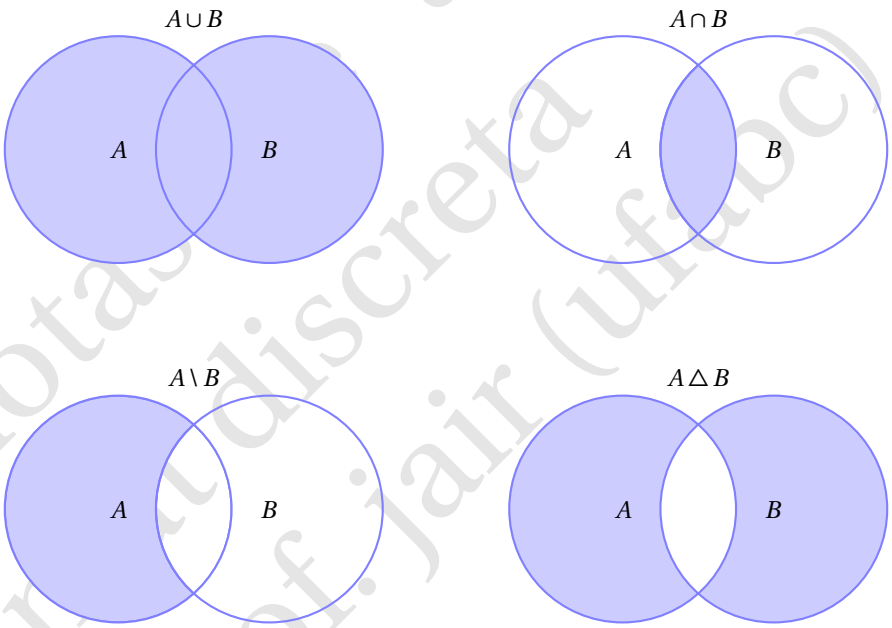


Figura 1.1: Diagrama de Venn das operações sobre conjuntos.

Fica como exercício a verificação das propriedades descritas na tabela 1.5 abaixo. Algumas delas seguem das equivalências lógicas notáveis, exercício 7, página 16 (as outras seguem de alguma equivalência lógica que você deve provar).

Exercício 18. Verifique que para quaisquer conjuntos A e B as duas inclusões abaixo são verdadeiras

$$A \cap B \subset A \subset A \cup B.$$

Exercício 19. Seja R um conjunto cujos elementos são conjuntos. Denote por $\bigcup R$ a união dos elementos de R, por exemplo, se $A = \{a, b, c\}$, então $\bigcup A = a \cup b \cup c$. Tome $R = \{\{\{1\}, \{1,2\}\}, \{\{1\}, \{1,3\}\}, \{\{2\}, \{2,3\}\}\}$ e descreva os conjuntos $\bigcup R$ e $\bigcup\bigcup R$.

Identidade	$A \cap (C \setminus A) = \varnothing$ $A \cup \varnothing = A$ $A \cap \varnothing = \varnothing$
Idempotência	$A \cup A = A$ $A \cap A = A$
Distributiva	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Comutativa	$A \cap B = B \cap A$ $A \cup B = B \cup A$
Associativa	$A \cap (B \cap C) = (A \cap B) \cap C$ $A \cup (B \cup C) = (A \cup B) \cup C$
Absorção	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$
De Morgan	$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$ $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$

Tabela 1.5: Propriedades das operações.

Partição de um conjunto

Dizemos que A e B são conjuntos **disjuntos** se $A \cap B = \varnothing$.

Se X é um conjunto, então dizemos que o conjunto P é uma **partição** de X se:

1. para todo $a \in P$, $a \in 2^X \setminus \{\varnothing\}$; em outras palavras, todo elemento de P é um subconjunto não vazio de X.
2. Para todo $a \in P$ e todo $b \in P$, se $a \neq b$ então $a \cap b = \varnothing$; em outras palavras, quaisquer dois elementos distintos de P são disjuntos.
3. $\bigcup P = X$; em outras palavras, a união dos elementos de P é exatamente X.

Exercício 20. Seja $\mathbb{Z}$ o conjunto dos números inteiros. Para cada $i \in \{0,1,2\}$ denote por R_i o subconjunto dos números inteiros que deixam resto i quando divididos por 3. Prove que $\{R_0, R_1, R_2\}$ é uma partição de $\mathbb{Z}$.

1.2.2 Abordagem axiomática (mas ainda intuitiva) da teoria dos conjuntos

A teoria axiomática dos conjuntos utilizada na matemática é formalizada a partir de uma coleção de axiomas que nos permitem construir, essencialmente a partir do zero, um universo grande o suficiente para manter toda a matemática sem contradições aparentes, evitando os paradoxos que podem surgir na teoria intuitiva dos conjuntos. Vamos descrever os dez axiomas usuais da teoria ZFC abaixo, esses axiomas garantem a existência de conjuntos específicos ou permite construir conjuntos a partir de outros conjuntos.

Os axiomas da ZF são adequadamente formulados na linguagem da lógica clássica de primeira ordem, mas aqui os axiomas são descritos informalmente. Lembremos que na teoria axiomática (formal) tudo é conjunto, a ideia é que podemos representar qualquer entidade matemática como conjunto.

Axioma do vazio Existe um conjunto que não tem elementos. Na linguagem formal[3]

$$\exists a \forall x (x \notin a).$$

Esse conjunto sem elementos é o conjunto vazio.

Axioma da extensionalidade Quaisquer dois conjuntos com os mesmos elementos são iguais.

$$\forall a \forall b ((a = b) \leftrightarrow \forall x (x \in a \leftrightarrow x \in b)).$$

Por esse axioma o conjunto vazio é único. Se existissem x e y conjuntos vazios diferentes, então pelo axioma da extensão existiria um elemento de x que não pertenceria a y ou um elemento de y não em x. Em ambos os casos há contradição ao fato de x e y serem vazios. Como o vazio é único podemos atribuir-lhe uma representação, que é o clássico $\varnothing$.

[3] Na linguagem formal as variáveis intencionam representar conjuntos, por isso nessa parte do texto, e só nela, conjuntos aparecem representados por letras minúsculas.

Axioma do par Dados conjuntos y e z, existe um conjunto a tal que se $x \in a$ então $x = y$ ou $x = z$. Pelo axioma anterior esse conjunto é único, é o conjunto $\{y, z\}$.

$$\forall y \forall z \exists a \forall x (x \in a \leftrightarrow (x = y \text{ ou } x = z)).$$

Axioma da união Para qualquer conjunto z existe um conjunto $\bigcup z$ tal que $y \in \bigcup z$ se, e só se, $y \in w$ para algum $w \in z$. De modo bem informal, se $z = \{a, b, c, \ldots\}$ então $a \cup b \cup c \cup \cdots$ é um conjunto.

$$\forall z \exists a \forall x (x \in a \leftrightarrow \exists y (x \in y \text{ e } y \in z)).$$

Assim, dados os conjuntos x e y temos o conjunto $\{x, y\}$, como vimos acima, e agora temos $\bigcup\{x, y\}$, ou seja, $x \cup y$.

Axioma das partes Para qualquer conjunto y, existe o conjunto a tal que $x \in a$ se, e só se, $x \subset y$.

$$\forall y \exists a \forall x (x \in a \leftrightarrow \forall z (x \in x \to z \in y)).$$

O conjunto a é único e é o conjunto das partes de y.

Axioma da especificação De um conjunto y e um predicado P onde a não ocorre livre, formamos o conjunto $a = \{x \in y \colon P(x)\}$

$$\forall y \exists a \forall x (x \in a \leftrightarrow (x \in y \text{ e } P(x))).$$

Esse axioma também é chamado de compreensão, separação ou seleção pois estamos "selecionando" do conjunto y os elementos que satisfazem P. Em $P(x)$ a variável x aparece livre e a não, para evitar auto referência que levaria ao paradoxo de Russel, por exemplo.

Exercício 21. Qual é a consequência de tomarmos por P a fórmula $x \neq x$? E se P for a fórmula $x \notin a$, assumindo que a pode ocorrer livre em P (faça $y = \{\varnothing\}$ e $x = \varnothing$)?

Notemos a definição de união como foi dada ingenuamente, $\{x \colon x \in A \text{ ou } x \in B\}$, não se enquadra nesses axiomas. Por outro lado, podemos formar $\{x \in A \colon x \in B\}$ que é $A \cap B$, a especificação permite escrever a intersecção. Ainda, se x é não vazio então $\bigcap x$, a intersecção dos elementos de x é

$$\left\{y \in \bigcup x \colon \forall z \in x, y \in z\right\}.$$

De fato, especificação não é um axioma, mas um esquema de axiomas, um para cada predicado que pode ser escrito na linguagem formal da teoria dos conjuntos.

Por fim, como já dissemos, note-se a forma diferente com que se escreve um conjunto por especificação, com respeito a teoria intuitiva. Agora não temos mais o paradoxo de Russell pois se

$$S = \{x \in A \colon x \notin x\}$$

então $S \in S$ se e só se $S \in A$ e $S \notin S$ o que não é contraditório, a conclusão é que $S \notin A$. Como subproduto temos o fato já mencionado de que em teoria dos conjuntos *não há conjunto universo*.

$$\neg \exists y \forall x (x \in y).$$

De fato, se existisse então tomaríamos-o por A no argumento acima o que daria uma contradição pois $S \notin A$.

Axioma da infinidade Assegura a existência de um conjunto infinito: existe um conjunto que tem $\varnothing$ como elemento e, se x é elemento, também é $x \cup \{x\}$

$$\exists a (\varnothing \in a \text{ e } \forall x (x \in a \to x \cup \{x\} \in a))$$

Um conjunto I que tem $\varnothing$ como elemento e também $x \cup \{x\}$ sempre que $x \in I$ é chamado de **conjunto indutivo**. Essa construção nos dá uma codificação dos números naturais na teoria dos conjuntos: $\varnothing$ representa 0 e $x \cup \{x\}$ representa $x + 1$. Efetivamente, estabelece cada número natural como o conjunto de todos números menores, e.g., $0 = \varnothing$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, essa definição de números naturais é atribuída ao matemático John von Neumann.

Axioma da fundação (ou da regularidade) Cada conjunto não vazio a tem um elemento b com $a \cap b = \varnothing$.

$$\forall a(a \neq \varnothing \rightarrow \exists b(b \in a \text{ e } a \cap b = \varnothing)).$$

Esse axioma evita construções "estranhas" como $x \in x$ e sequências infinitas da forma $x_1 \ni x_2 \ni x_3 \ni \cdots$, ou seja, garante que todo conjunto não-vazio possui um elemento $\in$-minimal. Isso significa que o axioma garante que a pertinência "é bem fundada" (em analogia à definição 142, na página 73).

Se x e y são conjuntos, então também é $z = \{x, y\}$ e, ainda, $z \neq \varnothing$. Então ou $x \cap z = \varnothing$ ou $y \cap z = \varnothing$, portanto, $y \notin x$ ou $x \notin y$. Disso concluímos que não existem conjuntos x e y tais que $x \in y$ e $y \in x$ e, feito $x = y$ concluímos que não existe x tal que $x \in x$.

O próximo axioma é controverso para alguns matemáticos (e.g., os matemáticos construtivistas[4]) e até hoje quando usado é explicitamente mencionado. Ainda mais, a bibliografia faz referência aos sistemas ZFC e ZF para a teoria dos conjuntos, dependendo de se o axioma da esclha ("C", de *choice*) é considerado ou não.

Embora seu enunciado pareça coerente há alguns enunciados equivalentes, ou decorrentes dele, que não são intuitivos como, por exemplo, o paradoxo de Banach–Tarski[5]. Por outro lado, a quantidade de resultados importantes na matemática, como o Teorema de Hahn–Banach e a existência de base para espaços vetoriais, que usam o axioma da escolha o tornam imprescindível; alguns deles são, de fato, equivalentes ao axioma da escolha, como o princípio da boa-ordem: *todo conjunto admite uma boa ordem* (veremos mais sobre isso a partir da página página 64) . Em particular, segue daí a afirmação de que os números reais podem ser ordenado de modo que qualquer subconjunto não vazio contenha um menor elemento.

Axioma da escolha Para todo conjunto x de conjuntos não vazios e dois-a-dois disjuntos existe um conjunto z que tem exatamente um elemento em comum com cada conjunto de x.

O conjunto z "escolhe" um elemento de cada y em x. Esse axioma tem um enunciado equivalente que usa uma função (conceito que ainda precisa ser definido na teoria) chamada de *função escolha. Para qualquer conjunto x formado de conjuntos não-vazios, existe uma função* $f\colon x \rightarrow \bigcup x$ *que atribui para cada* $y \in x$ *uma imagem* $f(y) \in y$.

Uma observação importante é que, embora f "escolha" um elemento de cada elemento de x, o axioma nada diz respeito de como se faz isso, sobre a existência de um procedimento efetivo para realizar uma escolha.

Para concluir, o último axioma da teoria diz que qualquer coisa razoável que fizermos com os elementos de um conjunto resulta num conjunto, é um axioma importante para a definição de ordinais.

Axioma da substituição Dado um conjunto x e um predicado $R(s,t)$ com a propriedade $\forall s \exists! t R(s,t)$, existe o conjunto z tal que $y \in z$ se, e só se, existe $w \in x$ para o qual $R(w,y)$ é verdadeiro.

1.2.3 Par ordenado e Produto cartesiano

Nesta seção definimos o produto cartesiano de dois conjuntos dados a partir dos axiomas.

Dados dois conjuntos não vazios A e B, tomemos um elemento qualquer de cada um, digamos $a \in A$ e $b \in B$. Pelo axioma do par $\{a, b\}$ é conjunto e por extensionalidade $\{a, b\} = \{b, a\}$.

Por **par ordenado** entendemos um par de elementos de modo que a ordem em que tais elementos se apresentam importa e, usualmente, denotamos-o por (a, b), de modo que $(a, b) \neq (b, a)$ exceto, possivelmente, quando $a = b$.

Denotamos por $A \times B$ o conjunto de todos os tais pares (a, b) com $a \in A$ e $b \in B$, isto é, intuitivamente

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

chamado de **produto cartesiano** de A com B. A seguir vamos definir o produto cartesiano (informalmente) dentro da teoria axiomática.

A definição mais simples de par ordenado em termos de conjunto foi dada pelo matemático polonês Kazimierz Kuratowski (1896–1980).

Definição 22. O par ordenado (a, b) é dado pelo conjunto $\{\{a\}, \{a, b\}\}$

$$(a, b) \coloneqq \{\{a\}, \{a, b\}\}$$

Agora, demonstramos que a definição acima faz o prometido, cumpre papel de definir par ordenado.

TEOREMA 23 *Se* $(a, b) = (x, y)$ *então* $a = x$ *e* $b = y$.

[4] Objetos matemáticos cuja existência depende do axioma da escolha não podem ser construídos explicitamente.

[5] Diz que, informalmente, existe uma forma de particionar uma esfera em uma quantidade finita de partes e remontar essas partes para formar duas esferas disjuntas, idênticas à primeira.

COROLÁRIO 24 *Se $a \neq b$ então $(a,b) \neq (b,a)$.*

Para provar o teorema usaremos o seguinte resultado auxiliar.

LEMA 25 *Se $\{a,x\} = \{a,y\}$ então $x = y$.*

DEMONSTRAÇÃO. Se $x = a$ então $y = a$, portanto $x = y$. Se $x \neq a$ e $\{a,x\} = \{a,y\}$, então $x \in \{a,y\}$, logo $x = a$ ou $x = y$. Portanto, $x = y$. □

Demonstração do teorema. A prova do teorema é por casos: em dois casos (1) $a = b$ e (2) $a \neq b$. Suponhamos que $(a,b) = (x,y)$, isto é, $\{\{a\},\{a,b\}\} = \{\{x\},\{x,y\}\}$.

Caso 1. Se $a = b$ então $(a,b) = \{\{a\}\}$ e temos as seguintes identidades[6]

$$\{\{x\},\{x,y\}\} = \{\{a\},\{a,b\}\} = \{\{a\}\}$$

de modo que $\{x\} = \{x,y\} = \{a\}$. Portanto $x = y$ e $x = a$, ou seja, $x = y = a = b$.

Caso 2. Se $\{\{a\},\{a,b\}\} = \{\{x\},\{x,y\}\}$ então $\{x\} \in \{\{a\},\{a,b\}\}$. Se $\{x\} \in \{\{a\},\{a,b\}\}$ então $\{x\} = \{a\}$ ou $\{x\} = \{a,b\}$. Se $a \neq b$ então $\{x\} = \{a\}$. Agora, se $\{\{a\},\{a,b\}\} = \{\{x\},\{x,y\}\}$ e $\{x\} = \{a\}$ então $\{x,y\} = \{a,b\}$, pelo lema acima. Se $\{x\} = \{a\}$ então $x = a$. Se $\{x,y\} = \{a,b\}$ e $x = a$, então $y = b$, pelo lema acima. Portanto $x = a$ e $y = b$. □

O corolário segue imediatamente do teorema.

Notemos que se $a \in A$ e $b \in B$ então $\{a\}$ e $\{a,b\}$ são conjuntos pelo axioma do par, o qual também nos dá que $\{\{a\},\{a,b\}\}$ é conjunto. Ainda, $\{a\} \in \wp(A \cup B)$ e $\{a,b\} \in \wp(A \cup B)$, portanto $\{\{a\},\{a,b\}\} \subset \wp(A \cup B)$, ou seja, $\{\{a\},\{a,b\}\} = (a,b) \in \wp(\wp(A \cup B))$, portanto, existe o conjunto cujos elementos são todos os pares (a,b) com $a \in A$ e $b \in B$, é o conjunto dada pela especificação

$$\left\{(x,y) \in \wp(\wp(A \cup B)) : x \in A \text{ e } y \in B \text{ e } z = (x,y)\right\}$$

sempre que A e B são ambos não vazio.

Como no produto cartesiano os pares são ordenados, temos que $A \times B \neq B \times A$ (exceto quando $A = B$ ou $A = \varnothing$ ou $B = \varnothing$).

1.2.4 Relações e Funções

Nesta seção definimos essas estruturas matemáticas importantes através de conjuntos. Um estudo mais específico de certos tipos de relações será apresentado mais adiante e em funções não nos aprofundaremos, contamos com algum conhecimento prévio do leitor.

Definição 26. Se A e B são conjuntos, uma **relação** com **domínio** A e **contradomínio** B é um subconjunto de um produto cartesiano $A \times B$. Se $A = B$ escrevemos A^2 para $A \times B$ e dizemos que $R \subset A^2$ é uma relação sobre A, ou em A. Se $R \subset A \times B$ e $(a,b) \in R$ escrevemos $a\,R\,b$.

Por exemplo, $<$ é uma relação sobre $\mathbb{N}$ e ao invés de escrevermos $(x,y) \in <$ escrevemos $x < y$, como em $3 < 4$ ao invés de $(3,4) \in <$.

Exemplo 27. Tomemos $A = \{1,2,3,4\}$ e consideremos

$$R = \{(1,1),(2,1),(2,2),(3,3),(3,2),(3,1),(4,4),(4,3),(4,2),(4,1)\} \subset A \times A.$$

O conjunto R é uma relação em A por definição. Desde que $(1,1) \in R$, temos $1\,R\,1$. Da mesma forma $2\,R\,1$ e $2\,R\,2$ e assim por diante. No entanto, por exemplo, $(3,4) \notin R$, então $3 \not R\, 4$. Agora, consideremos o seguinte conjunto:

$$S = \{(1,1),(1,3),(3,1),(3,3),(2,2),(2,4),(4,2),(4,4)\} \subset A \times A.$$

Aqui temos $1\,S\,1$, $1\,S\,3$, $4\,S\,2$, $3 \not S\, 4$ e $2 \not S\, 1$. Notemos que s pode ser entendido como significando "tem a mesma paridade que" no domínio da relação. Ademais

$$R \cap S = \{(1,1),(2,2),(3,3),(3,1),(4,4),(4,2)\} \subset A \times A$$

é uma relação em A. A expressão $x\,(R \cap S)\,y$ pode ser entendida com "$x \geq y$ e têm a mesma paridade"no domínio da relação.

Para uma relação genérica, usamos símbolos como $\sim$, $\equiv$, $\simeq$, $\approx$ em vez de R, S ou qualquer letra do alfabeto.

[6] Escrevemos $r = s = t$ com o significado de $r = s$ e $s = t$.

Funções

Definição 28. Uma relação $R \subset A \times B$ é uma **função** se para cada $x \in A$ existe um único $y \in B$ tal que $(x,y) \in R$, nesse caso escrevemos $R : A \to B$, o único y tal que $(x,y) \in R$ é denotado por $R(x)$ é dito *o valor que a função assume em x*. O conjunto de todas as função de A em B é um subconjunto de $\wp(A \times B)$ denotado por $\mathbf{B}^{\mathbf{A}}$.

Por exemplo, a função f que o axioma da escolha afirma existir é um subconjunto de $x \times \bigcup x$, ou seja, $f : x \to \bigcup x$, com a propriedade de que $f(y) \in y$, para todo $y \in x$.

Uma função $f : A \to B$ pode ou não ter uma (ou mais) das seguintes propriedades

injetividade se, e só se, é verdade que para todos $x, x' \in A$

$$\text{se } x \neq x' \text{ então } f(x) \neq f(x').$$

sobrejetividade se, e só se, é verdade que para todo $y \in B$, existe $x \in A$ tal que

$$f(x) = y.$$

bijetividade se, e só se, for injetiva e bijetiva, isto é, é vale a sentença

$$\forall y \in B \exists! x \in A,\ f(x) = y.$$

Composição e inversa de relações

As relações e funções podem ser *compostas*.

Dadas as relações $R \subset A \times B$ e $S \subset B \times C$ definimos a **relação composta**

$$(S \circ R) \subset A \times C$$

pela regra $(x,z) \in (S \circ R)$ se, e somente se, existe $y \in B$ tal que $(x,y) \in R$ e $(y,z) \in S$. Em notação usual

$$x\ (S \circ R)\ z \Leftrightarrow \exists y (x\ R\ y \wedge y\ S\ z)$$

Não é difícil ver que a composição ordinária de funções é um caso especial de composição de relação. Por exemplo, considere as relações

$$\begin{aligned} R &= \{(1,1),(1,4),(2,3),(3,1),(3,4)\} \\ S &= \{(1,0),(2,0),(3,1),(3,2),(4,1)\} \end{aligned}$$

A composição delas é

$$S \circ R = \{(1,0),(1,1),(2,1),(2,2),(3,0),(3,1)\}$$

Dada uma relação $R \subset A \times B$, a **relação inversa** é a relação R^{-1} em $B \times A$ definida a partir da equivalência

$$x\ R^{-1}\ y \text{ se e somente se } y\ R\ x.$$

Toda relação tem uma inversa, no entanto a inversa de uma função pode não ser função. Por exemplo, tome $A = \{1,2,3\}$ e

$$R = \{(1,2),(2,3),(3,3)\}$$

A relação inversa é

$$R^{-1} = \{(2,1),(3,2),(3,3)\}.$$

Ademais

$$\begin{aligned} R^{-1} \circ R &= \{(1,1),(2,2),(2,3),(3,2),(3,3)\} \\ R \circ R^{-1} &= \{(2,2),(3,3),(3,3)\} \end{aligned}$$

Exercício 29. Qual é a inversa da relação $<$ sobre $\mathbb{N}$?

Exercícios

1. Tome $A = \{1,\{1\},\{2\}\}$. Quais das afirmações a seguir são verdadeiras?

(a) $\varnothing \subset \{\varnothing\}$;
(b) $\varnothing \subset \varnothing$;
(c) $\varnothing \in \{\varnothing\}$;
(d) $\varnothing = \{\varnothing\}$;
(e) $\{\varnothing\} \subset \{\varnothing, \{\varnothing\}\}$;
(f) $\{\varnothing\} \in \{\varnothing, \{\varnothing\}\}$;
(g) $\{\varnothing\} = \{\varnothing, \{\varnothing\}\}$;
(h) $1 \in A$;
(i) $\{1\} \in A$;
(j) $\{2\} \in A$;
(k) $\{1\} \subset A$;
(l) $\{2\} \subset A$;
(m) $\{\{1\}\} \subset A$;
(n) $\{\{2\}\} \subset A$;
(o) $\{2\} \subsetneq A$;

2. Verifique cada uma das propriedades das operações de conjunto listas na tabela 1.5 usando equivalências lógicas.
3. Enuncie as leis de De Morgan no caso de união e interseção com mais de dois conjuntos.
4. Escreva o conjunto das partes de
   (a) $\{\varnothing\}$.
   (b) $\{1,2,3\}$;
   (c) $\{\{1\},\{2\},\{3\}\}$.
   (d) $\{\{1,2\},\{3\}\}$.
5. Tome $R = \{\{\{1\},\{1,2\},\{1,2,3\}\},\{\{\varnothing,\{1\},\{1,3\}\}\},\{\{\{\varnothing\},\{2\},\{2,3\}\}\}\}$ e escreva os conjuntos $\bigcup R$ e $\bigcup\bigcup R$.
6. Construa os seguintes conjuntos a partir dos axiomas da teoria ZFC. Dados os conjuntos A e B,
   (a) $A \cup B$;
   (b) todas as relações de A em B;
   (c) todas as funções de A em B.
7. Se $f \subset X \times Y$ é uma função e $B \subset Y$ então definimos
$$f^{-1}(B) = \{x \in X : f(x) \in B\}$$
   Verifique que
   (a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
   (b) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
   (c) $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$
8. Considere as seguintes relações sobre $\{0,1,2,3,4\}$
$$\begin{aligned} R &= \{(1,1),(1,4),(2,3),(3,1),(3,4)\} \\ S &= \{(1,0),(2,0),(3,1),(3,2),(4,1)\} \end{aligned}$$
   Determine $S \circ R$, $R \circ S$, $S \circ S$ e $R \circ R$.
9. Determine a relação inversa de $R = \{(1,2),(1,3),(2,3)\}$ sobre $A = \{1,2,3\}$. Determine também $R^{-1} \circ R$ e $R \circ R^{-1}$.
10. Considere o conjunto $\mathbb{N} \times \mathbb{N}$ com a relação $\trianglelefteq \subset (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ definida por
$$(x,y) \trianglelefteq (a,b) \text{ se } \begin{cases} x < a & \text{ou} \\ x = a & \text{e } y \leq b. \end{cases}$$
    Ordene os seguintes elementos de acordo com a relação $\trianglelefteq$: $(1,2),(2,1),(3,1),(1,1),(2,2),(3,3),(1,4),(3,5),(2,4),(4,4),(4,1)$.
    É verdade que todo subconjunto não vazio de $\mathbb{N} \times \mathbb{N}$ tem um menor elemento com respeito a tal ordem?
11. Prove que se $f\colon A \to B$ é injetiva e $g\colon B \to C$ é injetiva, então $g \circ f\colon A \to C$ é injetiva.
12. Prove que a composição de duas funções bijetivas é uma função bijetiva.

Complemento: Conjuntos numéricos

Não é difícil definir o conjunto $\mathbb{N}$ dos números naturais como conjunto na teoria axiomática dos conjuntos usando o axioma do infinito. Uma construção conhecida é devida ao matemático John von Neumann[7]. A partir da construção, definimos as operações aritméticas, a relação de ordem e tudo o mais da aritmética pode ser deduzido formalmente dentro da teoria dos conjuntos. A partir dos naturais podemos construir os inteiros usando produto cartesiano e um tipo especial de relação chamada de *relação de equivalência* (veja a definição 117, página 61). Também, podemos construir os números racionais e até os reais com, por exemplo, os cortes de Dedekind.

Neste texto não adotamos tal abordagem, a aritmética elementar dos naturais e dos inteiros e suas propriedades são assumidas, como axiomas, e a definição dos conjuntos em si é a intuitiva. Esse será o ponto de partida para estudarmos algumas técnicas de demonstração no próximo capítulo.

Números naturais e suas propriedades aritméticas e de ordem

O conjunto dos números naturais é o conjunto

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

que munido da adição[8], da multiplicação[9] e da relação[10] $\leqslant$ usuais nos números naturais, satisfazem as seguintes propriedades: para quaisquer a, b, c, m, n, p números naturais

1. (associativa) $(a+b)+c = a+(b+c)$ e $(m\cdot n)\cdot p = m\cdot(n\cdot p)$;
2. (comutativa) $a+b = b+a$ e $m\cdot n = n\cdot m$;
3. (elemento neutro) 0 é o único natural tal que $a+0 = 0+a = a$ e 1 é único tal que $m\cdot 1 = 1\cdot m = m$ e 1;
4. (cancelamento) se $a+c = b+c$ então $a = b$ e, para a multiplicação, se $mp = np$ e $p \neq 0$ então $m = n$;
5. (distributiva) $(a+b)\cdot m = a\cdot m + b\cdot m$;
6. se $a+b = 0$ então $a = b = 0$, se $m\cdot n = 1$ então $m = n = 1$.
7. se $m\cdot n = 0$ então $m = 0$ ou $n = 0$;
8. (reflexiva) $a \leqslant a$;
9. (antisimétrica) se $a \leqslant b$ e $b \leqslant a$ então $b = a$;
10. (transitiva) se $a \leqslant b$ e $b \leqslant c$ então $a \leqslant c$;
11. (comparabilidade) $a \leqslant b$ ou $b \leqslant a$;
12. (tricotomia) vale uma e só uma das relações
$$a = b,\ a < b,\ b < a;$$
13. (compatibilidade) se $a \leqslant b$ então $a + c \leqslant b + c$; se $a \leqslant b$ então $a\cdot c \leqslant b\cdot c$.

Uma propriedade muito importante da estrutura $(\mathbb{N}, +, \cdot, \leqslant)$ é que a relação de ordem nos dá uma **boa-ordem**.

Definição 30. Dizemos que $a \in \mathbb{N}$ é o **menor elemento** de $A \subset \mathbb{N}$ se, e só se,

$$a \in A \quad \text{e} \quad \text{para todo } x \in A,\ a \leqslant x.$$

Denotamos o menor elemento de A por $\min(A)$.

Princípio da Boa Ordem (PBO) *Para todo $A \subset \mathbb{N}$, se A é não-vazio então A tem um **menor elemento**.*

[7] Também foi um precursor do computador digital, os computadores pessoais têm uma arquitetura (um esquema de interligar memória, cpu, dispositivos de entrada e saída) chamada *arquitetura de von Neumann*.

[8] $+$ é uma operação binária $+ : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ e escrevemos $a+b$ para denotar $+(a,b)$.

[9] $\cdot$ é uma operação binária $\cdot : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ e escrevemos $a\cdot b$ para denotar $\cdot(a,b)$.

[10] Escrevemos $a \leqslant b$ se existe um natural m tal que $a+m = b$. Escrevemos $a < b$ caso $m \neq 0$. Ainda $a \geqslant b$ denota $b \leqslant a$ e $a > b$ denota $b < a$.

Números inteiros e suas propriedades aritméticas e de ordem

O conjunto

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

é o conjunto dos números inteiros que munidos das funções (operações) soma e produto $+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ e da relação de ordem $\leqslant$ satisfazem as propriedades listadas a seguir.

Com relação a soma Para quaisquer $a, b, c \in \mathbb{Z}$

1. (associativa) $a + (b + c) = (a + b) + c$;
2. (comutativa) $a + b = b + a$;
3. (elemento neutro) $a + 0 = a$ e 0 é o único inteiro que satisfaz essa sentença;
4. (elemento simétrico) $a + (-a) = 0$ e $-a$ é o único inteiro que satisfaz essa sentença;
5. (cancelativa) se $a + b = a + c$ então $b = c$;
6. (troca de sinal) $-(a + b) = (-a) + (-b) = -a - b$.

Com relação ao produto Para quaisquer $a, b, c \in \mathbb{Z}$

7. (associativa) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
8. (comutativa) $a \cdot b = b \cdot a$;
9. (elemento neutro) $a \cdot 1 = a$ e 1 é o único inteiro que satisfaz essa sentença;
10. (distributiva) $a \cdot (b + c) = a \cdot b + a \cdot c$;
11. (cancelativa)
$$b = c \Longrightarrow a \cdot b = a \cdot c$$
$$a \neq 0 \text{ e } a \cdot b = a \cdot c \Longrightarrow b = c;$$
12. (anulamento) se $a \cdot b = 0$ então $a = 0$ ou $b = 0$.
13. se $a \cdot b = 1$ então $a = 1$ e $b = 1$ ou $a = -1$ e $b = -1$.

Com relação à ordem Para quaisquer $a, b, c \in \mathbb{Z}$

13. (reflexiva) $a \leqslant a$;
14. (antissimétrica) se $a \leqslant b$ e $b \leqslant a$ então $b = a$;
15. (transitiva) se $a \leqslant b$ e $b \leqslant c$ então $a \leqslant c$;
16. (comparabilidade) $a \leqslant b$ ou $b \leqslant a$;
17. (tricotomia) vale uma e só uma das relações
$$a = b,\ a < b,\ b < a;$$
18. (compatibilidade)
$$a \leqslant b \Longleftrightarrow a + c \leqslant b + c$$
$$c \in \mathbb{N} \text{ e } a \leqslant b \Longleftrightarrow a \cdot c \leqslant b \cdot c.$$
19. $a < b$ e $b \leqslant c \Rightarrow a < c$.
20. $a \leqslant b$ e $b < c \Rightarrow a < c$.
21. $a \leqslant b \Leftrightarrow -a \geq -b$.
22. $a < b \Leftrightarrow -a > -b$.

23. Regras de sinal
    (a) $a > 0$ e $b > 0 \Rightarrow ab > 0$
    (b) $a < 0$ e $b < 0 \Rightarrow ab > 0$
    (c) $a < 0$ e $b > 0 \Rightarrow ab < 0$
24. $a \leqslant b$ e $c \leqslant d \Rightarrow a + c \leqslant b + d$.
25. $a \leqslant b$ e $c < d \Rightarrow a + c < b + d$.
26. $a^2 \geq 0$.
27. $a < b$ e $c > 0 \Rightarrow ac < bc$
28. $a < b$ e $c < 0 \Rightarrow ac > bc$
29. $ac \leqslant bc$ e $c < 0 \Rightarrow a \geq b$

Definimos, para todo $a \in \mathbb{Z}$, o **valor absoluto** ou **módulo** de a por

$$|a| := \begin{cases} a & \text{se } a \geq 0, \\ -a & \text{caso contrário.} \end{cases}$$

O valor absoluto satisfaz as seguintes propriedades para quaisquer inteiros a, b

30. $|a| \geq 0$, ademais $|a| = 0$ se e só se $a = 0$.
31. $-|a| \leqslant a \leqslant |a|$.
32. $|-a| = |a|$.
33. $|ab| = |a||b|$.
34. $|a| \leqslant b \Leftrightarrow -b \leqslant a \leqslant b$.
35. $||a| - |b|| \leqslant |a + b| \leqslant |a| + |b|$.
36. $|a| - |b| \leqslant |a - b| \leqslant |a| + |b|$.

Definição 31. O subconjunto não vazio $A \subset \mathbb{Z}$ é **limitado inferiormente** se existe $m \in \mathbb{Z}$ (chamado **cota inferior**) tal que

$$\text{para todo } a \in A,\ m \leqslant a.$$

Se $m \in A$, então m é **menor elemento** ou **mínimo** de A, denotado por $\min(A)$.

37. Todo $A \subset \mathbb{Z}$ não vazio e limitado inferiormente tem um elemento mínimo.
38. (**propriedade arquimediana**) Para todos $a, b \in \mathbb{Z}$ com $b \neq 0$, existe $n \in \mathbb{Z}$ tal que $n \cdot b > a$.

Capítulo 2

Demonstrações

2.1 Introdução a técnicas de demonstrações

Do ponto de vista lógico existem, essencialmente, dois tipos de sentenças verdadeiras: os axiomas, que são admitidos como verdadeiros, e os teoremas, que são demonstrados serem verdadeiros. Em textos matemáticos as sentenças que nós demonstramos são, geralmente, chamadas de *teoremas*, *proposições*, *lemas* e *corolários*. A diferença entre esses rótulos é circunstancial e depende de uma convenção não muito rígida que diz, em geral, que teoremas são resultados importantes, as proposições são menos importantes que os teoremas, os lemas são resultados auxiliares usadas nas provas de outros resultados e que merecem destaque, os corolários são sentenças que se seguem facilmente de outros resultados.

Ainda há sentenças que chamamos *princípio* que é um teorema ou axioma e que ocupa um papel fundamental numa teoria por ser a chave para demonstrar um grande número de propriedades importantes. Um exemplo típico é o Princípio da Indução Finita que em algumas exposições sobre os naturais ele aparece como um dos axiomas (como no tratamento axiomático de Peano), e em outras, como teorema (como na teoria dos conjuntos ZFC).

Um outro termo recorrente em textos matemáticos é *conjetura* (ou *conjectura*) que é uma sentença que está sendo proposta como uma sentença verdadeira porém não é conhecida uma demonstração. Se posteriormente demonstrada verdadeira, torna-se um teorema; se for mostrado um contraexemplo deixa de ser uma conjetura. Até o momento que este texto estava sendo escrito a seguinte sentença não tinha uma demonstração.

CONJECTURA 32 (CONJETURA DE GOLDBACH) *Todo inteiro par maior que 2 pode ser escrito como a soma de dois números primos.*

Muitas das sentenças de teoremas (talvez a maior parte) são generalizações de sentenças condicionais e vamos dar ênfase nesse caso já que é inviável considerarmos todos as possíveis estruturas lógicas dos enunciados de sentenças.

2.1.1 Considerações iniciais através de um exemplo

Para demonstrar uma sentença precisamos conhecer as definições dos termos usados na sentença. Vamos ver um exemplo. Começamos com uma definição de número par.

Definição 33. Um inteiro n é **par** se, e somente se, n é da forma $2k$ para algum inteiro k. Um inteiro n é **ímpar** se, e somente se, n é da forma $2k+1$ para algum inteiro k.

Observemos que a definição acima é dada por um "se, e somente se" de modo que é usada em demonstrações como uma equivalência lógica, para qualquer que seja o inteiro n

$$n \text{ é par} \Leftrightarrow \exists k \in \mathbb{Z},\ n = 2k. \tag{2.1}$$

Se a definição é dada por uma condicional

"n é par se n é da forma $2k$ para algum inteiro k"

ao invés de uma bicondicional ela, a rigor, não exclui a possibilidade de $n = 1$ ser par (veja a discussão no início da seção 1.1.1). Entretanto, em textos matemáticos é comum encontrar definições que usam uma condicional e nesses casos devemos entender que a intenção é a da equivalência. Por exemplo, em *um inteiro n é par se ele é múltiplo de* 2 não garante que um número par é múltiplo de 2.

Além das definições, usamos axiomas e teoremas já conhecidos. Essa metodologia de derivar teoremas a partir de axiomas, o método axiomático, foi usado de modo pragmático pela primeira vez por Euclides por volta de 300 aC. Como alguém pensa e

cria uma demonstração é uma ponto que está fora do nosso alcance, não vamos discutir, mas a demonstração em si tem que se desenrolar em passos logicamente válidos do início ao fim e é da praxe que as demonstrações sigam alguns paradigmas. Cada demonstração tem os seus próprios detalhes mas os paradigmas nos dão um referencial organizado para uma boa escrita das deduções.

Em muitos casos as sentenças de teoremas são sentenças condicionais não escritas explicitamente, as palavras-chave "se, então" e "para todo", ou equivalentes, não apareçam explicitamente, assim como os quantificadores são omitidos. O trabalho inicial sempre é o da interpretação e análise do texto. Por exemplo, em "o quadrado de todo número real não nulo é positivo" temos, implicitamente, a estrutura lógica "para todo número real x, se $x \neq 0$ então $x^2 > 0$".

TEOREMA 34 *A soma de inteiros pares é par.*

Para demonstrar essa afirmação, provamos que para quaisquer x e y inteiros, se x é par e y é par, então $x+y$ é par. Essa sentença tem a "forma lógica" $A \wedge B \rightarrow C$ e o que precisamos demonstrar que se A é verdadeiro (x é par) e B é verdadeiro (y é par), então C é verdadeiro ($x+y$ é par). Para isso, assumimos A e B como hipóteses, ou premissas verdadeiras, e construímos uma demonstração que conclui que C é verdadeiro.

Demonstração do teorema 34. Sejam x e y números inteiros e assuma que x é par e y é par. Então, por definição, existem inteiros k_1 e k_2 tais que $x = 2k_1$ e $y = 2k_2$, logo $x + y = 2(k_1 + k_2)$, portanto, pela definição, $x+y$ é par. □

Note que na demostração usamos a equivalência (2.1) nos dois sentido, se x é par então ele é múltiplo de 2, e se $x+y$ é múltiplo de 2 então ele é par.

Uma consideração importante ao escrever uma demonstração é reconhecer o que precisa ser provado e o que pode ser usado sem justificativa. Esse último depende do contexto e é, em geral, calibrado de acordo com a audiência a que se destina a demonstração. O nosso contexto é o de aprendizado elementar logo é necessário escrever com bastante detalhes. Também, um trabalho de rascunhagem investigativa é muito importante para descobrir a estratégia geral para abordar o problema a ser resolvido, antes de examinar os detalhes. Todo matemático teve que tentar muitas abordagens para provar um teorema antes de encontrar uma que funcionasse, aqui está a maior parte do trabalho.

Finalmente, as demonstrações devem se escritas em português, usando frases completas e com pontuação adequada, como foi feito no caso da *Demonstração do teorema 34* e não como feita na tabela abaixo. Fórmulas e símbolos matemáticos são partes de frases e não são tratados diferente de outras palavras.

A Leitura

Ler uma demonstração exige esforço para a validação do argumento. Em casos muito simples, como no teorema acima, não dá muito trabalho explicitar todo esquema lógico desse argumento. Fazemos isso abaixo na tabela 2.1, usando alguns símbolos para encurtar a escrita fazemos referência a algumas regras de inferência, apresentadas na página 11 e seguintes, e a propriedades aritméticas apresentadas na seção 1.2.4.

1)	x é par e y é par.	(hipótese)
2)	x é par.	(regra da simplificação)
3)	y é par.	(regra da simplificação)
4)	Se x é par, então $\exists k_1 \in \mathbb{Z}, x = 2k_1$	(definição)
5)	$\exists k_1 \in \mathbb{Z}, x = 2k_1$	(modus ponens)
6)	$x = 2k_1$	(regra da instanciação existencial)
7)	Se y é par, então $\exists k_2 \in \mathbb{Z}, y = 2k_2$	(definição)
8)	$\exists k_2 \in \mathbb{Z}, y = 2k_2$	(modus ponens)
9)	$y = 2k_2$	(regra da instanciação existencial)
10)	$x = 2k_1$ e $y = 2k_2$	(regra da conjunção)
11)	Se $x = 2k_1$ e $y = 2k_2$, então $x + y = 2(k_1 + k_2)$	(compatibilidade)
12)	$x + y = 2(k_1 + k_2)$	(modus ponens)
13)	Se $x + y = 2(k_1 + k_2)$, então $\exists c \in \mathbb{Z}, x + y = 2c$	(regra da generalização universal)
14)	$\exists c \in \mathbb{Z}$ tal que $x + y = 2c$	(modus ponens)
15)	Se $\exists c \in \mathbb{Z}, x + y = 2c$, então $x + y$ é par	(definição)
16)	$x + y$ é par	(modus ponens).

Tabela 2.1: Um escrutínio da demonstração do teorema 34.

Notemos que a partir das premissas na tabela 2.1, uma linha qualquer é uma sentença verdadeira sempre a linhas anteriores a ela são verdadeiras, portanto se a hipótese é verdadeira a última linha é uma sentença verdadeira.

2.1.2 Demonstração direta de implicação

Na argumentação mais direta para demonstrar que $P \to Q$ é verdadeiro, assumimos P verdadeiro e concluímos que Q é verdadeiro. Essa estratégia é chamada de prova direta da implicação.

TEOREMA 35 *Se a e b são números inteiros tais que $0 < a < b$, então $a^2 < b^2$.*

DEMONSTRAÇÃO. Sejam a e b são números inteiros. Vamos supor que $0 < a < b$ e provar que $a^2 < b^2$.
Se $a < b$ e $0 < a$ então $a^2 < ab$. Se $a < b$ e $0 < b$ então $ab < b^2$. Por transitividade, $a^2 < b^2$ como queríamos demonstrar. □

Uma leitura detalhada do argumento é dada na tabela 2.2.

1)	$0 < a$ e $a < b$	(hipótese)
2)	$a < b$	(regra da simplificação)
3)	$0 < a$	(regra da simplificação)
4)	se $0 < a$ e $a < b$, $0 < b$	(transitividade do $<$)
5)	$0 < b$	(modus ponens)
6)	se $a > 0$ e $a < b$ então $a \cdot a < a \cdot b$	(compatibilidade do $<$ com $\cdot$)
7)	$a^2 < ab$	(modus ponens)
8)	$b > 0$ e $a < b$	(regra da conjunção)
9)	se $b > 0$ e $a < b$ então, $a \cdot b < b \cdot b$	compatibilidade do $<$ com $\cdot$)
10)	$ab < b^2$	(modus ponens)
11)	$a^2 < ab$ e $ab < b^2$	(regra da conjunção)
12)	se $a^2 < ab$ e $ab < b^2$ então $a^2 < b^2$	(transitividade do $<$)
13)	$a^2 < b^2$	(modus ponens)

Tabela 2.2: Um escrutínio do teorema 35.

TEOREMA 36 *Sejam A, B, C conjuntos não vazios. Se $A \cap C \subset B$ e $a \in C$ então $a \notin A \setminus B$.*

De acordo com a estratégia de demonstração direta, devemos supor que $A \cap C \subset B$ e $a \in C$ é verdadeiro e provar que $a \notin A \setminus B$ é verdadeiro.

Pela definição de diferença de conjuntos $a \notin A \setminus B$ é logicamente equivalente a não($a \in A$ e $a \notin B$) que é logicamente equivalente a $a \notin A$ ou $a \in B$ que, por sua vez, é logicamente equivalente a $a \in A \to a \in B$. Portanto, se assumimos verdadeiro $A \cap C \subset B$ e $a \in C$ e deduzirmos que $a \in A \to a \in B$ é verdadeiro então podemos concluir, pela equivalência lógica, que $a \notin A \setminus B$ é verdadeiro. Assim, nossa tarefa é demonstrar que é verdadeira a (primeira) condicional

$$(A \cap C \subset B \text{ e } a \in C) \to (a \in A \to a \in B). \tag{2.2}$$

Para demonstrar que vale (2.2)

assumimos: $A \cap C \subset B$ e $a \in C$ verdadeiro

provamos: $a \in A \to a \in B$ verdadeiro

para provar que $a \in A \to a \in B$ é verdadeiro, uma condicional, assumimos $a \in A$ verdadeiro e deduzimos que $a \in B$ é verdadeiro, no caso $a \notin A$ não há o que fazer pois a condicional é verdadeira. Assim para demonstrar (2.2)

assumimos: $A \cap C \subset B$ e $a \in C$ e $a \in A$ verdadeiro

provamos: $a \in B$ verdadeiro.

Com esse rascunho em mãos escreveremos a demonstração.

DEMONSTRAÇÃO. Sejam A, B, C conjuntos não vazios e $a \in A$. Vamos assumir que $A \cap C \subset B$ e $a \in C$ e $a \in A$.
Se $a \in C$ e $a \in A$ então $a \in A \cap C$ por definição de interseção. Se $a \in A \cap C$ e $A \cap C \subset B$ então $a \in B$ por definição de inclusão. Portanto $a \in B$. □

Há uma esquema lógico genérico da ideia empregada acima, vale o seguinte:

$$P_1 \wedge P_2 \wedge \cdots \wedge P_n \Rightarrow (P \to Q) \text{ se, e somente se, } P_1 \wedge P_2 \wedge \cdots \wedge P_n \wedge P \Rightarrow Q.$$

Sobre enunciados Como já dissemos, muitos teoremas afirmam propriedades para todos os elementos de um domínio sem que o quantificador seja explicitamente mencionado, por exemplo,

1. Se 3 divide o inteiro n então 9 divide n^2.
2. Se n é um inteiro ímpar, então n^2 é ímpar.
3. Se $m \in \mathbb{Z}$ é par e $n \in \mathbb{Z}$ é par, então $m+n$ é par.

Essas sentenças significam,

1. Para todo $n \in \mathbb{Z}$, se 3 divide n então 9 divide n^2.
2. Para todo $n \in \mathbb{Z}$, se n é ímpar, então n^2 é ímpar.
3. Para todo $n \in \mathbb{Z}$, para todo $m \in \mathbb{Z}$, se m é par e n é par, então $m+n$ é par.

Em parte, esse comportamento é explicado pelo seguinte. Uma demonstração para uma sentença na forma lógica $\forall x(P(x) \to Q(x))$ tem os seguintes passos:

passo 1 considere c arbitrário do domínio de x

passo 2 prove $P(c) \to Q(c)$

passo 3 conclua $\forall x(P(x) \to Q(x))$ pela regra de inferência da generalização universal.

A parte principal dessa estratégia, onde se concentra todo o trabalho, é a prova da implicação $P(c) \to Q(c)$. Todo o trabalho de demonstrar "Para todo n, se 3 divide n então 9 divide n^2" está concentrado na parte "se 3 divide n então 9 divide n^2" para um número n arbitrário no universo de discurso.

No passo 2, demonstrar $P(c) \to Q(c)$, usando a estratégia direta, por exemplo, assumimos $P(c)$ verdadeiro e usamos regras de inferência, definições, axiomas e equivalências lógicas para concluir que $Q(c)$ é verdadeiro. Isso feito sabemos que $P(c) \to Q(c)$ é verdadeiro o que estabelece o passo 2 descrito acima.

No caso particular de "se 3 divide n então 9 divide n^2" vamos tomar a definição de "divide".

Definição 37. O inteiro k **divide** o inteiro n se, e somente se, existe $q \in \mathbb{Z}$ tal que $kq = n$. Nesse caso escrevemos $k \mid n$ e, também, dizemos que k e q são **fatores** de n.

Agora, vamos demonstrar que se n é um número inteiro arbitrário então

$$\text{se 3 divide o inteiro } n \text{ então 9 divide } n^2 \tag{2.3}$$

DEMONSTRAÇÃO. Seja n um inteiro e assumamos que 3 divide n.

Se $3 \mid n$ então existe $q \in \mathbb{N}$ tal que $n = 3q$, logo $n^2 = 9q^2$. Portanto, n^2 é da forma $9k$, para algum $k \in \mathbb{Z}$, ou seja, 9 divide n^2 por definição. □

Como a variável n acima pode assumir qualquer valor natural, ou seja, n é um elemento genérico de $\mathbb{Z}$, o que provamos de fato foi a seguinte sentença.

TEOREMA 38 *Para todo $n \in \mathbb{Z}$, se 3 divide n então 9 divide n^2.*

Mais um exemplo bastante simples de demonstração direta é a seguinte.

TEOREMA 39 *Para todo $n \in \mathbb{Z}$, se n é ímpar, então n^2 é ímpar.*

DEMONSTRAÇÃO. Seja n um número inteiro arbitrário. Vamos provar que se n é ímpar então n^2 é ímpar.

Assuma n ímpar. Por definição, existe $k \in \mathbb{N}$ tal que $n = 2k+1$. Se $n = 2k+1$ então $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$. Portanto, existe um número ℓ tal que n^2 é da forma $2\ell+1$, ou seja, n^2 é ímpar por definição. □

Usualmente, omitimos das demonstrações os passos muito elementares (já dissemos que isso depende do contexto) e omitimos os passos ubíquos como a menção explícita da generalização universal na conclusão (passo 3 na página anterior) e os *modus ponens*: se temos a premissa A e a condicional $A \to B$, não escrevemos a dedução "de A e $A \to B$, temos B", nesse caso, assim como noutros que usam as regras de inferência, assumimos direto que vale a conclusão, nesse caso B. Por exemplo, no caso "se x é par então é múltiplo de 2" e por hipótese x é par, da sentença condicional já assumimos que x é múltiplo de 2. Ainda, comumente usamos a mesma variável (quantificada) do enunciado para representar o elemento arbitrário do domínio, isto é, a instanciação de "para todo $x \in D, P(x)$" resulta em $P(x)$. Finalmente, embora tenhamos usados símbolos lógicos para explicitar formas e argumentos, **não** éuma boa prática usarxmos símbolos de conectivos e quantificadores para escrever uma demonstração na redação final, é uma questão de estilo e de boa escrita.

Exercício 40. Escreva um escrutínio da demonstração do teorema 39.

Exercício 41. Escreva uma demonstração para o teorema: para todo $x \in \mathbb{N}\setminus\{0\}$, para todo $y \in \mathbb{N}$, se x divide y então x^2 divide y^2. (Nota: a hipótese $x \neq 0$ é desnecessária, devemos cuidar para não enunciar sentenças com hipóteses desnecessárias.)

Demonstração de sentenças sobre conjuntos

Quando precisamos provar sentenças a respeito de conjuntos caímos, essencialmente, em dois tipos de tarefas.

1. Dados x e S, provar que $x \in S$. Isto requer verificar que x satisfaz as propriedades que os elementos de S satisfazem.
2. Dados A e B, provar que $A \subseteq B$. Uma demonstração considera um elemento arbitrário x em A e mostra que ele também deve ser um elemento de B. Note que isso recai no item anterior.
3. Para provar que $A = B$, usualmente, provamos em dois casos: $A \subseteq B$ e $B \subseteq A$.

Vejamos um esboço da demonstração de uma das leis de De Morgan: $C\setminus(A\cup B) = (C\setminus A)\cap(C\setminus B)$. Esse é um exemplo em que o item 3 acima pode ser abreviado, não precisamos mostrar as duas inclusões por causa da seguinte sequência de equivalências

$$\begin{aligned}
x \in C\setminus(A\cup B) &\Leftrightarrow x \in C \text{ e } x \notin A\cup B && \text{por definição}\\
&\Leftrightarrow x \in C \text{ e não}(x \in A\cup B) && \text{por definição de } \notin\\
&\Leftrightarrow x \in C \text{ e não}(x \in A \text{ ou } x \in B) && \text{por definição de } \cup\\
&\Leftrightarrow x \in C \text{ e não}(x \in A) \text{ e não}(x \in B) && \text{por De Morgan (lógico)}\\
&\Leftrightarrow x \in C \text{ e } x \notin A \text{ e } x \notin B && \text{por definição}\\
&\Leftrightarrow x \in C \text{ e } x \notin A \text{ e } x \in C \text{ e } x \notin B && \text{por definição}\\
&\Leftrightarrow x \in (C\setminus A)\cap(C\setminus B) && \text{por definição de } \cap.
\end{aligned}$$

Reescrevendo de modo a torná-la mais apresentável resulta na seguinte demonstração.

DEMONSTRAÇÃO. Sejam A, B e C conjuntos e vamos provar que $C\setminus(A\cup B) = (C\setminus A)\cap(C\setminus B)$. Por definição $x \in C\setminus(A\cup B)$ se, e só se, $x \in C$ e $x \notin A\cup B$. Mas, $x \notin A\cup B$ se, e só se, $x \notin A$ e $x \notin B$ de sorte que $x \in C\setminus(A\cup B)$ se, e só se, $x \in C$ e $x \notin A$ e $x \notin B$, ou seja, , ou seja, $x \in (C\setminus A)\cap(C\setminus B)$. Portanto, $x \in C\setminus(A\cup B)$ se, e só se, $x \in (C\setminus A)\cap(C\setminus B)$, donde concluímos que $C\setminus(A\cup B) = (C\setminus A)\cap(C\setminus B)$. □

2.1.3 Demonstração de equivalências

Para demonstrar que uma sentença da forma $P \leftrightarrow Q$ é verdadeira nem sempre conseguimos uma sequência de sentenças equivalentes como no exemplo anterior. Ao invés disso nós usamos que $(P \leftrightarrow Q)$ é logicamente equivalente a $(P \leftarrow Q) \wedge (P \rightarrow Q)$ e, de fato, escrevemos duas demonstrações para implicação, provamos $P \rightarrow Q$ e a sua recíproca $Q \rightarrow P$. Cada uma dessas duas implicações pode ser demonstrada com alguma das técnicas para demonstrar uma implicação.

TEOREMA 42 *Para todos $a, b \in \mathbb{Z}$ não nulos, $a \mid b$ e $b \mid a$ se, e somente se, $a = b$ ou $a = -b$.*

DEMONSTRAÇÃO. Sejam a e b números inteiros.

Primeiro, suponha que $a = b$ ou $a = -b$. Em cada um desses dois casos, $a \mid b$ e $b \mid a$ seguem imediatamente da definição.

Agora, suponha que $a \mid b$ e $b \mid a$. Se $a \mid b$ então existe um inteiro k tal que $ak = b$ e se $b \mid a$ então existe um inteiro q tal que $bq = a$, logo, $(bq)k = b$ donde tiramos que $qk = 1$, portanto, do item 13, página 28 concluímos que $a = b$ ou $a = -b$. □

TEOREMA 43 *Nos inteiros são equivalentes as afirmações:*

(i) Para todos a, b e $c \neq 0$, se $ac = bc$ então $a = b$.

(ii) Para todos a e b, se $ab = 0$ então $a = 0$ ou $b = 0$.

DEMONSTRAÇÃO. Vamos assumir que (i) é verdadeiro é demonstrar (ii).

Para provar (ii), sejam a e b inteiros tais que $ab = 0$. Se $a \neq 0$ então de $ab = a0$ temos, por (i) que $b = 0$. Por outro lado, se $b \neq 0$ então de $ab = 0b$ e temos que $a = 0$. Portanto, $a = 0$ ou $b = 0$.

Agora, vamos assumir que (ii) é verdadeiro é demonstrar (i).

Para provar (i), sejam a, b e c inteiros com $c \neq 0$ e tais que $ac = bc$. Se $ac = bc$, então $ac - bc = 0$. Fatorando o produto temos $(a-b)c = 0$ e, por (i), $a - b = 0$ já que $c \neq 0$. Se $a - b = 0$ então $a = b$. □

2.1.4 Demonstração indireta de implicação

Nesse tipo de prova demonstramos que é verdadeira uma sentença logicamente equivalente a $P \to Q$, como a contrapositiva, por exemplo.

Demonstração pela contrapositiva: Para provar que $P \to Q$ é verdadeira demonstramos $\neg Q \to \neg P$ é verdadeira.

Por exemplo, para um número natural n arbitrário, a seguinte implicação é verdadeira (tente uma prova direta)

$$\text{se } n^2 \text{ é par, então } n \text{ é par.} \tag{2.4}$$

A contrapositiva de (2.4) é, assumindo que ímpar é a negação de par (veja corolário 70),

$$\text{se } n \text{ é ímpar, então } n^2 \text{ é ímpar.}$$

que é verdadeira, como foi estabelecido pelo teorema 39.

Definição 44. O **maior divisor comum** dos inteiros a, b, denotado $\operatorname{mdc}(a,b)$ é dado por

$$\operatorname{mdc}(a,b) := \begin{cases} 0, & \text{se } a = b = 0, \\ \max\{d \in \mathbb{N} \colon d \,|\, |a| \text{ e } d \,|\, |b|\}, & \text{caso contrário.} \end{cases} \tag{2.5}$$

Os inteiros a e b são ditos **coprimos** se, e só se, $\operatorname{mdc}(a,b) = 1$.

Observamos que se d é um natural que divide $|a|$ então $d \leqslant |a|$, portanto o conjunto de todos os divisores de a tem um maior elemento. Se $a = 0$ então todo inteiro é divisor de a, portanto o conjunto de todos os divisores de a não tem um maior elemento. Analogamente, o conjunto de todos os divisores de $b \neq 0$ tem um maior elemento. Disso, o $\operatorname{mdc}(a,b)$ está bem definido por (2.5).

Teorema 45 *Para todos $a, b \in \mathbb{N}$, se a e b são coprimos, então a não é par ou b não é par.*

Vamos demonstrar pela contrapositiva que se a e b são coprimos então não são ambos par. Antes o leitor é convidado a dar uma prova direta da sentença. Demonstrar a contrapositiva significa provar que vale a sentença

$$\text{se } a \text{ é par e } b \text{ é par, então } \operatorname{mdc}(a,b) \neq 1. \tag{2.6}$$

para todos $a, b \in \mathbb{Z}$. A estratégia é clara nesse caso: (1) Tome a par e b par; (2) $2 \,|\, a$ e $2 \,|\, b \Rightarrow \operatorname{mdc}(a,b) \geqslant 2$; (3) portanto $\operatorname{mdc}(a,b) \neq 1$. Pela generalização universal, pois a e b são inteiros arbitrários, vale que a equação (2.6) é verdadeira. Passemos a demonstração.

Demonstração do teorema 45. Vamos provar o teorema 45 pela contrapositiva. Sejam a e b números inteiros quaisquer e assumamos que a é par e que b é par. Então, pela definição, 2 divide a e divide b, logo o $\operatorname{mdc}(a,b)$ é pelo menos 2. Portanto, $\operatorname{mdc}(a,b) \neq 1$. □

Demonstração por contradição: Para demonstrar que vale $P \to Q$ nós demonstramos a veracidade da condicional $(P \wedge \neg Q) \to \mathbf{F}$.

A regra da contradição, dada na página 12, é a consequência lógica

$$\neg A \to \mathbf{F} \Rightarrow A$$

e fazendo A ser a sentença $P \to Q$, cuja negação é $P \wedge \neg Q$, justifica tal equivalência lógica.

Assim, numa demonstração por contradição assumimos que a hipótese é verdadeira e a *negação* da sentença a ser provada é verdadeira e, com essas hipótese, derivamos uma *contradição*. Um exemplo de estratégia para prova por contradição é

1)	P	(por hipótese)
2)	$\neg Q$	(por hipótese)
3)	$\neg P$	(por dedução)
4)	$P \wedge \neg P$	(pela regra da conjunção)

De fato, na linha 3 deduzimos alguma sentença que junto com as premissas formam uma sentença lógica falsa. Também, pode ser o caso em que a contradição seja alguma outra sentença que negue algum teorema (alguma sentença que é sabida ser verdadeira). Veja o exemplo 50 mais adiante.

Demonstração do teorema 45. A demonstração é por contradição. Sejam a e b números inteiros arbitrários. Assumamos que a e b são coprimos. Se a é par e b é par então $\operatorname{mdc}(a,b) \geqslant 2$, ou seja, $\operatorname{mdc}(a,b) = 1$ e $\operatorname{mdc}(a,b) \geqslant 2$, uma contradição. Portanto, se a e b são coprimos, então a e b não são ambos números pares. □

Um caso clássico de prova do contradição é o da irracionalidade da raiz de dois.

Definição 46. O número real x é **racional** se existem números inteiros n e m, com $m \neq 0$, tais que $x = \frac{n}{m}$. O conjunto de todos os números racionais é denotado por $\mathbb{Q}$.

Se x não é racional então x é **irracional** e $\mathbb{R} \setminus \mathbb{Q}$ é o conjunto dos números irracionais.

TEOREMA 47 *$\sqrt{2}$ é irracional.*

Essa sentença pode ser enunciada usando uma condiconal

Para todo real x, se $x^2 = 2$ então x é irracional.

A prova segue assumindo que $x^2 = 2$ e que $x \in \mathbb{Q}$.

Demonstração tirada do livro de Bases Matemáticas, de A. Caputi e D. Miranda. Faremos a demonstração pelo método de redução ao absurdo. Ou seja, supomos que $\sqrt{2}$ é um número racional, i.e., que existem números inteiros positivos a e b tais que $\frac{a}{b} = \sqrt{2}$ ou, equivalentemente $\left(\frac{a}{b}\right)^2 = 2$.

Podemos supor que a e b não são ambos números pares, pois se fossem, poderíamos simplificar a fração até termos que pelo menos um dos termos da fração seja ímpar.

Agora, escrevemos $\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2$, então:

$$qa^2 = 2b^2 \tag{2.7}$$

Concluímos então que a^2 é um número par, pois é dobro de b^2. Logo a também deve ser par, pois se a fosse ímpar o seu quadrado também seria ímpar.

Temos então que a é um número par e, portanto, é o dobro de algum número inteiro, digamos k: $a = 2k$. em (2.7) temos:

$$(2k)^2 = 2b^2 \Rightarrow 4k^2 = 2b^2 \Rightarrow 2k^2 = b^2.$$

De modo análogo, temos que b deve ser um número par. O que é absurdo pois a e b não são ambos números pares. Portanto, $\sqrt{2}$ tem que ser um número irracional. Como queríamos demonstrar. □

O método da redução ao absurdo mencionado na demonstração é como também é chamado o método da contradição. Um escrutínio dessa demonstração é apresentado na tabela 2.3. Nela usamos que todo racional pode ser escrito como uma fração de números coprimos, a qual chamamos de **forma reduzida**. Para demonstrar que toda fração tem uma forma reduzida vamos primeiro mostrar um resultado mais poderoso.

O que precisamos para usar na linha 2 da tabela 2.3 acima seguirá como corolário do seguinte resultado.

TEOREMA 48 *Para todo $d \in \mathbb{N}^*$ e todo $e \in \mathbb{N}^*$*

$$\text{mdc}\left(\frac{d}{\text{mdc}(d,e)}, \frac{e}{\text{mdc}(d,e)}\right) = 1.$$

Nesse caso, vamos provar que se o mdc acima for maior que 1 então temos um contradição. O resultado segue da regra da contradição pois inferimos que o mdc é $\leqslant 1$ e como não são ambos os números iguais a 0 temos por definição de mdc que o mdc é $\geqslant 1$. Portanto concluímos que vale a igualdade, isto é, o mdc vale 1.

DEMONSTRAÇÃO. Sejam d e e números naturais arbitrários e não nulos. Façamos, para fins de simplificação,

$$m \coloneqq \text{mdc}(d,e) \text{ e } k \coloneqq \text{mdc}\left(\frac{d}{m}, \frac{e}{m}\right).$$

Vamos assumir $k > 1$. Pela definição de mdc, k divide $\frac{d}{m}$ e k divide $\frac{e}{m}$.

Se k divide $\frac{d}{m}$ então km divide d. (verifique) Logo km divide d. Analogamente, km divide e.

Se $k > 1$ então $km > m$. Se $km \mid d$ e $km \mid e$ então $km \leqslant m$, pois m é o maior divisor de d e e.

Portanto $km > m$ e $km \leqslant m$, uma contradição. □

COROLÁRIO 49 *Todo número racional pode ser escrito como $\frac{a}{b}$ com a e b coprimos.*

DEMONSTRAÇÃO. Seja q um racional arbitrário. Por definição, existem inteiros n e $m \neq 0$ tais que $q = \frac{n}{m}$. Faça $d = \text{mdc}(n,m)$, $a = \frac{n}{d}$ e $b = \frac{m}{d}$ que temos, pelo teorema anterior, $\text{mdc}(a,b) = 1$. Portanto $q = \frac{n}{m} = \frac{a}{b}$. □

1)	$\sqrt{2} \in \mathbb{Q}$	(premissa)
2)	$\sqrt{2} \in \mathbb{Q} \rightarrow \exists a, b \in \mathbb{N}$ coprimos e $\sqrt{2} = \frac{a}{b}$.	(corolário 49 dado abaixo)
3)	$\exists a, b \in \mathbb{N}$ coprimos e $\sqrt{2} = \frac{a}{b}$.	(modus ponens)
4)	$\sqrt{2} = \frac{a}{b}$ e a e b são coprimos.	(instanciação existencial)
5)	a e b são coprimos.	(regra da simplificação)
6)	$\sqrt{2} = \frac{a}{b}$.	(regra da simplificação)
7)	Se $\sqrt{2} = \frac{a}{b}$ então $2 = \left(\frac{a}{b}\right)^2$.	(compatibilidade)
$7\frac{1}{2}$)	Se $2 = \left(\frac{a}{b}\right)^2$ então $2 = \frac{a^2}{b^2}$.	(propriedade da potência)
8)	Se $2 = \frac{a^2}{b^2}$ então $a^2 = 2b^2$.	(compatibilidade)
9)	Se $\sqrt{2} = \frac{a}{b}$ então $a^2 = 2b^2$.	(silogismo)
10)	$a^2 = 2b^2$.	(modus ponens)
11)	Se $a^2 = 2b^2$ então a^2 é par.	(definição de par)
12)	Se a^2 é par então a é par	(contrapositiva teo. 39)
13)	Se $a^2 = 2b^2$ então a é par	(silogismo)
14)	a é par	(modus ponens)
15)	Se a é par então existe $k \in \mathbb{N}$, $a = 2k$.	(definição de par)
16)	Existe $k \in \mathbb{N}$, $a = 2k$.	(modus ponens)
17)	$a = 2k$.	(instanciação universal)
18)	$a = 2k$ e $a^2 = 2b^2$.	(conjunção)
19)	Se $a = 2k$ e $a^2 = 2b^2$ então $4k^2 = 2b^2$.	(compatibilidade)
$19\frac{1}{2}$)	Se $4k^2 = 2b^2$ então $2k^2 = b^2$.	(compatibilidade)
20)	Se $b^2 = 2k^2$ então b^2 é par.	(definição de par)
21)	Se b^2 é par então b é par.	(contrapositiva teo. 39)
22)	Se $a = 2k$ e $a^2 = 2b^2$ então b é par.	(silogismos)
23)	b é par.	(modus ponens)
24)	a é par e b é par.	(conjunção)
25)	a e b coprimos e a é par e b é par.	(contradição)

Tabela 2.3: Um escrutínio da demonstração da irracionalidade de $\sqrt{2}$.

Exemplo 50 (Outra prova de que $\sqrt{2} \notin \mathbb{Q}$). Suponha $\sqrt{2} = \frac{p}{q}$ de modo que $2 = \frac{p^2}{q^2}$. Escreva, $q^2 = 2^k r$ com r ímpar; isso pode ser feito por causa do teorema fundamental da aritmética (teorema 73, página 42). Por $2^k r$ ser um quadrado k tem que ser par. Por outro lado $p^2 = 2q^2 = 2^{k+1} r$ e por $2^{k+1} r$ ser um quadrado k é impar. Portanto k é par e k é ímpar, o que é uma contradição (pelo corolário 70, pagína 41).

A seguir damos um exemplo de prova de uma equivalência usando métodos diferentes para cada condicional.

TEOREMA 51 *Para todo $n \in \mathbb{Z}$, n é ímpar se, e somente se, n^2 é ímpar.*

DEMONSTRAÇÃO. Seja $n \in \mathbb{Z}$ arbitrário. Vamos provar que n^2 ímpar se, e só se, n ímpar.

Vamos assumir que n é ímpar. Então n^2 é ímpar pelo teorema 39.

Agora, vamos assumir que n^2 ímpar e provar que n ímpar. A prova é por contradição, suponha que n é par. Então $n = 2k$ para algum $k \in \mathbb{Z}$ e se $n = 2k$, então $n^2 = 4k^2$, ou seja, n^2 é par e n^2 ímpar, uma contradição. Portanto, se n^2 é ímpar então n é ímpar.

Portanto n^2 ímpar se, e só se, n ímpar, para todo natural n. □

COROLÁRIO 52 *Para todo $n \in \mathbb{Z}$, n é par se, e somente se, n^2 é par.*

DEMONSTRAÇÃO. Exercício. □

2.1.5 Demonstração por vacuidade e prova trivial

Estabeleceremos que a sentença $P \to Q$ é verdadeira se assegurarmos que P é falso, independentemente do valor lógico de Q, ou assegurarmos que Q é verdadeiro, independentemente do valor de P. No primeiro caso chamamos de *prova por vacuidade* e no segundo *prova trivial*.

Um exemplo de prova por vacuidade foi dado no teorema 15, na página 19, de que vazio é subconjunto de qualquer conjunto A, isso vale por vacuidade com a condicional que define a inclusão $x \in \varnothing \to x \in A$.

Os dois próximos exemplo são irrelevantes do ponto de vista matemático e servem apenas para ilustração.

TEOREMA 53 *Se x é um número real tal que $x^2 + 1 < 0$ então $x^5 \geqslant 4$.*

Isso é um teorema pois para qualquer real x temos que $x^2 \geqslant 0$, logo $x^2 + 1 > 0$.

TEOREMA 54 *Se $n > 3$ é um número par e primo, então n é da forma $4n + 1$.*

Isso é um teorema pois não há número primo par maior que 3. Uma curiosidade é que existem infinitos números primos da forma $4n + 1$, mas todos são ímpares pois são da forma $2(2n) + 1$.

Notemos que a contrapositiva do primeiro teorema afirma que "se $x^5 < 4$ então $x^2 + 1 \geqslant 0$". Como a conclusão é sempre verdadeira a implicação também será, isto é, "se $x^5 < 4$ então $x^2 + 1 \geqslant 0$" é verdadeiro porque $x^2 + 1 \geqslant 0$ é verdadeiro. Essa é uma prova trivial.

Consideremos o predicado "se $n > 1$ então $n^2 > n$" para números naturais. Por vacuidade vale "se $0 > 1$ então $0^2 > 0$" e também vale "se $1 > 1$ então $1^2 > 1$", qualquer outro valor de n é maior que 1 e, se $n > 1$ é verdadeiro, então $n^2 > n$ é verdadeiro, pois deduzimos multiplicando ambos os lados na desigualdade da hipótese por n.

Exercício 55. A sentença:

$$\text{para todo } n \in \mathbb{N}^*, \text{ se } n + \tfrac{1}{n} < 2 \text{ então } n^2 + \left(\tfrac{1}{n}\right)^2 < 2$$

é verdadeira? Demonstre ou dê um contraexemplo para justificar a resposta.

2.1.6 Demonstração por casos

O argumento por casos para $P \to Q$ é usado quando P é equivalente na forma $P_1 \vee P_2 \vee \cdots \vee P_n$ baseado na equivalência lógica

$$((P_1 \vee P_2 \vee \cdots \vee P_n) \to Q) \text{ se e somente se } ((P_1 \to Q) \wedge (P_2 \to Q) \wedge \cdots \wedge (P_n \to Q))$$

as implicações $P_i \to Q$ são os casos. Um cuidado importante nessa estratégia é assegurar que $P_1 \vee P_2 \vee \cdots \vee P_n$ equivale a P ou que nenhum caso é deixado de lado. Por exemplo, se P afirma algo sobre inteiros podemos escrevê-la como a disjunção dos casos "inteiros positivos", "inteiros negativos" e o "inteiro nulo" (o 0, que não é negativo, nem positivo), como na sentença

$$\text{para todo inteiro } n,\ n^2 \geqslant n$$

DEMONSTRAÇÃO. Seja n um inteiro artbitrário. Então $n \leqslant -1$ ou $n = 0$ ou $n \geqslant 1$.

1. Caso $n = 0$: se $n = 0$ então $n^2 = 0^2 = 0 = n$, portanto $n^2 \geqslant n$.

2. Caso $n \geqslant 1$: se $n \geqslant 1$ então $n^2 \geqslant n$, multiplicando os dois lados da desigualdade por n, portanto $n^2 \geqslant n$.

3. Caso $n \leqslant -1$: se $n \leqslant -1$ então $n^2 \geqslant n$. Suponha $n \leqslant -1$, então $n < 0$. Se $n < 0$ e $0 \leqslant n^2$ então $n \leqslant n^2$.

Portanto, para todo n natural, $n^2 \geqslant n$. □

TEOREMA 56 *Para todo $n \in \mathbb{Z}$, $n^2 + 3n + 5$ é ímpar.*

DEMONSTRAÇÃO. Seja n um inteiro arbitrário. Vamos provar que $n^2 + 3n + 5$ é ímpar em dois casos: (1) $2 \mid n$ e (2) $2 \nmid n$.

Caso 1: Assuma que $2 \mid n$. Se $2 \mid n$ então $n = 2k$ para algum inteiro k e

$$n^2 + 3n + 5 = (2k)^2 + 3(2k) + 5 = 2(2k^2 + 3k + 2) + 1$$

portanto $n^2 + 3n + 5$ é ímpar.

Caso 2: Assuma $2 \nmid n$. Se $2 \nmid n$ então $n = 2k + 1$ para algum inteiro k e

$$n^2 + 3n + 5 = (2k + 1)^2 + 3(2k + 1) + 5 = 2(2k^2 + 5k + 4) + 1.$$

logo $n^2 + 3n + 5$ é ímpar. Portanto, para todo n inteiro, $n^2 + 3n + 5$ é ímpar. □

Algumas situações não deixam alternativa a não ser uma prova exaustiva, como no próximo exemplo.

TEOREMA 57 *Seja n um número inteiro. Se $1 \leqslant n \leqslant 40$ então $n^2 - n + 41$ é primo.*

DEMONSTRAÇÃO. Defina $f(n) = n^2 - n + 41$.

$f(1) = 41$ é primo, $f(2) = 43$ é primo, $f(3) = 47$ é primo, $f(4) = 53$ é primo, $f(5) = 61$ é primo, $f(6) = 71$ é primo, $f(7) = 83$ é primo, $f(8) = 97$ é primo, $f(9) = 113$ é primo, $f(10) = 131$ é primo, $f(11) = 151$ é primo, $f(12) = 173$ é primo, $f(13) = 197$ é primo, $f(14) = 223$ é primo, $f(15) = 251$ é primo, $f(16) = 281$ é primo, $f(17) = 313$ é primo, $f(18) = 347$ é primo, $f(19) = 383$ é primo, $f(20) = 421$ é primo, $f(21) = 461$ é primo, $f(22) = 503$ é primo, $f(23) = 547$ é primo, $f(24) = 593$ é primo, $f(25) = 641$ é primo, $f(26) = 691$ é primo, $f(27) = 743$ é primo, $f(28) = 797$ é primo, $f(29) = 853$ é primo, $f(30) = 911$ é primo, $f(31) = 971$ é primo, $f(32) = 1033$ é primo, $f(33) = 1097$ é primo, $f(34) = 1163$ é primo, $f(35) = 1231$ é primo, $f(36) = 1301$ é primo, $f(37) = 1373$ é primo, $f(38) = 1447$ é primo, $f(39) = 1523$ é primo, $f(40) = 1601$ é primo. □

Exercício 58. A demonstração por casos em geral é útil para provar propriedades do valor absoluto, porque esse é definido por casos. Sejam a e $b \neq 0$ números reais. Demonstre que $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$.

2.1.7 Demonstrações existenciais

Para provar uma sentença da forma lógica $\exists x \in D,\ P(x)$ podemos exibir um elemento do domínio D para o qual o predicado P vale ou inferir indiretamente que tal elemento existe, por exemplo, derivando uma contradição caso assumamos a não existência de um tal elemento. Esses dois casos são, usualmente, classificadas como demonstrações construtivas e demonstrações não construtivas.

Demonstração construtiva: Exibe um elemento c do universo tal que $P(c)$ seja verdade.

Demonstração não-construtiva: Infere, indiretamente, a existência de um objeto que torna $P(x)$ verdadeira.

Exercício 59. Prove que existe um quadrado perfeito da forma $1 + 13n$, para $n \geqslant 1$ natural.

TEOREMA 60 *Existe um inteiro positivo n que pode ser escrito como a soma de dois cubos de duas maneiras diferentes.*

Demonstração (construtiva). Faça $n = 1729$ e temos $1729 = 10^3 + 9^3 = 12^3 + 1^3$. □

TEOREMA 61 *Existem x, y irracionais tais que x^y é racional.*

Demonstração (não-construtiva). Sabemos que $\sqrt{2}$ é irracional. Prosseguimos em dois casos, o número $\sqrt{2}^{\sqrt{2}}$ é racional ou irracional.

Caso 1: Se $\sqrt{2}^{\sqrt{2}}$ é racional então faça $x = y = \sqrt{2}$ e temos x^y racional.

Caso 2: Se $\sqrt{2}^{\sqrt{2}}$ é irracional então faça $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ e temos

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

que é racional.

Portanto existem x, y irracionais com x^y racional. □

É possível provar que $\sqrt{2}^{\sqrt{2}}$ é irracional, é consequência do teorema de Gelfond–Schneider, um resultado da teoria dos números bastante difícil para exibirmos aqui.

TEOREMA 62 *Para todo racional y, existe um inteiro x tal que $y < x$.*

Demonstração (construtiva). Seja $\frac{p}{q}$ um racional arbitrário. Vamos exibir um inteiro n tal que $\frac{p}{q} < n$.

Faça $n = |p| + 1$. Temos da definição de valor absoluto que $\frac{p}{q} \leqslant |\frac{p}{q}|$. Ademais $|\frac{p}{q}| \leqslant |p|$ e $|p| < |p| + 1$. Portanto $\frac{p}{q} < |p| + 1$. □

TEOREMA 63 *O polinômio $p(x) = x^3 + x - 1$ tem exatamente uma raiz real.*

Nesse enunciado temos duas afirmações a serem demonstradas. A primeira é que o polinômio tem raiz. A segunda é que a raiz do passo anterior é única.

Demonstração (não-construtiva). Seja $p(x) = x^3 + x - 1$. Então p é uma função real e contínua em todo intervalo da reta real.

Pelo Teorema do Valor Intermediário, para todo $b \in [p(0), p(1)]$, existe $a \in [0,1]$ tal que $p(a) = b$. Como $p(0) = -1$ e $p(1) = 1$ temos $0 \in [p(0), p(1)]$ assim fazendo $b = 0$ concluímos, pelo enunciado acima, que existe $a \in [0,1]$ tal que $p(a) = 0$. Portanto a é raiz de p.

Agora, vamos demonstrar que essa raiz é única. A prova é por gg contradição. Suponha que p tenha pelo menos duas raízes. Sejam r_1 e r_2 raízes distintas de $p(x)$, sem perda de generalidade, $r_1 < r_2$.

Como $p(x)$ é contínua em $[r_1, r_2]$ e derivável em (r_1, r_2), pelo Teorema do Valor Médio existe um ponto $c \in [r_1, r_2]$ tal que

$$p'(c) = \frac{p(r_2) - p(r_1)}{r_2 - r_1}$$

mas $p(r_2) - p(r_1) = 0$, portanto $p'(c) = 0$ que é uma contradição pois o $p'(x) = 3x^2 + 1 > 0$ qualquer que seja x. Portanto, não pode haver duas raízes de p. □

Exercício 64. Prove que existe um real que é a raiz quadrada principal de 2. Note que, dado que existe $x \in \mathbb{R}$ positivo tal que $x^2 = 2$, então tal número é irracional de modo que não conseguimos escrever tal número, ou seja, é preciso dar uma prova indireta de sua existência.

2.1.8 Mais exemplos - demonstração de algumas propriedades de inteiros

Vamos começar essa seção com um prova da propriedade arquimediana dos inteiros dada na página 29: *dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existe um n tal que $nb > a$.*

Demonstração do item 38, página 29. Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$, arbitrários.

Se $|b| \neq 0$, então $|b| \geqslant 1$. Logo $(|a| + 1) \cdot |b| \geqslant |a| + 1$ e, também, $|a| + 1 > |a| \geqslant a$, ou seja, $(|a| + 1) \cdot |b| > a$ por transitividade. Agora, se $b > 0$ então tomamos $n = |a| + 1$ e se $b < 0$ então tomamos $n = -(|a| + 1)$. Em ambos os casos $nb > a$. □

Usando o PBO

O próximo resultado tem como corolário que não existe um número inteiro entre dois inteiros "consecutivos" quaisquer.

TEOREMA 65 *Prove que não existe natural p tal que $0 < p < 1$.*

DEMONSTRAÇÃO. A prova é por contradição. Vamos assumir que $p \in \mathbb{N}$ é tal que $0 < p < 1$. Com isso temos que $A := \{x \in \mathbb{N} : 0 < x < 1\}$ é um subconjunto não vazio dos naturais e pelo PBO existe $m = \min(A)$. De $m > 0$, temos $m^2 > 0$. De $m < 1$, temos $m^2 < m$ e como $m < 1$ deduzimos que $m^2 < 1$, logo $m^2 \in A$ e $m^2 < \min(A)$, uma contradição. □

Agora, vamos provar que toda sequência não-crescente de números naturais é constante a partir de um algum momento.

Definição 66. Uma **sequência numérica** $a_0, a_1, a_2, \ldots$, denotada por (a_n) é uma função $f : \mathbb{N} \to A$, onde A é um conjunto de números, tal que $f(n) = a_n$.

A sequência é **não-crescente** se, e só se, $x < y$ implica $f(x) \geqslant f(y)$ e é **não-decrescente** se, e só se, $x < y$ implica $f(x) \leqslant f(y)$.

A sequência é **crescente** se, e só se, $x < y$ implica $f(x) < f(y)$ e é **decrescente** se, e só se, $x < y$ implica $f(y) < f(x)$.

PROPOSIÇÃO 67 *Para toda sequência (a_n) não-crescente de números naturais, existe um natural n_0 a partir do qual a é constante.*

DEMONSTRAÇÃO. Seja (a_n) uma sequência não-crescente de números naturais. Seja f a função que define (a_n).

A imagem da função, $\mathrm{Im}(f)$, é um subconjunto não vazio de naturais. Seja n_0 um natural tal que $f(n_0)$ é o menor elemento de $\mathrm{Im}(f)$, esse menor elemento existe pelo PBO. Como f é não-crescente, se $n > n_0$ então $f(n) \leqslant f(n_0)$, mas $f(n) \not< f(n_0)$ pois $f(n_0)$ é o menor elemento de $\mathrm{Im}(f)$, portanto $n > n_0 \Rightarrow f(n) = f(n_0)$. □

COROLÁRIO 68 (PRINCÍPIO DA DESCIDA INFINITA DE FERMAT) *Não existe uma sequência decrescente de números naturais.* □

Podemos usar o princípio de Fermat para dar a seguinte prova de que $\sqrt{2}$ não é racional.

Esboço de uma demonstração de $\sqrt{2} \notin \mathbb{Q}$ usando o corolário 68. Suponha que existam inteiros p e q tais $\sqrt{2} = \frac{p}{q}$. Então $2q^2 = p^2$, donde concluímos que p é par. Mas se assim for, então $2q^2 = (2p_1)^2$, ou seja, $q^2 = 2k^2$, donde concluímos que p é par, $q = 2q_1$. Repetindo esse argumento encontramos $p > p_1 > p_2 > \cdots$, contrariando o corolário 68. □

Agora provaremos o teorema da divisão euclidiana. Na aritmética, a divisão euclidiana ou divisão inteira é uma operação que, com dois inteiros não nulos chamados dividendo e divisor, associa dois outros inteiros chamados quociente e resto, que é menor que o divisor. Sua principal propriedade é que o quociente e o resto existem e são únicos Essa divisão está na base dos teoremas da aritmética elementar, como a aritmética modular que dá origem à criação de congruências em inteiros e o algoritmo euclidiano para encontrar o maior divisor comum de dois inteiros.

Pode-se também definir uma divisão euclidiana em outros conjuntos, como o anel de polinômios ou outros anéis. O termo "divisão euclidiana" foi surgiu no século XX como uma abreviação para "divisão em anéis euclidianos". Embora a divisão tenha o nome associado a Euclides, acredita-se que ele não conhecia o teorema e que o único método de computação que ele conhecia era a divisão por subtração repetida. Curiosamente, antes da descoberta do sistema numeral hindu-arabico (400 aC), cuja utilização na Europa Ocidental se deve muito a Fibonacci no século XIII, a divisão era extremamente difícil, e apenas os melhores matemáticos eram capazes de fazê-lo.

TEOREMA 69 (TEOREMA DA DIVISÃO EUCLIDIANA) *Para todo inteiro a e todo inteiro $b > 0$ existe um único inteiro q e existe um único inteiro r tal que*

$$a = qb + r \ \ e \ \ 0 \leqslant r < b.$$

DEMONSTRAÇÃO. Sejam a e b inteiros com $b > 0$.

Definimos

$$R := \{a - nb \colon n \in \mathbb{Z}\}$$

e temos que $R \cap \mathbb{N} \neq \varnothing$ pois para $n = -|a|b$ temos $a + |a|b^2 \geqslant a + |a| \geqslant 0$ pertence a $R \cap \mathbb{N}$. Seja r o menor inteiro positivo de $R \cap \mathbb{N}$, que existe pelo princípio da boa-ordem, então $r \geqslant 0$ é da forma

$$r = a - qb$$

para algum q.

Se $r \geqslant b$ então $r - b \geqslant 0$ e

$$r - b = a - (q+1)b \in R \cap \mathbb{N}$$

e $r - b < r$, uma contradição pois r é mínimo de $R \cap \mathbb{N}$.

Falta provar que r e q são únicos. Suponha que $a = q_1 b + r_1$ e $a = q_2 b + r_2$. Se $r_1 \neq r_2$, então $(q_2 - q_1)b = r_1 - r_2$, logo $b \mid r_1 - r_2$. Porém, $-b < r_1 - r_2 < b$, e temos uma contradição. Logo $r_1 = r_2$ e $q_1 = q_2$. □

COROLÁRIO 70 *Para todo natural n, se n não é par então n é ímpar.*

DEMONSTRAÇÃO. Seja n um natural. Pelo teorema da divisão existe $q_1 \mathbb{Z}$ e $r \in \{0, 1\}$ tal que $n = 2q + r$. Se n não é par então $r \neq 0$, logo $r = 1$, ou seja, n é ímpar. □

Exercício 71. Enuncie e prove o teorema da divisão para todo inteiro $b \neq 0$.

Agora, provaremos outro resultado importante, o **teorema fundamental da aritmética** afirma que todo número inteiro maior que 1 é primo ou pode ser decomposto num produto fatores primos e esta decomposição é única a menos da permutações dos fatores. Por exemplo, podemos fatorar 6936 como $23 \cdot 3 \cdot 172$ e não há nenhuma outra fatoração de 6936 como primo ou produto de primos, com exceção de um rearranjo dos fatores acima como, por exemplo, $3 \cdot 23 \cdot 172$.

Como no teorema da divisão, esse resultado pode ser generalizado para outros conjuntos, os anéis de fatoração única, tais como os anéis de polinômios com coeficientes nos números reais ou complexos. Carl Friedrich Gauss, em seu livro *Disquisitiones arithmeticae* desenvolve a aritmética em outras estruturas nos quais a existência de uma fatoração única vale, como é o caso dos polinômios com coeficientes em um corpo e o caso do anel de inteiros algébricos, os inteiros de Gauss. A noção de número primo é então estendida nessas estruturas (polinômios irredutíveis e os números primos de Gauss).

Definição 72. Um número natural maior que 1 é **primo** se, e só se, tem exatamente dois divisores positivos, o 1 e o próprio número. Um número natural maior que 1 que não é primo é dito **composto**, o qual tem um divisor positivos diferente do 1 e do próprio número.

TEOREMA 73 (TEOREMA FUNDAMENTAL DA ARITMÉTICA) *Para todo $n \in \mathbb{N}$, se $n > 1$ então n é primo ou pode ser escrito como produto de números primos, ademais tal escrita é única a menos da ordem com que se escreve os fatores primos.*

DEMONSTRAÇÃO. Seja $n > 1$ um natural. A prova é por contradição. Assuma que exista $n > 1$ natural que não é primo e não pode ser escrito como produto de primos e defina o conjunto não vazio A formado por todos naturais com tal propriedade.

Pelo PBO o conjunto A tem um mínimo m. Como m não é primo, tem um divisor $a \neq 1, m$, isto é, existe $q \in \mathbb{N}$ tal que $m = a \cdot q$. Claramente, $1 < a, q < m$. Como m é mínimo a e q são primos ou produtos de primos e em todos os casos m é produto de primos, assim temos uma contradição. □

Exercício 74. Prove que há um único modo de escrever $n > 1$ como produto de primos, exceto pela ordem dos fatores.

COROLÁRIO 75 *Se $n \neq -1, 0, 1$ é inteiro então existem primos $p_1, \ldots, p_k$ tais que $n = \pm p_1 p_2 \cdots p_k$.*

Vejamos uma prova existencial construtiva para outra propriedade de inteiros dada na página 29:

TEOREMA 76 *Todo $A \subset \mathbb{Z}$ não vazio e limitado inferiormente tem um menor elemento.*

DEMONSTRAÇÃO. Seja $A \subset \mathbb{Z}$ um subconjunto limitado inferiormente e seja m é uma cota inferior de A. Defina o conjunto

$$B = \{a - m \colon a \in A\}.$$

Então $B \subset \mathbb{N}$ e $B \neq \varnothing$, logo, para algum $b \in A$ temos $b - m = \min(B)$. Se $a \in A$ então $a - m \in B$, logo $b - m \leqslant a - m$, portanto $b \leqslant a$, ou seja, $b = \min(A)$. □

Uma aplicação dessa versão do PBO é o seguinte resultado.

PROPOSIÇÃO 77 *Qualquer postagem que custe pelo menos oito reais pode ser feita com selos de 3 e 5 reais.*

Vamos chamar $n \in \mathbb{N}$ de *postal* se n pode ser um valor obtido a partir de selos de 3 e 5 reais. Por exemplo 8 é postal pois $8 = 3 + 5$, também 9 é postal pois $9 = 3 \cdot 3 + 0 \cdot 5$ e 10 é postal pois $10 = 0 \cdot 3 + 2 \cdot 5$.

DEMONSTRAÇÃO. O teorema afirma que para todo elemento de $\{n \in \mathbb{N} \colon n \geqslant 8\}$ é postal. A prova é por contradição.

Suponha que a afirmação do teorema é falsa. Seja $A \subseteq \mathbb{N}$ o subconjunto dos naturais maiores ou iguais a 8 não-postais. Por hipótese $A \neq \varnothing$, portanto tem um menor elemento m.

Como 8 é postal, basta tomar $x = y = 1$, deduzimos que $m \geqslant 9$. Dessa forma, $m - 1 \geqslant 8$ e é postal. Logo existem x_0 e y_0 inteiros tais que $m - 1 = 3x_0 + 5y_0$. Assim, deduzimos

$$\begin{aligned} m &= 3x_0 + 5y_0 + 1 \\ &= 3x_0 + 5y_0 + 3(-3) + 5(2) \\ &= 3(x_0 - 3) + 5(y_0 + 2) \end{aligned}$$

e como m não é postal obtemos uma contradição. □

Se permitimos troco, todo valor pode ser obtido com selos de 3 e 5. Por exemplo, se entregamos 3 selos de 3 e recebemos de volta 1 selo de 5, ficamos com $3 \cdot 3 + 5 \cdot (-1) = 4$ pagos pela postagem.

Exercício 78. Prove que qualquer inteiro z pode se obtido como múltiplo (inteiro) de 3 mais múltiplo (inteiro) de 5.

Exercício 79 (**teorema de Bézout**). Escreva um enunciado preciso e use o PBO para provar a seguinte sentença. Sejam $a, b \in \mathbb{N}$ números coprimos. Existem inteiros x e y tais que $ax + by = 1$ (*dica:* tome o mínimo do conjunto dos números positivos da forma $ax + by$; prove por contradição que esse mínimo é 1).

2.1.9 Considerações sobre a escrita de uma demonstração

Em um sentido técnico e abstrato, uma demonstração matemática é a verificação de uma proposição por uma cadeia de deduções lógicas a partir de um conjunto básico de axiomas, porém o objetivo de uma demostração é fornecer aos leitores provas convincentes para a veracidade de uma afirmação. Para cumprir o objetivo de fornecer aos leitores provas convincentes para a veracidade de uma afirmação uma boa demonstração deve ser clara. Uma prova bem escrita é mais provável de ser uma prova correta, já que os erros são difíceis de esconder. Aqui estão algumas dicas sobre como escrever boas provas:

Indique sua estratégia, uma boa prova começa por explicar a linha geral de raciocínio, por exemplo. "Nós usamos indução em n" ou "Nós provamos por contradição". Isso cria uma imagem mental na qual o leitor pode ajustar os detalhes subsequentes.

Explique seu raciocínio. Muitos estudantes inicialmente escrevem provas da forma como eles computam integrais. O resultado é uma longa sequência de expressões sem explicação. Uma boa prova geralmente parece um ensaio com algumas equações lançadas. Use frases completas. Evite o simbolismo excessivo.

Simplifique, provas longas e complicadas levam o leitor mais tempo e esforço para entender e pode ocultar mais facilmente os erros. Então, uma demonstração com menos passos lógicos é melhor.

Introduza a notação cuidadosamente, às vezes, um argumento pode ser bastante simplificado introduzindo uma variável, elaborando uma notação especial ou definindo um novo termo. Mas faça isso com moderação, já que você exige que o leitor se lembre de todas essas coisas novas. E lembre-se de realmente definir os significados de novas variáveis, termos ou notações; não basta começar a usá-los.

Estruture provas longas. Um programa longo geralmente é dividido em um hierarquia de pequenos procedimentos. As provas longas são iguais. Fatos necessários na sua prova que são fáceis mas não prontamente provados são lemas. Além disso, se você repete essencialmente o mesmo argumento repetidamente, tente capturar esse argumento em um lema.

Conclua. Em algum momento de uma demonstração, você terá estabelecido todos os fatos essenciais que você precisa. Resista à tentação de encerrar e deixar o leitor tirar conclusões corretas. Em vez disso, amarre tudo e explicite a sentença original.

Não seja "telegráfico" como no seguinte exemplo.

Teorema. *Há infinitos números primos.*

DEMONSTRAÇÃO. Vamos assumir que há finitos números primos. Tomemos P o produto desses primos, $P = \prod_{p \text{ primo}} p$.

$$0 < \prod_{p \text{ primo}} \sin\left(\frac{\pi}{p}\right) = \prod_{p \text{ primo}} \sin\left(\pi \frac{1+2P}{p}\right) = 0$$

uma contradição. □

Antes de redigir a sua demonstração, revise sua estratégia e seu rascunho. Pense cuidadosamente em cada passo da prova, se você não sabe explicar claramente um passo, precisa voltar e pensar um pouco mais. Em tese, cada etapa de uma prova deve ser justificada por uma definição ou teorema. Na prática, a profundidade com que se deve fazer isso é uma questão de experiência. Uma justificação pode ser apresentada sem provas apenas se você estiver absolutamente confiante de que está correta o leitor concordará automaticamente que está correto.

Exercícios

1. Escreva as definições de número primo e de número composto. Enuncie, em seguida simbolize na linguagem da lógica (informal) o Teorema Fundamental da Aritmética.

2. Enuncie precisamente[1] cada proposição abaixo, incluindo quantificadores, domínio das variáveis e dê uma prova direta para:

   (a) se a divide b e a divide c então a divide $xb + yc$, quaisquer que sejam x e y inteiros.

   (b) se a divide b e b divide c então a divide c.

   (c) se $a > 0$ é composto então a tem um fator primo p com $1 < p \leqslant \sqrt{a}$.

   (d) se $\text{mdc}(a,b) = 1$ então $\text{mdc}(a^2, b^2) = 1$

3. Enuncie precisamente cada proposição abaixo, incluindo quantificadores, domínio das variáveis e dê uma prova pela contra-positiva:

   (a) se n não tem divisor primo d com $1 < d \leqslant \sqrt{n}$ então n é primo.

   (b) se $x \in B \setminus A$ então $x \notin A \cap B$.

   (c) se $3n + 2$ é ímpar então n é ímpar.

   (d) se $c^5 + 7$ é par, então c é ímpar.

4. Enuncie precisamente cada proposição abaixo, incluindo quantificadores, domínio das variáveis e dê uma prova por contradição:

   (a) se a não divide bc, então a não divide b.

   (b) se $3n + 2$ é ímpar então n é ímpar.

   (c) $\sqrt[3]{3}$ não é racional.

[1] isso não significa usar símbolos, significa dizer *tudo* o que precisa ser dito e *só* o que precisa ser dito

(d) se $d > 1$ e $d \mid n$ então d não divide $n+1$.

(e) Prove que existem infinitos números primos. (Dica: exercício anterior)

5. Justifique os passos do seguinte leitura da demonstração de (2.3).

1) Suponha que 3 divide n
2) Se 3 divide n, então existe $q \in \mathbb{N}$ tal que $n = 3q$
3) $n = 3q$
4) Se $n = 3q$, então $n^2 = 9q^2$
5) Se $n^2 = 9q^2$ então existe $k \in \mathbb{Z}$ tal que $n^2 = 9k$
6) Se existe $k \in \mathbb{Z}$ tal que $n^2 = 9k$ então 9 divide n^2
7) Se $n = 3q$ então 9 divide n^2
8) 9 divide n^2

6. Prove que $n^2 + 1 > 2^n$ sempre que $n \in \{1,2,3,4\}$.

7. Para números reais x e y usamos $\max\{x,y\}$ para denotar o maior deles e usamos $\min\{x,y\}$ para denotar o menor deles. Prove que $\max\{x,y\} + \min\{x,y\} = x + y$.

8. **Desigualdade triangular.** Prove que para todo $x \in \mathbb{R}$, para todo $y \in \mathbb{R}$, vale $|x+y| \leqslant |x| + |y|$.

9. Prove que para todo real x, se $x > 0$ então existe y real tal que $y(y+1) = x$.

10. Sejam A, B, C conjuntos. Prove que se $A \subseteq B$ e $A \cap C = \varnothing$ então $A \subseteq B \setminus C$.

11. **Quantificador de unicidade:** $\exists!$. A proposição $(\exists! x) P(x)$ indica que existe um único x no domínio do discurso tal que $P(x)$ é verdadeiro. Por exemplo, $(\forall n \in \mathbb{N})(\exists! m \in \mathbb{N}) nm = n$ é verdadeiro pois somente o número 1 tem a propriedade de que qualquer outro natural x vezes ele resulta em x.

$$(\exists! x) P(x) \text{ se, e somente se, } (\exists x)\big(P(x) \wedge (\forall y)(P(y) \to x = y)\big). \tag{2.8}$$

Prove que para todo irracional r, existe um único inteiro n tal que $|r - n| < \frac{1}{2}$ (*dica:* use (2.8) mostre que existe n e depois mostre que para qualquer m com a mesma propriedade $m = n$. Nesse último passo pode ser preciso usar a desigualdade triangular).

12. Prove que não há uma quantidade finita de números primos.

13. Prove que não há um "menor racional positivo".

14. Prove que para qualquer natural $n > 1$, existe uma sequência formada por n números naturais consecutivos tal que nenhum deles é primo (*dica:*$(n+1)! + j$ é divisível por j.).

15. Prove que no domínio dos números reais a seguinte sentença é verdadeira:

$$\forall \varepsilon > 0,\ \exists \delta > 0, \forall x \in \mathbb{R},\ \left(|x-3| < \delta \to \left|\frac{2x^2 - 5x - 3}{x-3}\right| < \varepsilon\right).$$

16. $A \subseteq \mathbb{N}$ é dito **limitado superiormente** se existir um natural n tal que

$$\forall x \in A,\ x \leq n \tag{2.9}$$

Um natural n com a propriedade (2.9) e que pertence a A é dito **maior elemento** de A. Demonstre que se $A \neq \varnothing$ é limitado superiormente, então admite maior elemento. Denotamos o maior elemento de A por $\max(A)$.

17. A seguinte estratégia prova que $\sqrt{3} \notin \mathbb{Q}$?

Assuma $\sqrt{3}$ racional. Então $\sqrt{3}$ pode ser representado como $\frac{a}{b}$ onde a e b são coprimos e positivos. Então, $3b^2 = a^2$. Agora, $3 \mid 3b^2$, portanto $3 \mid a^2$, mas então $3 \mid a$. Assim, temos $3b^2 = (3k)^2$, logo $3b^2 = 9k^2$ ou seja $b^2 = 3k^2$ e temos uma contradição.

18. Nesse exercício assuma que todas as variáveis têm mesmo domínio e vamos omiti-lo. Leia atentamente o teorema 80 e a sua demonstração dados abaixo.

TEOREMA 80 *Se existe x tal que $P(x)$ e existe x tal que $Q(x)$ então existe x tal que $P(x)$ e $Q(x)$.*

Em símbolos: $(\exists x,\, P(x)) \wedge (\exists x,\, Q(x)) \rightarrow \exists x\, (P(x) \wedge Q(x))$.

DEMONSTRAÇÃO. Considere o seguinte argumento

1)	$(\exists x,\, P(x))$ e $(\exists x,\, Q(x))$	(premissa)
2)	$\exists x,\, P(x)$	(simplificação de 1)
3)	$P(c)$	(instanciação existencial de 2)
4)	$\exists x,\, Q(x)$	(simplificação de 1)
6)	$Q(c)$	(instanciação existencial de 4)
7)	$P(c)$ e $Q(c)$	(conjunção de 3 e 5)
8)	$\exists x, (P(x)$ e $Q(x))$	(generalização existencial de 7)

□

(a) Dê um contraexemplo para a afirmação feita no teorema, isto é, encontre um domínio D e predicados P e Q sobre elementos de D para o qual a sentença não vale.

(b) Indique o(s) erro(s) na demonstração.

19. Leia com atenção o seguinte teorema e uma suposta demonstração.

TEOREMA 81 *Para todos a, b, c, d números naturais, se c divide a e c divide b e d divide a e d divide b e c não divide d, então dc divide a e dc divide b.*

Em símbolos[a]: $\forall a, b, c, d \in \mathbb{N}, \left(c \,\middle|\, a \text{ e } c \,\middle|\, b \text{ e } d \,\middle|\, a \text{ e } d \,\middle|\, b \text{ e } c \not| d \rightarrow dc \,\middle|\, a \text{ e } dc \,\middle|\, b\right)$.

DEMONSTRAÇÃO. Sejam a, b, c, d números naturais tais que c divide a, c divide b, d divide a, d divide b e c não divide d.
Se d divide a e b, então existem x e y naturais tais que $a = xd$ e $b = yd$.
Se c divide a então c divide xd.
Se c divide xd e não divide d, então c divide x.
Analogamente, se c divide b então c divide yd.
Se c divide yd e não divide d, então c divide y.
Se c divide x e y, então existem z e w tais que $x = cz$ e $y = cw$.
Das conclusões acima temos $a = xd = (cz)d = (dc)z$ e $b = yd = (cw)d = (dc)w$, portanto, dc divide a e dc divide b. □

[a] isso ajudou a fixar as informações?

(a) Dê um contraexemplo para a afirmação feita no teorema.

(b) Indique o(s) erro(s) na demonstração.

20. Dizem que nos seus primeiros anos de Hogwarts, Harry Potter resolveu usar seus poderes para escrever uma prova análoga de que $\sqrt{4}$ não é racional, coisa que quase todo mundo sabe que não é. A prova de Harry Potter foi:

TEOREMA 82 *$\sqrt{4}$ não é racional.*

DEMONSTRAÇÃO. Se $\sqrt{4}$ é racional então existem $a, b \in \mathbb{N}^*$, primos entre si, tais que

$$\frac{a}{b} = \sqrt{4}.$$

Elevando os dois termos da equação ao quadrado, temos

$$a^2 = 4b^2$$

Logo a^2 é divisível por 4 e, portanto, a também o é. Por definição,podemos escrever $a = 4k$, para algum $k \in \mathbb{N}$, e ficamos com

$$(4k)^2 = 4b^2$$

e, portanto

$$16k^2 = 4b^2,$$

ou seja

$$b^2 = 4k^2.$$

Logo b^2 é divisível por 4 e, portanto, b também o é, o que contraria a escolha de a e b primos entre si.
Portanto, $\sqrt{4}$ não é racional. □

Onde está "a mágica"?

21. Seja n um natural. Prove que se n não é um quadrado então $\sqrt{n}$ é irracional (*dica*: exerc. 2, item 4, ou o corolário 68).

22. Prove que existe um racional x e um irracional y tais que x^y é irracional.

23. O que está errado na seguinte demonstração.

TEOREMA 83 *Para todo natural n, $n^2 + n + 1$ é par.*

DEMONSTRAÇÃO. A prova é por contradição, assuma que existem naturais tais que $n^2 + n + 1$ é ímpar e seja A o subconjunto formado por tais números. Pelo PBO, podemos tomar $m = \min A$.
Como $m - 1 \notin S$ temos que $(m-1)^2 + (m-1) + 1$ é par. Porém $(m-1)^2 + (m-1) + 1 = m^2 - m + 1 = (m^2 + m + 1) - 2m$, ou equivalentemente, $m^2 + m + 1 = ((m-1)^2 + (m-1) + 1) - 2m$, que é par e temos uma contradição. □

24. Prove que todo subconjunto não vazio de $\mathbb{N} \times \mathbb{N}$ tem um menor elemento com respeito a relação de ordem definida no exercício 10, página 26,

Complemento: O método probabilístico

O método probabilístico é um método não construtivo usado para provar a existência de um objeto matemático com uma propriedade prescrita. Nas várias estratégias probabilísticas a ideia geral pode ser resumida como: mostrar que escolhendo aleatoriamente objetos de uma classe especificada, a probabilidade de que o resultado seja do tipo prescrito é estritamente maior do que zero, o que indica a existência de tal objeto. Uma explicação intuitiva para essa abordagem é pensar que a probabilidade de que a propriedade prescrita ocorra como a razão do número de objetos com a propriedade pelo número total de objetos. Se esta proporção for positiva, é garantido que deve haver pelo menos uma construção que exiba a propriedade.

Embora esse método de prova use probabilidade, a conclusão final não é probabilística. Este método também é aplicado em outras áreas como a teoria dos números, álgebra, análise real, ciência da computação e teoria da informação.

Seja $\mathcal{H}$ um conjunto cujos elementos são os conjuntos $A_1, \ldots, A_m$ todos eles com k elementos e fixamos $V := \bigcup \mathcal{H}$.

TEOREMA 84 *Se $m < 2^{k-1}$ então é possível pintar os elementos de V com duas cores sem que tenha um A_i com todos os seus elementos da mesma cor.*

DEMONSTRAÇÃO. Para cada elemento de V lançamos uma moeda, se resultar cara pintamos tal elemento de *azul* e se resultar coroa pintamos tal elemento de *vermelho*. Fixado i, a probabilidade com que A_i tem todos os seus elementos azuis é $(1/2)^k$. A probabilidade com que A_i tem todos os seus elementos da mesma cor é $2 \cdot (1/2)^k = 2^{1-k}$.

A probabilidade de existir $i \in \{1,\dots,m\}$ tal que os seus elementos são da mesma cor é $m \cdot 2^{1-k}$.

Pela hipótese em m temos que $m \cdot 2^{1-k} < 2^{k-1} \cdot 2^{1-k} = 1$, portanto, a probabilidade de existir $i \in \{1,\dots,m\}$ tal que os seus elementos são da mesma cor é < 1. Logo a probabilidade com que ocorram as duas cores em cada A_i, para todo $i \in \{1,\dots,m\}$, é maior que 0, ou seja, deve existir um modo de colorir V com duas cores sem que tenha um A_i com todos os seus elementos da mesma cor. □

Dizemos que $H \subset V$ é um *conjunto de acerto* se H encontra todo elemento de $\mathscr{H}$, isto é, $H \cap A_i \neq \varnothing$ para todo i. O próprio V é um conjunto de acerto. Também é qualquer H com $|V| - k + 1$ elementos pois para todo i temos que o número de elementos em A_i somado ao número de elementos de H é $|V| + 1 > |V|$ portanto eles devem ter elemento em comum. Ainda, podemos escolher um elemento de cada A_i para formar um conjunto de acerto com $\leqslant m$ elementos. Claramente, o desafio é encontrar um H tão pequeno quanto possível.

TEOREMA 85 *Existe um conjunto de acerto para $\mathscr{H}$ com no máximo $\left\lceil \frac{|V| \log m}{k} \right\rceil$ elementos.*

DEMONSTRAÇÃO. Sorteamos uniformemente $h := \left\lceil \frac{|V| \log m}{k} \right\rceil$ elementos de V com repetição; para cada um deles, a probabilidade de não estar em A_j é $1 - (k/|V|)$. A probabilidade de nenhum dos sorteados estarem em A_j é $(1 - (k/|V|))^h$.

Usando que $(1 - 1/x)^x < \mathrm{e}^{-1}$ temos

$$\left(1 - \frac{k}{|V|}\right)^h < \mathrm{e}^{\frac{hk}{|V|}} \leqslant \mathrm{e}^{-\log(m)} = \frac{1}{m}.$$

A probabilidade de haver algum $j \in \{1,2,\dots,m\}$ tal que nenhum dos sorteados estarem em A_j é menor que

$$\sum_{j=1}^{m} \frac{1}{m} = 1,$$

portanto, com probabilidade positiva essa seleção define um conjunto com $\leqslant h$ elementos (por causa da repetição) que encontra todos os elementos de $\mathscr{H}$. □

Esses dois teoremas são clássicos em combinatória. De fato, a combinatória é um terreno fértil para o método probabilístico, em parte porque probabilidade está intrinsecamente ligada a contagem, que é uma ferramenta central em combinatória.

Vamos usar o método probabilístico para provar, por contradição, que existem infinitos números primos.

TEOREMA 86 *Há infinitos números primos.*

DEMONSTRAÇÃO. Vamos assumir que M é o maior número primo. Seja R um número aleatório sorteado de acordo com a seguinte regra: $R = 2^{T_2} \cdot 3^{T_3} \cdot 5^{T_5} \cdots M^{T_M}$ onde T_p é um a menos da quantidade de lançamentos de um dado com p faces (as faces são $1,\dots,p$) até obtermos um resultado diferente de 1

$$\mathrm{Prob}\big(T_p = n\big) = \frac{1}{p^n} - \frac{1}{p^{n+1}} = \frac{1}{p^n}\left(1 - \frac{1}{p}\right).$$

Por exemplo, para T_2 se os lançamentos resultam $1,1,1,1,1,2$ então $T_2 = 5$, se o primeiro lançamento é 2 então $T_2 = 0$. Os sorteios são independentes de modo que, por exemplo,

$$\begin{aligned}\mathrm{Prob}(R = 10) &= \mathrm{Prob}(T_2 = 1)\mathrm{Prob}(T_3 = 0)\mathrm{Prob}(T_5 = 1)\mathrm{Prob}(T_7 = 0)\cdots\mathrm{Prob}(T_M = 0)\\ &= \frac{1}{2}\frac{1}{5}\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)\cdots\left(1 - \frac{1}{M}\right)\end{aligned}$$

e, de modo geral,

$$\mathrm{Prob}(R = k) = \frac{1}{k}\prod_p \left(1 - \frac{1}{p}\right)$$

onde o produto é sobre todo primo p. Mas disso temos que

$$\sum_{k \geqslant 1} \mathrm{Prob}(R = k) = \sum_{k \geqslant 1} \frac{1}{k} \prod_p \left(1 - \frac{1}{p}\right) \prod_p \left(1 - \frac{1}{p}\right) \sum_{k \geqslant 1} \frac{1}{k}$$

o lado esquerdo é 1, por ser uma distribuição de probabilidade, e o lado direito é ∞ pois $\sum_{k \geqslant 1} 1/k$ diverge, uma contradição que encerra a prova. □

Capítulo 3

Princípios de Indução Finita e demonstrações por indução

Vimos, e usamos em algumas demonstações, o Princípio da Boa Ordenação (PBO) para os números naturais com respeito a ordem usual

todo $A \subset \mathbb{N}$ não-vazio tem um menor elemento

e, como consequência (provado na página 42), provamos uma versão do PBO para subconjuntos dos inteiros que são limitados inferiormente

todo $A \subset \mathbb{Z}$ não vazio e limitado inferiormente tem um menor elemento.

Ambos são ferramentas que provam teoremas importantes sobre números inteiros como o teorema da divisão, o teorema de Bézout e o teorema fundamental da aritmética. Isso não é por acaso, o PBO é de fato um princípio muito forte.

Esse princípio não vale noutros conjuntos numéricos como $\mathbb{Q}$ e $\mathbb{R}$ com respeito a *ordem canônica*. Por exemplo o intervalo $(0,1]$ em $\mathbb{R}$ não tem menor elemento, enquanto que $[0,1]$ em $\mathbb{R}$ tem menor elemento. Entretanto, é uma consequência da axioma da escolha que todo conjunto não vazio admite uma relação de ordem que o bem-ordena. Embora o axioma afirme que $\mathbb{R}$ pode ser bem ordenado, não sabemos como fazê-lo. Neste texto, por "Princípio da Boa Ordem", ou a forma curta "PBO", referem-se exclusivamente ao enunciado acima a respeito da ordem usual nos naturais e as vezes, por abuso, a versão para inteiros como acima.

3.1 Princípios de indução

Há várias formulações equivalentes para o Princípio de Indução Finita (PIF) e todos podem ser provados a partir do PBO.

TEOREMA 87 (PRINCÍPIO DA INDUÇÃO FINITA (PIF)) *Seja $X \subseteq \mathbb{N}$. Se*

1. *$0 \in X$ e*
2. *para todo $k \in \mathbb{N}$, se $k \in X$ então $k+1 \in X$,*

então $X = \mathbb{N}$.

DEMONSTRAÇÃO. A prova é por contradição. Seja X um subconjunto dos naturais que satisfaz as hipóteses 1 e 2 do teorema. Suponha que a conclusão do teorema seja falsa, ou seja, que $X \subsetneq \mathbb{N}$. Então $A = \mathbb{N} \setminus X$ é não vazio e, pelo PBO, tomamos $m = \min(A)$. De $0 \in X$ temos $m \geqslant 1$, portanto $m-1$ é natural. Pela minimalidade de m temos que $m-1 \notin A$, portanto, $m-1 \in X$. Porém, se $m-1 \in X$ então $m \in X$ pela hipótese 2. Portanto $m \in X$. Agora, e $m \in A = \mathbb{N} \setminus X$e $m \in X$ é uma contradição. Portanto $X = \mathbb{N}$. □

A forma mais usual é enunciada da seguinte forma.

COROLÁRIO 88 (PRINCÍPIO DA INDUÇÃO FINITA (PIF)) *Seja $P(n)$ um predicado de números naturais. Se*

1. *$P(0)$ é verdadeiro e*
2. *para todo $k \geqslant 0$, se $P(k)$ é verdadeiro então $P(k+1)$ é verdadeiro,*

então $P(n)$ é verdadeiro para todo natural n.

DEMONSTRAÇÃO. Seja P um predicado e suponha que vale as hipóteses 1 e 2 dadas. Faça $X = \{k \in \mathbb{N}\colon P(k)\}$ e temos, da hipótese 1 que $0 \in X$ e da hipótese 2, se $k \in X$ então $k+1 \in X$. Assim, estamos nas hipóteses do teorema 87 e podemos concluir que $X = \mathbb{N}$, ou seja, $P(n)$ é verdadeiro para todo natural n. □

TEOREMA 89 (PRINCÍPIO DA INDUÇÃO FINITA COMPLETO (PIFC)) *Seja $X \subseteq \mathbb{N}$. Se*

1. $0 \in X$
2. *para todo $k \in \mathbb{N}$, se $\{0,1,\ldots,k\} \subset X$ então $k+1 \in X$*

então $X = \mathbb{N}$.

DEMONSTRAÇÃO. Seja $X \subseteq \mathbb{N}$ um conjunto que satisfaz as hipóteses do 1 e 2 do teorema 89. Nesse caso, as hipóteses do teorema 87 ficam satisfeitas, donde concluímos que $X = \mathbb{N}$. □

Antes de prosseguirmos, vejamos como podemos deduzir esse teorema do PBO: A prova é por contradição, seja $S := \mathbb{N} \setminus X \neq \varnothing$. Podemos tomar $k \in \mathbb{N}$ tal que $k+1$ seja o menor elemento de S com respeito a ordem dos naturais. Então $x < k+1 \Rightarrow x \in X$ para todo $x \in \mathbb{N}$, o que implica $k+1 \in X$, uma contradição pois $k+1 \in S$.

O seguinte enunciado é a forma mais diretamente usada nas demonstrações por indução.

COROLÁRIO 90 (PRINCÍPIO DA INDUÇÃO FINITA COMPLETO (PIFC)) *Seja $P(n)$ um predicado de números naturais. Se*

1. *$P(0)$ é verdadeiro e*
2. *para todo $k \geqslant 0$, $P(0)$ e $P(1)$ e $\ldots$ e $P(k)$ implica $P(k+1)$,*

então $P(n)$ é verdadeiro para todo natural $n \geqslant 0$.

DEMONSTRAÇÃO. Exercício. □

3.1.1 Indução em subconjuntos dos inteiros limitados inferiormente

Como corolário do PIF ou, mais diretamente, da consequência do PBO para subconjuntos de inteiros limitados inferiormente, temos o seguinte resultado que estende o PIF para subconjuntos dos inteiros limitados inferiormente.

TEOREMA 91 (PRINCÍPIO DA INDUÇÃO FINITA GENERALIZADO (PIFG)) *Sejam $P(n)$ um predicado de números inteiros e $n_0 \in \mathbb{Z}$. Se*

1. *$P(n_0)$ é verdadeiro e*
2. *para todo $z \geqslant n_0$, se $P(z)$ é verdadeiro então $P(z+1)$ é verdadeiro,*

então $P(n)$ é verdadeiro para todo inteiro $n \geqslant n_0$.

DEMONSTRAÇÃO. Sejam P e n_0 como enunciado no teorema. A prova é por contradição. Se existe $z \geqslant n_0$ inteiro que não satisfaz P então o conjunto $A := \{z \in \mathbb{Z}\colon z \geqslant n_0 \text{ e não-}P(z)\}$ é não vazio e limitado inferiormente, portanto, tem $m = \min(A)$.

Pela hipótese 1, $m \geqslant n_0 + 1$, logo $m-1 \geqslant n_0$ e $P(m-1)$ é verdadeiro, por causa da minimalidade de m. Pela hipótese 2, $P(m)$ é verdadeiro e temos uma contradição. Portanto $P(n)$ é verdadeiro para todo inteiro $n \geqslant n_0$. □

A versão completa também vale para subconjuntos de inteiros limitados inferiormente.

TEOREMA 92 (PRINCÍPIO DA INDUÇÃO FINITA COMPLETO GENERALIZADO (PIFCG)) *Sejam $P(n)$ um predicado de números inteiros e $n_0 \in \mathbb{Z}$. Se*

1. *$P(n_0)$ é verdadeiro, e*
2. *para todo inteiro $z \geqslant n_0$, se $P(n_0)$ e $P(n_0+1)$ e $\ldots$ e $P(z)$ é verdadeiro então $P(z+1)$ é verdadeiro,*

então $P(n)$ é verdadeiro para todo inteiro $n \geqslant n_0$.

Para fins didáticos, vamos demonstrar esse teorema transformando o problema em $\mathbb{Z}$ num problema equivalente em $\mathbb{N}$.

DEMONSTRAÇÃO. Sejam P e n_0 como no enunciado do teorema. Defina o conjunto

$$X := \{m \in \mathbb{N}\colon P(m+n_0)\} \subset \mathbb{N}.$$

Então $0 \in X$ pela condição 1 da hipótese do enunciado do teorema. Dado $n \in \mathbb{N}$, suponha que $\{0,1,\ldots,n\} \subset X$. Então $P(n_0)$ e $P(1+n_0)$ e $\cdots$ e $P(n+n_0)$ é verdadeiro e, pela hipótese 2 do enunciado do teorema, temos que e $P(n+1+n_0)$ é verdadeiro, isto é, $n+1 \in X$. Pelo PIFc, teorema 89, $X = \mathbb{N}$, ou seja, $P(m+n_0)$ para todo natural m. Portanto, $P(n)$ é verdadeiro para todo inteiro $n \geqslant n_0$. □

3.1.2 Mais duas variantes

Em alguma situações podem ser úteis as seguintes variantes do PIF.

Exercício 93 (**PIF passo** k). *Seja $P(n)$ um predicado a respeito de $n \in \mathbb{N}$. Se*

1. *$P(0)$ e $P(1)$ e ... e $P(k-1)$ é verdadeiro e*
2. *para todo $n \in \mathbb{N}$, $P(n)$ e $P(n+1)$ e ... e $P(n+k-1)$ verdadeiro implica $P(n+k)$ verdadeiro*

então $P(n)$ para todo $n \in \mathbb{N}$.

TEOREMA 94 (INDUÇÃO PRA FRENTE–PRA TRÁS) *Seja (a_i) uma sequência crescente de números naturais. Seja $P(n)$ um predicado a respeito dos números naturais. Se*

1. *$P(a_i)$ é verdadeiro para todo índice $i \in \mathbb{N}$ e*
2. *para todo natural k, se $P(k+1)$ é verdadeiro então $P(k)$ é verdadeiro,*

então $P(n)$ é verdadeiro para todo natural n.

DEMONSTRAÇÃO. Sejam (a_i) e $P(n)$ como no enunciado e que as hipóteses sejam verdadeiras. A prova é por contradição, suponha que exista k tal que $P(k)$ seja falso. Existe um natural ℓ tal que $a_{\ell-1} < k \leqslant a_\ell$ (justifique).

Definimos o conjunto $A := \{n \in \mathbb{N}\colon a_{\ell-1} < n < a_\ell \text{ e não-}P(n)\}$ que é não vazio, por hipótese. Pelo exercício 16, página 44, podemos tomar $m = \max(A)$. Assim temos que $P(m+1)$ é verdadeiro e pela hipótese 2 do enunciado do teorema $P(m)$ é verdadeiro, uma contradição. Portanto, $P(n)$ é verdadeiro para todo natural n. □

Exercício 95. Demonstre o teorema 94 usando o PIF. (*Dica*: para provar $P(k)$ no passo, defina $Q(n)$ para $n = 0, 1, \ldots, a_\ell - a_{\ell-1}$ pondo $Q(n) = P(a_\ell - n)$, onde a_ℓ é como na demonstração acima; prove $Q(k) = P(a_\ell - k)$ usando indução em n).

3.1.3 Equivalência entre os princípios

Acima deduzimos PIFc de PIF e PIF de PBO. Todos esses princípios são, de fato, teoremas equivalentes. Para provar a equivalência vamos provar que PBO segue de PIFc e teremos as implicações

$$\text{PBO} \Rightarrow \text{PIF} \Rightarrow \text{PIFc} \Rightarrow \text{PBO}.$$

Demonstração de PIFc $\Rightarrow$ PBO. Seja $A \subset \mathbb{N}$ não vazio. Vamos provar que A tem um menor elemento. A prova é por contradição, suponha que A não tem menor elemento.

Definimos o conjunto X como o complemento de A

$$X = \{n \in \mathbb{N}\colon n \notin A\}$$

e vamos provar que X satisfaz as hipóteses de PIFc: (i) $0 \in X$, e (ii) para todo $k \in \mathbb{N}$, se $\{0, \ldots, k\} \subset X$ então $k+1 \in X$.

Se $0 \notin X$ então $0 \in A$, portanto 0 é o menor elemento de A, contradição. Com isso provamos que $0 \in X$.

Seja $k \geqslant 0$ arbitrário e suponha $\{0, \ldots, k\} \subset X$. Se $k+1 \notin X$ então $k+1 \in A$, portanto $k+1$ é o menor elemento de A, já que $\{0, \ldots, k\} \subset X$, contradição. Portanto $k+1 \in X$ e, com k é arbitrário, provamos para todo $k \in \mathbb{N}$, $\{0, \ldots, k\} \subset X$ implica $k+1 \in X$.

Com (i) e (ii) podemos usar o PIFc para concluir que $X = \mathbb{N}$, ou seja $A = \varnothing$, uma contradição. Portanto, A tem menor elemento. □

Exercício 96. Na página 40 provamos, a partir do PBO o Princípio da descida infinita de Fermat (PDI): *não existe uma sequência decrescente de números naturais.* De fato, o PDI é equivalente ao PBO e, portanto, aos PIF. Deduza o PBO do PDI

3.2 Demonstrações por indução

Indução matemática também é uma técnica de prova para sentenças da forma "para todo $n \geqslant a$, $P(n)$". Já vimos alguns exemplos nas demonstrações dos teoremas 89 e 92, da implicação PIFc $\Rightarrow$ PBO.

Numa prova por indução verificamos a validade das duas hipóteses do princípio de indução finita e, se sendo verdadeiras, concluímos que "para todo $n \geqslant a$, $P(n)$". Na verificação das hipóteses, provamos $P(a)$ (isto é, verificamos que a instanciação da variável com a resulta numa sentença verdadeira), a isso chamamos **base da indução**, e provamos a segunda hipótese, que é uma condicional, a isso chamamos **passo da indução**. O passo é provado usando as estratégias que já aprendemos para isso, no caso direto fixamos um k arbitrário, supomos $P(k)$ verdadeiro e provamos que $P(k+1)$ é verdadeiro.

Exemplo 97. *Para todo $n \in \mathbb{N}$, $0+1+\cdots+n = n(n+1)/2$.*

Vamos provar usando indução em n.

base: Para $n = 0$ a igualdade afirmada se verifica $0 = 0(0+1)/2$.

passo: Seja $k \geqslant 0$ um natural arbitrário e suponha que $0+1+\cdots+k = k(k+1)/2$. Precisamos provar que $0+1+\cdots+k+(k+1) = (k+1)(k+2)/2$. Usando a hipótese

$$0+1+\cdots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+2)(k+1)}{2}$$

Portanto, pelo PIF $0+1+\cdots+n = n(n+1)/2$ para todo $n \in \mathbb{N}$.

Exemplo 98. *Para todo $n \geqslant 5$, $2^n > n^2$.*

Vamos provar usando indução em n.

base: Para $n = 5$ a desigualdade afirmada se verifica $2^5 > 5^2$.

passo: Seja $k \geqslant 5$ um natural arbitrário e suponha que $2^k > k^2$. Precisamos demonstrar que $2^{k+1} > (k+1)^2$. Por definição e usando as hipóteses de indução e $k \geqslant 5$

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot k^2 \geqslant k^2 + 2k + 1$$

Portanto, pelo PIFg $2^n > n^2$ para todo $n \geqslant 5$.

Exemplo 99. *Se em 2^n moedas 1 é falsa, mais leve, então é possível descobrir a moeda falsa em n pesagens numa balança de comparação com 2 pratos.*

Vamos provar usando indução em n.

base: Se $n = 0$ então a afirmação vale trivialmente, a única moeda é a falsa.

passo: Seja $k \geqslant 0$ um natural arbitrário e suponha que para 2^k moedas sabemos encontrar a mais leve usando k pesagens. Precisamos demonstrar que com 2^{k+1} moedas, achamos a moeda falsa com $k+1$ pesagens.

De fato, consideremos um conjunto com 2^{k+1} moedas e dividimos as moedas em duas partes iguais de 2^k moedas. Comparamos essas metades usando 1 pesagem e na metade mais leve achamos a moeda falsa com k pesagens, totalizando $k+1$ pesagens.

Portanto, pelo PIF, se em 2^n moedas 1 é mais leve, então é possível descobrir a moeda leve em n pesagens, para qualquer $n \geqslant 0$.

Exemplo 100 (**Desigualdade de Bernoulli**). Para todo $n \in \mathbb{N}$ e todo $h > -1$, vale $(1+h)^n \geqslant 1+hn$.

Seja $h > -1$ um real arbitrário. Vamos provar por indução em n que a desigualdade vale.

base: Se $n = 0$ então $(1+h)^n \geqslant 1+hn$ é verdadeira.

passo: Seja k um natural arbitrário e suponha que $(1+h)^k \geqslant 1+hk$. Vamos provar que $(1+h)^{k+1} \geqslant 1+(k+1)h$. Pela hipótese

$$(1+h)^{k+1} \geqslant (1+h)(1+h)^k \geqslant (1+h)(1+hk) = 1+hk+h+h^2k = 1+h(k+1) \geqslant 1+h(k+1)$$

Portanto, pelo PIF $(1+h)^n \geqslant 1+nh$ para todo $n \in \mathbb{N}$.

Exemplo 101 (**números de Fibonacci**). Os números de Fibonacci F_n, para todo $n \in \mathbb{N}$ são definidos por $F_0 = 0$, $F_1 = 1$ e $F_n + 2 = F_{n+1} + F_n$ para todo n. É sabido que F_n é dada, também, pela expressão

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right). \tag{3.1}$$

Vamos provar por indução em n que a equação (3.1) vale.

base: Se $n = 0$ ou se $n = 1$ vale que (faça as contas)

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

passo: Seja k um natural arbitrário e suponha que

$$F_k = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right) \text{ e } F_{k+1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right).$$

Precisamos provar que

$$F_{k+2} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+2}\right).$$

Por definição $F_{k+2} = F_{k+1} + F_k$, pela hipótese

$$\begin{aligned} F_{k+1} + F_k &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right) + \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k} - \left(\frac{1-\sqrt{5}}{2}\right)^{k}\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k}\left(\frac{1+\sqrt{5}}{2}+1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{k}\left(\frac{1-\sqrt{5}}{2}+1\right)\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k}\left(\frac{1+\sqrt{5}}{2}\right)^{2} - \left(\frac{1-\sqrt{5}}{2}\right)^{k}\left(\frac{1-\sqrt{5}}{2}\right)^{2}\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+2}\right). \end{aligned}$$

Pelo PIF passo 2 (princípio do exercício 93) concluímos que (3.1) vale para todo $n \geqslant 0$.

Exemplo 102 (Teorema Fundamental da Aritmética). *Para todo natural $n \geqslant 2$, n é primo ou pode ser escrito como produto de primos.*

Seja $P(n)$ a sentença *n é primo ou pode ser escrito como produto de primos* (para facilitar a escrita somente). Vamos provar que $P(n)$ vale para todo $n \geqslant 2$.

base: 2 é primo, portanto $P(2)$ é verdadeiro.

passo: Seja $k \geqslant 2$ um natural arbitrário e suponha

$$P(2) \text{ e } P(3) \text{ e } \cdots \text{ e } P(k) \tag{3.2}$$

verdadeiro. Vamos provar que $P(k+1)$ vale em dois casos.

Caso 1: se $k+1$ é primo então $P(k+1)$ é verdadeiro.

Caso 2: se $k+1$ não é primo então $k+1 = ab$ com $2 \leqslant a, b \leqslant k$. Pela hipótese (3.2) valem $P(a)$ e $P(b)$ portanto ab é um produto de primos, portanto $P(k+1)$ é verdadeiro.

Pelo PIFc, $P(n)$ para todo $n \geqslant 2$.

3.2.1 A base é importante

Sem ela poderíamos "demonstrar"

$$n(n+1) \text{ é ímpar para todo } n \geqslant 1$$

(que obviamente não vale) pois conseguimos provar a implicação do passo da indução para essa sentença. Vamos provar

$$\text{para todo } n \geqslant 1,\ n(n+1) \text{ ímpar} \Rightarrow (n+1)(n+2) \text{ ímpar.}$$

Seja $t \geqslant 1$ um natural arbitrário e suponha que $t(t+1)$ é ímpar. Então

$$(t+1)(t+2) = (t+1)t + (t+1)2$$

que é da forma "ímpar + par", portanto ímpar.

3.2.2 O passo é importante

Uma prova descuidada do passo indutivo pode por tudo a perder. Por exemplo, vamos provar que todos os naturais são iguais.

Tomemos $\max\{a,b\}$ como o maior dentre os naturais a e b, por exemplo, $\max\{1,2\} = \max\{2,1\} = 2$ e $\max\{3,3\} = 3$. Seja $P(n)$ a sentença

$$\forall a \in \mathbb{N},\ \forall b \in \mathbb{N},\ (\max\{a,b\} = n \to a = b).$$

e vamos "demonstrar" que $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Se $\max\{a,b\} = 0$ então $a = b = 0$, portanto $P(0)$ é verdadeiro. Agora, seja $t \in \mathbb{N}$ arbitrário e assuma que $P(t)$ é verdadeiro, isto é, que vale

$$\forall a\, \forall b\, (\max\{a,b\} = t \to a = b).$$

Vamos provar que $P(t+1)$ é verdadeiro, isto é, que vale para todos $a, b \in \mathbb{N}$, $\max\{a,b\} = t+1$ implica $a = b$.

Sejam a e b naturais tais que $\max\{a,b\} = t+1$. Se fizermos $x = a-1$ e $y = b-1$, então $\max\{x,y\} = t$ e, pela hipótese da indução, deduzimos que $x = y$. Mas, se $x = y$ então $a = b$. Portanto $a = b$, e com isso temos $P(t+1)$ verdadeiro. Pelo PIF, $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Para concluir, sejam a e b números naturais. Se $\max\{a,b\} = a$ então $a = b$ por $P(a)$. Se $\max\{a,b\} = b$ então $a = b$ por $P(b)$. Logo quaisquer dois números naturais são iguais. □

3.2.3 Outro exemplo de prova errada

Seja $P(n)$ a sentença: *para todo n natural,* $6n = 0$.

Vamos provar $P(n)$ por indução em n. Para $n = 0$ a sentença $P(0)$ é, claramente, verdadeira.

Seja t um natural arbitrário e vamos provar que vale a condicional $P(0)$ e $P(1)$ e $\cdots$ e $P(t) \to P(t+1)$. Assuma $P(0)$ e $P(1)$ e $\cdots$ e $P(t)$. Então $6(t+1) = 6 \cdot t + 6 \cdot 1$ e, por $P(t)$ e $P(1)$ temos $6 \cdot t + 6 \cdot 1 = 0 + 0 = 0$. Portanto $6(t+1) = 0$, ou seja $P(t+1)$. Pelo PIFc, $P(n)$ vale para todo n. □

3.2.4 Desigualdade das médias aritmética e geométrica

A desigualdade entre a média aritmética e a média geométrica (MA–MG) afirma que a média aritmética de uma lista de números reais não negativos é maior ou igual à média geométrica dos números dessa lista. Além disso, vale a igualdade se, e somente se, a lista for constante, isto é, a lista é uma repetição do mesmo número.

Sejam $x_1, x_2, \ldots, x_n$ números reais positivos. Sejam

$$A(x_1, x_2, \ldots, x_n) = \frac{x_1 + x_2 + \cdots + x_n}{n}$$

a **média aritmética** desses números e

$$G(x_1, x_2, \ldots, x_n) = \sqrt[n]{x_1 \cdot x_2 \cdots x_n}$$

a **média geométrica** desses números.

Teorema 103 (MA–MG) *$x_1, x_2, \ldots, x_n$ números reais positivos.*

$$A(x_1, x_2, \ldots, x_n) \geqslant G(x_1, x_2, \ldots, x_n)$$

com igualdade se, e só se, $x_1 = x_2 = \cdots = x_n$.

Primeiro, vamos provar por indução que MA–MG vale quando n é potência de 2, ou seja, por indução em $k \geqslant 1$ que $A(x_1, x_2, \ldots, x_{2^k}) \geqslant G(x_1, x_2, \ldots, x_{2^k})$.

Para a base dessa indução, tome $k = 1$ e MA–MG afirma que

$$\frac{x_1 + x_2}{2} \geqslant \sqrt{x_1 \cdot x_2}$$

o que segue de $\left(\sqrt{x_1} - \sqrt{x_2}\right)^2 \geqslant 0$ com igualdade se, e só se, $x_1 = x_2$ (verifique).

Para o passo dessa indução, tome k arbitrário e assuma que MA–MG vale para qualquer lista com 2^k números reais positivos. Tome $x_1, x_2, \ldots, x_{2^{k+1}} \in \mathbb{R}^+$. Primeiro, note que

$$\frac{x_1 + x_2 + \ldots + x_{2^{k+1}}}{2^{k+1}} = \frac{1}{2}\left(\frac{x_1 + x_2 + \ldots x_{2^k}}{2^k} + \frac{x_{2^k+1} + x_{2^k+2} + \ldots x_{2^{k+1}}}{2^k}\right)$$

agora, aplicamos a hipótese indutiva no lado direito

$$\frac{x_1 + x_2 + \ldots + x_{2^k}}{2^k} \geqslant \sqrt[2^k]{x_1 \cdot x_2 \cdots x_{2^k}}$$

com igualdade se, e só se $x_1 = x_2 = \cdots = x_{2^k}$, e

$$\frac{x_{2^k+1} + x_{2^k+2} + \ldots x_{2^{k+1}}}{2^k} \geqslant \sqrt[2^k]{x_{2^k+1} \cdot x_{2^k+2} \cdots x_{2^{k+1}}}$$

com igualdade se, e só se, $x_{2^k+1} = x_{2^k+2} = \cdots = x_{2^{k+1}}$, e em seguida usamos MA–MG para dois números

$$\frac{1}{2}\left(\sqrt[2^k]{x_1 \cdot x_2 \cdots x_{2^k}} + \sqrt[2^k]{x_{2^k+1} \cdot x_{2^k+2} \cdots x_{2^{k+1}}}\right) \geqslant \sqrt[2^{k+1}]{x_1 \cdots x_{2^k} \cdot x_{2^k+1} \cdot x_{2^k+2} \cdots x_2^{k+1}}$$

com igualdade se, e só se, $x_1 \cdot x_2 \cdots x_{2^k} = x_{2^k+1} \cdot x_{2^k+2} \cdots x_{2^{k+1}}$, portanto

$$\frac{x_1 + x_2 + \ldots + x_{2^{k+1}}}{2^{k+1}} \geqslant \sqrt[2^{k+1}]{x_1 \cdots x_{2^k} \cdot x_{2^k+1} \cdot x_{2^k+2} \cdots x_2^{k+1}}$$

com igualdade se, e só se,

1. $x_1 = x_2 = \cdots = x_{2^k}$,
2. $x_{2^k+1} = x_{2^k+2} = \cdots = x_{2^{k+1}}$, e
3. $x_1 \cdot x_2 \cdots x_{2^k} = x_{2^k+1} \cdot x_{2^k+2} \cdots x_{2^{k+1}}$

logo, se e só se $x_1 = x_2 = \cdots = x_{2^k} = x_{2^k+1} = x_{2^k+2} = \cdots = x_{2^{k+1}}$. Pelo PIF, a desigualdade MA–MG vale para qualquer lista com 2^k números reais positivos, para todo $k \geqslant 1$.

Para concluir usamos indução de novo, agora a versão "para trás". Tomando $a_i = 2^i$ no teorema 94, a demonstração acima prova a base da indução.

Para o passo da indução, tomamos $j \geqslant 2$ arbitrário e assumimos que MA–MG vale para qualquer lista com j números reais positivos. Vamos provar que vale para $x_1, x_2, \ldots, x_{j-1}$. Pela hipótese indutiva

$$\frac{x_1 + x_2 + \ldots + x_{j-1} + G(x_1, x_2, \ldots, x_{j-1})}{j} \geqslant \sqrt[j]{x_1 \cdot x_2 \cdots x_{j-1} \cdot G(x_1, x_2, \ldots, x_{j-1})}$$

reescrevendo lado esquerdo

$$\frac{x_1 + x_2 + \ldots + x_{j-1} + G(x_1, \ldots, x_{j-1})}{j} = \frac{(j-1)A(x_1, x_2, \ldots, x_{j-1}) + G(x_1, \ldots, x_{j-1})}{j}$$

e reescrevendo lado direito

$$\begin{aligned}\sqrt[j]{x_1 \cdot x_2 \cdots x_{j-1} \cdot G(x_1, x_2, \ldots, x_{j-1})} &= \sqrt[j]{\big(G(x_1, \ldots, x_{j-1})\big)^{j-1} \cdot G(x_1, x_2, \ldots, x_{j-1})} \\ &= G(x_1, \cdots, x_{j-1})\end{aligned}$$

e a desigualdade inicial fica

$$(j-1)A(x_1, x_2, \ldots, x_{j-1}) + G(x_1, \ldots, x_{j-1}) \geqslant jG(x_1, \ldots, x_{j-1})$$

donde concluímos que

$$A(x_1, x_2, \ldots, x_{j-1}) \geqslant G(x_1, \ldots, x_{j-1}).$$

Falta verificar a condição de igualdade, que deixamos como exercício.

Portanto, pelo teorema 94 (indução "pra frente–pra trás"), concluímos que MA–MG vale para qualquer lista com $n \geqslant 1$ números reais positivos. □

Exercício 104. Prove que dentre todos os triângulos de mesmo perímetro, o equilátero é o de maior área.

Exercício 105. Considere a sequência (a_n) definida por $a_0 = 1$ e $a_n = \left(1 + \frac{1}{n}\right)^n$. Prove usando indução que essa sequência é crescente. Prove usando a desigualdade MA–MG que essa sequência é crescente.

3.3 Definições recursivas

Quando a indução é usada para definir funções e objetos matemáticos chamamos de definição recursiva. Conhecemos vários exemplos de definição recursiva:

1. o fatorial: $0! = 1$ e, para todo $n > 0$, $(n+1)! = (n+1) \cdot n!$;
2. o somatório: $\sum_{i=0}^{0} x_i = x_0$ e, para todo n, $\sum_{i=0}^{n+1} x_i = x_{n+1} + \sum_{i=0}^{n} x_i$;
3. o produtório: $\prod_{i=0}^{0} x_i = x_0$ e, para todo n, $\prod_{i=0}^{n+1} x_i = x_{n+1} \cdot \prod_{i=0}^{n} x_i$;
4. a união: $\bigcup_{i=0}^{0} A_i = A_0$ e, para todo n, $\sum_{i=0}^{n+1} x_i = x_{n+1} + \sum_{i=0}^{n} x_i$;
5. a interseção: $\bigcap_{i=0}^{0} A_i = A_0$ e, para todo n, $\bigcap_{i=0}^{n+1} A_i = A_{n+1} \cap \left(\bigcap_{i=0}^{n} A_i\right)$;
6. exponencial: $a^0 = 1$ e, para todo n, $a^{n+1} = a^n \cdot a$;
7. sequência de Fibonacci: $F_0 = 0$, $F_1 = 1$ e $F_n = F_{n-1} + F_{n-1}$ para todo $n \geqslant 2$.

Podemos definir recursivamente o produto cartesiano de mais de dois conjuntos. De um modo geral, se $A_1, A_2, \ldots, A_n$ são conjuntos não vazios

$$\prod_{i=1}^{n} A_i = \begin{cases} A_1 & \text{se } n = 1 \\ \left(\prod_{i=1}^{n-1} A_i\right) \times A_n & \text{se } n > 1 \end{cases}$$

Definimos $(a_1, a_2, \ldots, a_n) = (a_1)$ se $n = 1$ e $(a_1, a_2, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$ se $n > 1$ então

$$\prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \colon a_i \in A_i (\forall i)\}.$$

No caso em que os conjuntos $A_1, A_2, \ldots, A_n$ são iguais a A denotamos por A^n o produto cartesiano $\prod_{i=1}^{n} A_i$.

Funções definidas recursivamente Definimos qualquer função $f \colon \mathbb{N} \to A$, ou uma sequência (a_n) de elementos de A modo que $a_n = f(n)$, recursivamente em duas etapas: na *base* especificamos o valor da função f em $0, \ldots, k$ e no *passo* damos uma regra para encontrar o valor de $f(n)$, $n \geqslant k$, em função de seus valores no inteiros menores, $f(n-1), f(n-2), \ldots, f(n-k-1)$ em função de n. Por exemplo,

$$f(0) = 0,\ f(n+1) = f(n) + g(n)$$

em que g é uma função qualquer definida em $\mathbb{N}$. Tal definição é chamada de **definição recursiva** ou indutiva. Uma **equação de recorrência** é uma expressão que define uma sequência recursivamente. As funções definidas recursivamente estão **bem definidas** se dado qualquer n podemos usar as duas partes da definição para encontrar o valor da função no ponto n de forma inequívoca.

Exemplo 106 (**fatorial**). O fatorial de qualquer número natural fica bem definido por $f \colon \mathbb{N} \to \mathbb{N}$ dada por $f(0) = 1$ e $f(n+1) = (n+1) \cdot f(n)$. Nesse caso, $f(n)$ é denotado por $n!$.

Note que podemos usar o PIF para verificar que f está bem definida. Chame de X o conjunto dos $n \colon \mathbb{N}$ para os quais sabemos calcular $f(n)$. Certamente, $0 \in X$; por outro lado, de $f(n+1) = (n+1) \cdot f(n)$ concluímos que, para todo n, se $n \in X$ então $n+1 \in X$. Portanto pelo PIF $X = \mathbb{N}$.

Exemplo 107. A sequência de Fibonacci (F_n) é (bem) definida por $F_0 = 0$, $F_1 = 1$ e $F_{n+2} = F_{n+1} + F_n$.

Nesse caso, o PIF passo 2 (exercício 93, página 50), garante que F está bem definida pois sabemos calculá-la em 0 e em 1, e se sabemos calculá-la em k e em $k+1$, também sabemos em $k+2$, para todo k.

Exemplo 108 (**juro composto**). Se começamos uma poupança com um capital de C unidades monetárias, após n meses o montante poupado supondo $i \in (0,1)$ fixo como a taxa de juros mensal é $M_{n+1} = M_n + iM_n$ (e $M_0 = C$). Se poupamos D_n unidades monetárias no mês n ($D_0 = C$) e o aplicamos nessa poupança

$$M_0 = C,\ M_{n+1} = (1+i)M_n + D_{n+1}.$$

Exemplo 109 (**progressões aritmética e geométrica**). Uma progressão aritmética que começa em $a \in \mathbb{R}$ e tem razão $r \in \mathbb{R}$ é uma sequência (a_n) tal que $a_0 = a$ e $a_{n+1} = a_n + r$ para todo $n \in \mathbb{N}$.

Uma progressão geométrica que começa em $a \in \mathbb{R}$ e tem razão $r \in \mathbb{R}$ é uma sequência (a_n) tal que $a_0 = a$ e $a_{n+1} = a_n \cdot r$ para todo $n \in \mathbb{N}$.

Exemplo 110. O método de Newton–Raphson para achar zero de função real, quando aplicado a $x^2 - a$ computa, aproximadamente, a raiz quadrada de a. A partir de $x_0 = 1$ podemos computar $\sqrt{2}$ usando

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{2}{x_n}\right).$$

Exemplo 111 (**mapa logístico**). O mapa logístico é uma equação de recorrência frequentemente dada como um exemplo de como o comportamento complexo e caótico pode surgir a partir de equações não lineares muito simples

$$x_{n+1} = r x_n (1 - x_n)$$

onde r é uma constante e x_0 um valor inicial dado. Essa equação foi popularizado em um artigo de 1976 do biólogo Robert May, em parte como um modelo demográfico em tempo discreto. Nesse caso estuda-se o comportamento assintótico de (x_n) variando o parâmetro $r \in [0,4]$, o período das órbitas são descritas pelo seu célebre diagrama de bifurcações

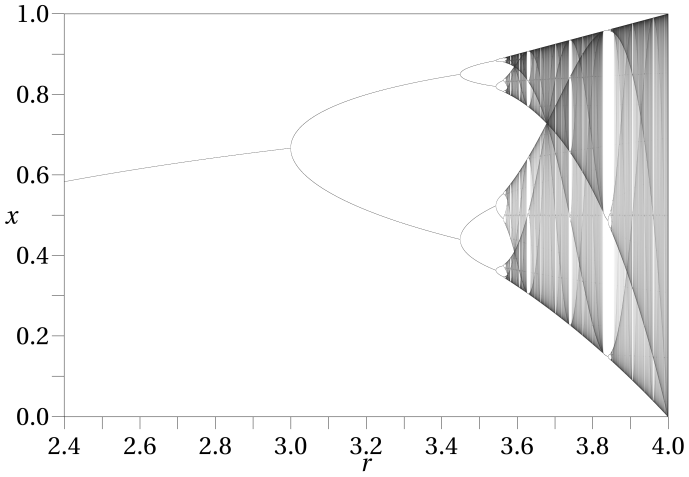


Figura 3.1: diagrama de bifurcações do mapa logístico.

Uma função φ satisfaz uma recorrência para (a_n) se $\varphi(n) = a_n$. Do exemplo 101 temos que

$$\varphi(x) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^x - \left(\frac{1-\sqrt{5}}{2}\right)^x\right)$$

satisfaz a recorrência que define os números de Fibonacci. Uma vantagem dessa expressão é que torna, em princípio, mais fácil o cálculo de número de Fibonacci grandes com F_{2019}, por exemplo.

Essa função φ é chamada de solução da equação de recorrência. Uma **solução** para uma relação de recorrência é uma *forma fechada* da função que satisfaz. Uma **forma fechada** é uma expressão matemática que pode ser avaliada com um número "pequeno" de operações, em geral, as operações aritméticas usuais e as funções bem conhecidas como, por exemplo, n-ésima raiz, exponencial, logaritmo, funções trigonométricas e funções hiperbólicas inversas. Uma recorrência sempre tem uma função que a satisfaz (aquela que a recorrência define), porém pode não ter uma solução (uma forma fechada).

Veremos na seção 5.3 uma técnica que permite encontrar solução de alguns tipos de equações de recorrência. Em todo caso é sempre fácil, usando indução, verificar se uma expressão é solução de uma recorrência.

Por exemplo, podemos provar por indução que a sequência $a_n = nr + a$, para todo n, é uma solução para a recorrência da progressão aritmética que começa em a e tem razão r. De fato, a base $(n = 0)$ é verdadeira, $a_0 = 0r + a = a$ portanto confere com a definição. Seja k um natural arbitrário e suponha que $a_k = kr + a$. Vamos provar que $a_{k+1} = (k+1)r + a$. Temos $a_{k+1} = a_k + r$ por definição e $a_k = kr + a$ por hipótese. Portanto, $a_{k+1} = (k+1)r + a$. Portanto, pelo PIF, para todo n, $a_n = nr + a$.

Exercício 112. Use o PIF para provar que uma função F definida pela especificação de $F(0)$ e uma regra para obtenção de $F(n+1)$ a partir de $F(n)$ está bem definida.

Exercício 113. Use o PIFc para provar que uma função F definida especificando $F(0)$ e uma regra para obter $F(n+1)$ dos valores $F(k)$ para $k = 0, 1, 2, \ldots, n$ está bem definida.

Conjuntos definidos recursivamente As definições recursivas de conjuntos tem duas etapas que correspondem a base e o passo indutivo. Na base especificamos uma coleção inicial de elementos e no passo especificamos uma ou mais regras para "adicionar" novos elementos e para "não adicionar" outros elementos. Além disso, especificamos uma regra de fechamento, estabelecendo que somente os elementos obtidos por aplicação das duas etapas pertencem ao conjunto que está sendo definido. Normalmente, a condição de fechamento é assumida implicitamente, uma vez que é padrão.

Exemplo 114. Vamos definir recursivamente o conjunto $I \subseteq \mathbb{N}$ por

1. $1 \in I$;
2. para todo $a \in \mathbb{N}$, se $a \in I$ então $a + 2 \in I$;
3. somente os naturais obtidos pelas regras acima pertencem a I.

Vamos assumir a convenção de que os elementos dos conjuntos definidos recursivamente são só aqueles dados pelas regras da base e do passo, de modo que no exemplo acima poderíamos ter omitido o item 3. Note que essa condição é necessária pois, por exemplo, as outras duas condições são verdadeiras para $\mathbb{N}$: $1 \in \mathbb{N}$ e se $a \in \mathbb{N}$ então $a + 2 \in \mathbb{N}$.

Tal conjunto I do exemplo 114 é o subconjunto dos números naturais ímpares. Para provar que todo elemento de I é ímpar, suponha o contrário, que existe ao menos um natural em I não ímpar. Seja m o menor natural em I que não é ímpar, que existe pelo PBO. Certamente $a \neq 1$, portanto $a = b+2$ para algum $b \in I$. Pela minimalidade de a deduzimos que b é ímpar, portanto, $b+2$ é ímpar, uma contradição. Agora, vamos provar que todo natural ímpar pertence a I. Por indução que $2n+1 \in I$ para todo natural n. Se $n = 0$ então $2n+1 = 1 \in I$. Seja k um natural arbitrário e assuma que $2k+1 \in I$. Mas $2(k+1)+1 = (2k+1)+2$ e, por definição, $(2k+1)+2 \in I$, logo $2(k+1)+1 \in I$. Pelo PIF temos $2n+1 \in X$ para todo n.

Exercício 115. Para o conjunto I do exemplo 114 prove que qualquer A que satisfaz as duas regras de definição $A \supseteq I$. Prove também que a interseção de todos os conjuntos que satisfazem as duas regras de definição é I.

Exercícios

1. Considere o predicado sobre os números naturais $P(n)$: "Se $n > 1$ então $n^2 > n$". Prove $P(0)$. Em que método de prova se encaixa sua demonstração?

2. Demonstre usando indução:

   (a) para todo $n \geqslant 1$, $9 + 9\cdot 10 + 9\cdot 10^2 + \cdots + 9\cdot 10^{n-1} = 10^n - 1$.

   (b) para todo $n \geqslant 1$, $1/(1\cdot 2) + 1/(2\cdot 3) + \cdots + 1/(n\cdot n+1) = 1 - 1/(n+1)$.

   (c) para todo $n \geqslant 3$, $((n+1)/n)^n < n$.

   (d) para todo $n \geqslant 1$, $(1+1/1)(1+1/2)\cdots(1+1/n) \leqslant n+1$

   (e) para todo $n \geqslant 1$, $a^n < 1$ para todo $0 \leqslant a < 1$

   (f) para todo $n \geqslant 1$,
   $$\frac{1}{2n} \leqslant \frac{1\cdot 3\cdots(2n-1)}{2\cdot 4\cdots(2n)} \leqslant \frac{1}{\sqrt{n+1}}$$

   (g) para todo $n \geqslant 1$, Se $x_1, x_2, \ldots, x_n$ são números reais então
   $$|x_1 + x_2 + \cdots x_n| \leqslant |x_1| + |x_2| + \cdots |x_n|.$$

3. Ache uma falha na seguinte prova por indução.

Teorema *Todos os marcianos são da mesma cor (verde, como sabemos).*

DEMONSTRAÇÃO. Vamos provar por indução sobre o número de marcianos em Marte (não vale contestar a existência de marcianos).

Base: Se o número de marcianos é 1, todos os marcianos são da mesma cor.

Passo: Suponha que existem n marcianos numerados de 1 até n. Removendo um marciano $m \in \{1,\ldots,n\}$ de Marte temos, pela hipótese do passo indutivo, que os $n-1$ marcianos restantes são da mesma cor. Resta descobrir a cor do marciano m. Removendo um marciano $\ell \in \{1,\ldots,n\}$ com $\ell \neq m$ temos, pelo mesmo motivo, que os marcianos restantes, inclusive m, são da mesma cor. Portanto, todos os marcianos $1,\ldots,n$ são da mesma cor. □

---

4. Prove usando a variante do exercício 93 da indução que qualquer valor maior ou igual a oito pode ser obtido com cédulas de 5 e 3 reais (*dica*: bases 8,9,10)

5. Prove usando indução que todo número natural não-nulo pode ser expresso como soma de potências distintas de 2.

6. Prove usando indução que se $n \geqslant 3$ pontos distintos sobre um círculo são conectados consecutivamente com segmentos de reta, então a soma dos ângulos internos do polígono resultante é $(n-2)180^o$.

7. Prove usando indução que existem 2^n seqüências de n bits. Deduza que o número de subconjuntos de um conjunto com n elementos é 2^n.

8. Para todo natural n, mostre que uma grade de quadrados $2^n \times 2^n$ (conforme Figura 1(b)) com qualquer um de seus quadrados removidos pode ser coberta por ladrilhos de tamanho fixo em forma de L (conforme Figura 1(a)).

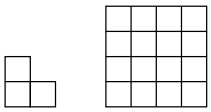


Figura 3.2: (a) Ladrilho em L. (b) Grade de quadrados $2^2 \times 2^2$.

9. Prove usando indução as seguintes afirmações para os números de Fibonacci.
   (a) $F_0^2 + \cdots + F_n^2 = F_n F_{n+1}$.
   (b) $F_0 + \cdots + F_{2n} = F_{2n+1}$.
   (c) $F_{n-1}F_{n+1} + F_n^2 = (-1)^{n+1}$, para todo $n \geqslant 1$.
   (d) $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$, para todo $n \geqslant 1$.
   (e) F_{5n} é divisível por 5.
   (f) F_{3n} é par.
   (g) $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$.
10. Encontre $f(1)$, $f(2)$, $f(3)$, e $f(4)$ se $f(n)$ for definido recursivamente por $f(0) = 1$ e para $n > 0$, $f(n+1) = 2^{f(n)}$.
11. Determine se cada uma das definições propostas é uma definição recursiva válida de uma função $f : \mathbb{N} \to \mathbb{Z}$.
   (a) $f(0) = 0$, $f(n) = 2f(n-2)$ para todo $n \geqslant 1$.
   (b) $f(0) = 1$, $f(n) = f(n-1) - 1$ para todo $n \geqslant 1$.
   (c) $f(0) = 2$, $f(1) = 3$, $f(n) = f(n-1) - 1$ para todo $n \geqslant 2$.
   (d) $f(0) = 1$, $f(1) = 2$, $f(n) = 2f(n-2)$ para todo $n \geqslant 2$.
   (e) $f(0) = 1$, $f(n) = 3f(n-1)$ se n é ímpar e $n \geqslant 1$ e $f(n) = 9f(n-2)$ se n é par e $n \geqslant 2$.
12. Considere um conjunto S de números naturais definido recursivamente da seguinte maneira: (1) $3 \in S$; (2) se $x \in S$ e $y \in S$ então $x + y \in S$. Todo elemento de S é obtido somente por aplicação das regras anteriores. Prove que s é o conjunto dos naturais múltiplos de 3.
13. Sejam $A_1, A_2, \ldots, A_n$ conjuntos e $n \geqslant 2$. Suponha que para dois conjuntos quaisquer A_i e A_j vale que $A_i \subseteq A_j$ ou $A_j \subseteq A_i$. Prove, por indução, um desses conjuntos é subconjunto de todos eles.
14. Seja r um número real tal que $r + \frac{1}{r}$ seja um inteiro. Prove que $r^{100} + \frac{1}{r^{100}}$ também é um inteiro.
15. Prove que para todo $n \geqslant 6$, um quadrado pode ser dissecado em n quadrados, não necessariamente todos do mesmo tamanho.
16. Mostre que $2^n - 1$ é múltiplo de 3 para todo $n \in \mathbb{N}$ par.
17. Seja P um polígono no plano. *Triangular* um polígono é traçar diagonais pelo interior do polígono de modo que as diagonias não se cruzem e cada região criada é um triângulo. Um triângulo é exterior se 2 de seus 3 lados são lados do polígono. Prove que se um polígono de n lados, $n \geqslant 4$, for triangulado então pelo menos dois triângulos são exteriores.
18. Prove usando indução que o termo geral de uma progressão geométrica com termo inicial r e razão r é $x_n = ar^n$ para todo $n \geqslant 0$.
19. Defina a sequência (x_n) de números reais pela recorrência: $x_0 = 1$ e $x_{n+1} = \frac{1}{2}\left(x_n + \frac{2}{x_n}\right)$.

    Prove que $1 \leqslant x_n \leqslant \frac{3}{2}$ para todo n.

    Prove que $x_{n+1} - \sqrt{2} = \frac{1}{2x_n}(x_n - \sqrt{2})^2$ para todo n.
20. Dois jogadores se alternam nas jogadas em que retiram 1, 2 ou 3 palitos de um monte com n palitos. Mostre que o primeiro jogador a jogar tem uma estratégia vencedora se, e só se, n divido por 4 deixa resto diferente de 1.
21. Prove usando indução em n que a soma $\sum_{t=1}^{x} t^n$ é um polinômio de grau $n+1$ em x.

22. Prove usando indução que a sequência $\left(1+\frac{1}{n}\right)^n$ é crescente.

23. Considere $S \subseteq \mathbb{N}$ definido recursivamente por $0 \in S$ e, para todo n, se $n \in S$ então $2n+1 \in S$. De uma definição não recursiva para S e prove que o conjunto da sua definição é de fato o mesmo conjunto que o definido recursivamente.

24. Suponha que um casal de urubus começa a dar crias com dois anos de idade, e produz 6 crias (três casais) de urubuzinhos a cada ano. Suponha que um lixão começou a ser frequentado por 1 casal recém-nascido e que nenhum urubu é acrescentado ou eliminado do lixão. Escreva uma definição recursiva para o número de urubus que existem no ano n.

25. Qual é o erro da seguinte demonstração por indução que "prova" a identidade

$$\sum_{i=1}^{n} i = \frac{(n+1/2)^2}{2}.$$

Base da indução. O caso $n = 1$ vale como pode ser facilmente verificado, o que deixamos para o leitor.

Passo da indução. Seja $k \geqslant 1$ um inteiro qualquer e suponha que vale $\sum_{i=1}^{k} i = (k+1/2)^2/2$. Então

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\
&= \frac{(k+1/2)^2}{2} + k + 1 \\
&= \frac{k^2 + k + 1/4 + 2k + 2}{2} \\
&= \frac{(k+1)^2 + (k+1) + 1/4}{2} \\
&= \frac{(k+1+1/2)^2}{2}
\end{aligned}$$

26. Qual é o erro na seguinte dedução por indução para a sentença "para qualquer conjunto de n retas no plano, se não há quaisquer duas delas paralelas, então todas se encontram num ponto". Para $n = 1$ e para $n = 2$ a sentença é, claramente, verdadeira. Seja $k \geqslant 2$ um inteiro arbitrário e assuma que $P(k)$ é verdadeiro. Considere um conjunto qualquer de $k+1$ retas no plano, dadas por $r_1, r_2, \ldots, r_{k+1}$, em que quaisquer duas não são paralelas. Pela hipótese da indução $r_1, r_2, \ldots, r_k$ se encontram em um ponto p. Também pela hipótese da indução $r_2, r_3, \ldots, r_{k+1}$ se encontram em um ponto q. Como r_2 e r_3 estão nos dois conjuntos, $p = q$, portanto, $r_1, r_2, \ldots, r_{k+1}$ se encontram em um ponto. Pelo PIF, a sentença enunciada vale para todo $n \geqslant 1$.

27. Qual é o erro na seguinte dedução por indução para a sentença "Para qualquer $m \geqslant 2$, se exatamente uma dentre m moedas for falsificada e pesa menos do que o resto, então a moeda leve pode ser identificada com no máximo quatro pesagens em balança de pratos". Demonstração: (base) se existem apenas duas moedas, apenas uma pesagem é necessária. (Passo) Suponha que a sentença seja verdadeira para $m \geqslant 2$ moedas e considere um punhado de $m+1$ moedas, das quais apenas uma é mais leve. Remova uma moeda e aplique a hipótese de indução para as moedas restantes. Se a moeda mais leve não for descoberta dentre essas m moedas em quatro pesagens, então o moeda posta de lado é a falsa, assim a sentença é verdadeira para $m+1$ moedas, completando a etapa indutiva. Pelo princípio de indução a afirmação é verdadeira para qualquer número $m \geqslant 2$ de moedas.

Capítulo 4

Relações

Vamos relembrar que uma relação com domínio A e contradomínio B, ambos não vazio, é um subconjunto de um produto cartesiano $A \times B$. Se $A = B$ escrevemos A^2 para $A \times B$ e dizemos que $R \subset A^2$ é uma relação sobre A, ou em A. Usualmente, $R \subset A \times B$ e $(a,b) \in R$ escrevemos $a\ R\ b$. Por exemplo, $<$ é uma relação sobre $\mathbb{N}$ e ao invés de escrevermos $(x,y) \in <$ escrevemos $x < y$, como em $3 < 4$ ao invés de $(3,4) \in <$. Ademais, no que se refere a notação, é mais comum usarmos símbolos como $\sim$, $\equiv$, $\simeq$, $\approx$ em vez de R, S ou qualquer letra do alfabeto.

Propriedades de relações

Uma relação $\sim$ sobre um conjunto A não vazio pode ou não ter uma ou mais das seguintes propriedades

reflexiva para todo $a \in A$, $a \sim a$;

irreflexiva para todo $a \in A$, $a \not\sim a$;

simétrica para todo $a \in A$, para todo $b \in A$, se $a \sim b$ então $b \sim a$;

antissimétrica para todo $a \in A$, para todo $b \in A$, se $a \sim b$ e $b \sim a$ então $b = a$;

transitiva para todo $a \in A$, para todo $b \in A$, para todo $c \in A$, se $a \sim b$ e $b \sim c$ então $a \sim c$.

Uma relação pode ser simétrica e antissimétrica ao mesmo tempo, como $\{(1,1)\}$ sobre $\{1\}$, ou pode não ser nem simétrica nem antissimétrica, como $\{(1,2)\}$ sobre $\{1,2\}$. Uma relação pode não ser reflexiva e nem irreflexiva, porém uma relação não pode ser ao mesmo tempo reflexiva e irreflexiva sobre A (dê um exemplo). Por exemplo, as relações sobre $A = \{1,2,3,4\}$

1. $R_1 = \{(1,1),(1,2),(2,1),(2,2),(3,3),(3,4),(4,1),(4,4)\}$ é reflexiva.
2. $R_2 = \{(1,1),(1,2),(2,1)\}$ é simétrica.
3. $R_3 = \{(1,1),(1,2),(2,1),(2,2),(3,3),(4,1),(1,4),(4,4)\}$ é reflexiva e simétrica.
4. $R_4 = \{(2,1),(3,1),(3,2),(4,1),(4,2),(4,3)\}$ é irreflexiva, antissimétrica e transitiva.
5. $R_5 = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$ é reflexiva, antissimétrica e transitiva.
6. $R_6 = \{(3,4)\}$ é irreflexiva, antissimétrica e transitiva.

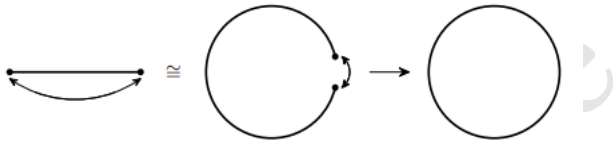
Exercício 116. A seguir, considere $A = \{1,2,3,4\}$ e $B = \{1,2,3\}$ e classifique, quanto as propriedades acima, as relações

1. $R_1 = \{(1,2),(2,1),(1,3),(3,1)\}$.
2. $R_2 = \{(1,1),(2,2),(3,3)\}$.
3. $R_3 = \{(1,1),(2,2),(3,3),(2,3)\}$.
4. $R_4 = \{(1,1),(2,3),(3,3)\}$.
5. $R_5 = \{(1,2),(2,3),(3,1)\}$.

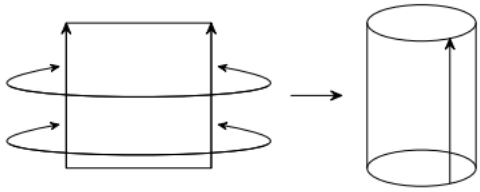
4.1 Relação de equivalência

Relação de equivalência é um tipo de relação ubíqua em matemática, usada, por exemplo, na definição de cardinalidade, na construção dos números inteiros e dos racionais a partir dos números naturais, na definição de objetos geométricos como a garrafa de Klein e a fita de Möbius.

Dizendo de modo bastante ingênuo, as relações de equivalência permitem construções de novos conjuntos a partir de um conjunto dado onde tratamos elementos diferentes do conjunto dado como iguais no novo conjunto. Por exemplo, em certas situações pode se interessante estudar a circunferência como o conjunto dos pontos obtidos de um intervalo quando identificamos (tratamos como iguais) os seus extremos



estudar o cilindro como o conjunto dos pontos obtidos de um retângulo quando identificamos (tratamos como iguais) dois de seus lados paralelos



oi, ainda, estudar o toro como o conjunto dos pontos obtidos de um retângulo quando identificamos (tratamos como iguais) seus lados paralelos

Definição 117. Uma **relação de equivalência** em um conjunto A é uma relação $\sim$ que satisfaz as propriedades reflexiva, simétrica e transitiva.

Por exemplo

1. $=$ é uma relação de equivalência em $\mathbb{N}$.
2. $\leqslant$ não é uma relação de equivalência em $\mathbb{N}$.
3. Se T e S são triângulos no plano euclideano e $T \cong S$ se os triângulos são semelhantes, então $\cong$ é relação de equivalência sobre o conjunto de todos os triângulos no plano.
4. Semelhança de matriz é uma relação de equivalência sobre o conjuntos de todas as matrizes quadradas de ordem n de números reais.
5. $\equiv \pmod 3$ é a relação dada pelos pares de inteiros que deixam o mesmo resto quando divididos por 3, assim $13 \equiv 22 \pmod 3$ e $7 \not\equiv 13 \pmod 3$. Essa relação é de equivalência.
6. $\subset$ não é relação de equivalência sobre o conjunto das partes de A.

Em $\mathbb{R}$ a relação $x \sim y$ se, e só se, $|x-y| < 1$ é reflexiva, simétrica e transitiva?

Definição 118. Seja $\sim$ uma relação de equivalência qualquer sobre o conjunto $A \neq \varnothing$ e $x \in A$, a **classe de equivalência** de x é o subconjunto

$$[x]_\sim = \{b \in A \colon b \sim x\}$$

de A formado por todos os elementos de A equivalentes a x. O elemento dentro dos colchetes, nesse caso x, é chamado de **representante** da classe.

Por causa da transitividade da relação qualquer elemento da classe pode ser seu representante, pois ambos definem a mesma classe de equivalência.

PROPOSIÇÃO 119 *Sejam $\sim$ uma relação de equivalência sobre um conjunto A. Para quaisquer $a, b \in A$ são equivalentes as sentenças*

1. $a \sim b$,
2. $[a]_\sim = [b]_\sim$,
3. $[a]_\sim \cap [b]_\sim \neq \varnothing$.

DEMONSTRAÇÃO. Vamos provar a equivalência entre os itens 1 e 2. Sejam $a, b \in A$ com $b \sim a$. Para todo $c \in [a]_\sim$ vale $c \sim a$, portanto, $c \sim b$ pela transitividade, logo $c \in [b]_\sim$. Por argumento análogo, se $c \in [b]_\sim$ então $c \in [a]_\sim$. Assim $[a]_\sim = [b]_\sim$. Agora, assumimos que $[a]_\sim = [b]_\sim$. Se $[a]_\sim = [b]_\sim$ então $a \sim b$. Assim provamos

$$a \sim b \text{ se, e só se, } [a]_\sim = [b]_\sim. \tag{4.1}$$

Para provar a equivalência das três afirmações e suficiente provar que 1 implica 3 e que 3 implica 2. Que 1 implica 3 é imediato.

Provamos que 3 implica 2, pela contrapositiva. Se $[a]_\sim \neq [b]_\sim$ então, por (4.1), segue que $a \not\sim b$, logo para todo $c \in A$ vale $c \sim a$, se e só se $c \not\sim b$ (por transitividade), de modo que $[a]_\sim \cap [b]_\sim = \varnothing$. □

Exemplo 120. Em $\mathbb{Z}$ definimos a relação *"congruência módulo 3"* pondo, para quaisquer inteiros a, b, que $a \equiv b \pmod 3$ se, e só se, a e b deixam o mesmo resto quando divididos por 3. Essa relação é de equivalência e tem, pela proposição acima e o teorema da divisão euclidiana, três classes de equivalência

$$\begin{aligned}
[0]_{\equiv_3} &= \{3k \colon k \in \mathbb{Z}\},\\
[1]_{\equiv_3} &= \{3k+1 \colon k \in \mathbb{Z}\},\\
[2]_{\equiv_3} &= \{3k+2 \colon k \in \mathbb{Z}\}.
\end{aligned}$$

Qualquer múltiplo de três define a mesma classe de equivalência do 0, qualquer inteiro que deixa resto 1 quando dividido por 3 define a mesma classe de equivalência do 1 e qualquer inteiro que deixa resto 2 quando dividido por 3 define a mesma classe de equivalência do 2.

Exemplo 121. Tomemos o intervalo $I = [0,1]$ da reta real. Definimos uma relação de equivalência formada pelos pares (x,x) para todo $x \in I$ mais os pares $(0,1)$ e $(1,0)$. As classes de equivalência dessa relação são $[x] = \{x\}$ para $x \in (0,1)$ e $[0]$, que é a mesma que $[1]$.

Exemplo 122. No produto $I \times I$, definimos uma relação de equivalência formada pelos pares $\big((x,y),(x,y)\big) \in (I \times I) \times (I \times I)$ para todo $(x,y) \in I \times I$ mais os pares $\big((0,y),(1,y)\big)$ para todo $y \in I$. As classe são $\{(0,y),(1,y)\}$ para cada $y \in I$ mais os unitários $\{(x,y)\}$ para $x \in (0,1)$ e $y \in I$.

Notemos que no caso do exemplo 120 acima, $[0]_{\equiv_3} \cup [1]_{\equiv_3} \cup [2]_{\equiv_3} = \mathbb{Z}$ e isso, de fato, é uma propriedade das classes de uma relação de equivalência.

Para todo $A \neq \varnothing$ e todo $a \in A$, se $\sim \subseteq A \times A$ é relação de equivalência, então da propriedade reflexiva segue que $a \in [a]_\sim$ de modo que $A \subseteq \bigcup_{a \in A} [a]_\sim$. Por outro lado, $[a]_\sim \subseteq A$ por definição, logo $\bigcup_{a \in A} [a]_\sim \subseteq A$. Portanto,

$$A = \bigcup_{a \in A} [a]_\sim. \tag{4.2}$$

TEOREMA 123 (TEOREMA FUNDAMENTAL DAS RELAÇÕES DE EQUIVALÊNCIA) *Se $\sim$ é uma relação de equivalência sobre o conjunto $A \neq \varnothing$ então $A/\!\sim$ é uma partição de A. Por outro lado, qualquer partição P de A define uma relação de equivalência $\sim_P$ em A tal que as partes da partição de A são as classes de equivalência de A por $\sim_P$.*

DEMONSTRAÇÃO. Sejam A e $\sim$ como dados no enunciado. Da proposição 119 e equação (4.2), $A/\sim$ é uma partição de A.

Agora, vamos considerar uma partição $\mathscr{A}$ de A e definir a relação $\sim_P$ em A por $x \sim_P y$ se, e só se, x e y estão numa mesma parte da partição. Tal relação é reflexiva pois para todo $a \in A$ existe um $B \in \mathscr{A}$ tal que $a \in B$ pelo item 3 da definição de partição. A relação é simétrica pois para todos $a, b \in A$, se existe um $B \in \mathscr{A}$ tal que $\{a, b\} \subseteq B$ então $\{b, a\} \subseteq B$. A relação é transitiva pois para todos $a, b, c \in A$ se existe um $B \in \mathscr{A}$ tal que $\{a, b\} \subseteq B$ e existe um $C \in \mathscr{A}$ tal que $\{b, c\} \subseteq C$ então, como $b \in B \cap C$, temos $B = C$ pelo item 2 da definição de partição.

Ainda, se X é uma parte da partição então $X \neq \varnothing$, logo podemos tomar $x \in X$. Por definição $y \in X$ se, e só se, $y \sim_P x$. Ademais, $y \sim_P x$ se, e só se, $y \in [x]_{\sim_P}$. Portanto, $X = [x]_{\sim_P}$. Assim, as partes da partição de A são as classes de equivalência de A por $\sim_P$. □

Se $\sim$ é uma relação de equivalência sobre A, então chamamos de **conjunto quociente** de A pela relação de equivalência $\sim$ o conjunto das classes de equivalência da relação

$$A/\sim = ([a]_\sim : a \in A).$$

Exemplo 124. No caso da relação *"congruência módulo 3"* o conjunto quociente $\mathbb{Z}/\equiv_3$ é o conjunto

$$\left\{ [0]_{\equiv_3}, [1]_{\equiv_3}, [2]_{\equiv_3} \right\}$$

e $\mathbb{Z}/\equiv_3$ é, usualmente, denotado por $\mathbb{Z}_3$.

Exemplo 125. No caso do exemplo 121 o conjunto quociente é um conjunto de pontos topologicamente idêntico a uma circunferência. No caso do exemplo 122 o conjunto quociente é um conjunto de pontos topologicamente idêntico a um cilindro.

Exercícios

1. Prove ou dê contraexemplo: Para todo R_1 e todo R_2, se R_1 e R_2 são relações de equivalência sobre um conjunto A então $R_1 \cap R_2$ é uma relação de equivalência sobre A.

2. Sejam A um conjunto não vazio, $\mathfrak{P}$ o conjunto de todas as partições de A e $\mathfrak{R}$ o conjunto de todas as relações de equivalência sobre A.

   Prove que $f : \mathfrak{R} \to \mathfrak{P}$ dada por $f(R) = \{[a]_R : a \in A\}$ para todo $R \in \mathfrak{R}$ é uma função bijetiva.

3. Explique o que está errado na seguinte demonstração sobre uma relação R sobre A:

   TEOREMA 126 *Se R é uma relação simétrica e transitiva então R é uma relação reflexiva.*

   DEMONSTRAÇÃO. Seja x um elemento de A. Para todo y, se $x\,R\,y$ então $y\,R\,x$, pois a relação é simétrica. Se $x\,R\,y$ e $y\,R\,x$, então $x\,R\,x$ pela transitividade. Portanto, R é reflexiva. □

   ---

4. Seja $f : X \to Y$ uma função qualquer. Defina a relação K em X por $x\,K\,y$ se, e só se, $f(x) = f(y)$. Prove que essa relação é de equivalência e que $[x]_K = f^{-1}(f(x))$. Essa relação é chamada de relação de equivalência do núcleo de f.

5. Seja A um conjunto e $\sim$ uma relação de equivalência sobre A. Prove que a função $\pi : A \to A/\sim$ dada por $\pi(a) = [a]_\sim$, chamada de **projeção canônica**, é sobrejetiva.

6. O que é a relação de equivalência do núcleo de uma projeção canônica?

7. Sejam $f : A \to B$ uma função e $\sim$ uma relação de equivalência sobre A tal que se $a \sim b$ então $f(a) = f(b)$, para quaisquer $a, b, \in A$. Prove que existe uma única função $g : A/\sim \to B$ tal que $f = g \circ \pi$, onde π é a projeção canônica.

8. Sejam $f : A \to B$ uma função sobrejetiva e $\sim$ uma relação de equivalência sobre A tal que $a \sim b$ se e somente se $f(a) = f(b)$, para quaisquer $a, b, \in A$. Prove que existe uma única função injetiva $g : A/\sim \to B$ tal que $f = g \circ \pi$, onde π é a projeção canônica.

9. Prove que entre quaisquer duas classes de equivalência de $\equiv \pmod 3$ há uma bijeção.

10. Sejam $\sim$ e $\cong$ duas relações de equivalência sobre o mesmo conjunto A. Se $a \sim b$ implica $a \cong b$ para todos $a, b \in A$, então dizemos que $\sim$ é uma relação que **refina** $\cong$. Dê uma relação de equivalência que refina a relação $\equiv \pmod 3$.

11. Demonstre que se $\sim$ **refina** $\cong$ então cada classe de equivalência de $\sim$ é um subconjunto de uma classe de equivalência de $\cong$.

Complemento: Construção dos Inteiros

Intuitivamente, digamos que queremos construir um conjunto de números onde $n-k$ faça sentido quaisquer que sejam os naturais n,k, por exemplo $4-11$. Façamos $-7 := 4-11$. Mas então há várias representações $-7 := 4-11 = 3-10 = 5-12 = \cdots$. Notemos que se $a-b=n-m$ então $a+m=b+n$ e se fizermos todas essas representações do -7 equivalentes temos uma relação de equivalência. Formalmente, considere a relação $\mathbf{Z} \subset \mathbb{N}\times\mathbb{N}$ definida por

$$(a,b)\mathbf{Z}(n,m) \text{ se, e só se } a+m=b+n$$

$\mathbf{Z}$ que é uma relação de equivalência.

Para cada (a,b), a *classe de equivalência de* (a,b) é o conjunto

$$[(a,b)] := \{(n,m)\in\mathbb{N}\times\mathbb{N}\colon (a,b)\mathbf{Z}(n,m)\}.$$

Por exemplo,

$$[(1,2)] = \{(0,1),(1,2),(2,3),(3,4),\ldots\}$$
$$[(5,2)] = \{(3,0),(4,1),(5,2),(6,3),\ldots\}$$

Notemos que $[(1,2)] = [(2,3)] = [(0,1)] \neq [(5,2)] = [(4,1)]$.

$\mathbb{Z}$ é o conjunto dessas classes de equivalência e seus elementos são chamados números inteiros.

Denotamos

$$0 := [(0,0)] = \{(n,n)\colon n\in\mathbb{N}\}$$
$$1 := [(1,0)] = \{(n+1,n)\colon n\in\mathbb{N}\}$$
$$-1 := [(0,1)] = \{(n,n+1)\colon n\in\mathbb{N}\}$$
$$-a := [(0,a)] = \{(n,n+a)\colon n\in\mathbb{N}\}$$

Se p é a classe $[(a,b)]$ e q a classe $[(n,m)]$, definimos $p+q$ como a classe de equivalência

$$p+q := [(a+n,b+m)]$$

Notemos que $[(1,2)]+[(5,2)] = [(0,1)]+[(3,0)]$. Definimos $p\cdot q$ como a classe de equivalência

$$p\cdot q := [(a\cdot n+b\cdot m, a\cdot m+b\cdot n)]$$

Definimos

$$p-q := p+(-q)$$

e definimos

$$p\leq q \Leftrightarrow q-p\in\mathbb{N}$$

para quaisquer inteiros p e q.

4.2 Relação de ordem

A relação $\leqslant$ sobre $\mathbb{N}$ comporta-se, em alguns aspectos, da mesma forma que $\subseteq$ sobre $2^{\mathbb{N}}$ (não há nada de especial em ser $\mathbb{N}$ aqui) e da mesma forma que $|$ sobre $\mathbb{N}$. Essas são relações de ordem.

Definição 127. Uma relação $\preceq$ sobre um conjunto A não vazio é uma **relação de ordem** em A se valem as propriedades reflexiva, antissimétrica e transitiva. O par $(A,\preceq)$ é chamado de **ordem parcial** e dizemos que A **é conjunto parcialmente ordenado por** $\preccurlyeq$.

Exemplo 128. São exemplos de ordens parciais $\left(2^{\mathbb{Z}},\subseteq\right)$, $(\mathbb{Z},\leqslant)$ e a ordem lexicográfica $(\mathbb{N}\times\mathbb{N},\trianglelefteq)$ definida no exercício 10, página 26.

Uma ordem é classificada como "parcial" pelo seguinte motivo. Há uma diferença importante entre, por exgemplo, as relações de ordem $\subseteq$ sobre $2^{\mathbb{Z}}$ e $\leqslant$ sobre $\mathbb{Z}$. Na primeira, a inclusão $\subseteq$, pode haver elementos incomparáveis, por exemplo, os conjuntos $\{1,2\}$ e $\{2,3\}$ são incomparáveis pois

$$\{1,2\}\not\subseteq\{2,3\} \text{ e } \{2,3\}\not\subseteq\{1,2\}$$

enquanto que quaisquer dois números inteiros x e y são comparáveis pela relação, isto é, vale que

$$x \leqslant y \text{ ou } y \leqslant x.$$

Seja A um conjunto não vazio e $\preccurlyeq$ um relação de ordem em A. O elementos $a, b \in A$ são ditos **comparáveis** por $\preccurlyeq$ se, e só se, vale que

$$x \preccurlyeq y \text{ ou } y \preccurlyeq x.$$

Caso contrário são ditos **incomparáveis**.

Definição 129. Escrevemos $x \prec y$ se, e só se, $x \preccurlyeq y$ e $x \neq y$. O $\prec$ é uma relação sobre o mesmo conjunto que $\preccurlyeq$, chamada de **ordem estrita** definida por $\preccurlyeq$. O par $(A, \prec)$ é a **ordem estrita associada** a ordem parcial $(A, \preccurlyeq)$.

De modo geral, uma relação sobre A é uma **ordem estrita** se é uma relação irreflexiva e transitiva.

Exercício 130. Seja $\prec$ uma ordem estrita sobre A. Prove que $\prec$ é assimétrica, ou seja, para quaisquer $a, b \in A$, se $a \prec b$ então $b \not\prec a$.

Diagrama de Hasse

Quando $x \preccurlyeq y$ e não existe $z \in A$ tal que $x \prec z \prec y$ então dizemos que y **cobre** x. Essa relação "cobre" é um subconjunto da relação $\preccurlyeq$. Usamos essa subrrelação para, em alguns casos, montar um diagrama que representa a ordem parcial, conhecido como **diagrama de Hasse**, que é bastante útil para ilustrar propriedades de uma ordem parcial. Representamos cada elemento de A como um ponto no plano (vértice) e desenhamos um segmento ou curva (aresta) que vai para cima de x para y sempre que y cobre x e $y \neq x$. A relação de ordem é indicada tanto pelas arestas quanto pelo posicionamento relativo dos vértices. As ordens são desenhadas de baixo para cima: se um elemento x é menor que y, então existe um caminho de x para y que é direcionado para cima. Pode ser necessário, no desenho, que as arestas conectando os elementos se cruzem fora dos vértices, mas uma aresta deve ligar só dois vértices, a saber, o elementos da ordem relacionados por "cobre". Tal diagrama determina unicamente sua ordem parcial. A figura 4.1 abaixo exibe um diagrama de Hasse da ordem parcial $\big(\wp(\{1,2,3\}), \subseteq\big)$. Na figura 4.2, temos um

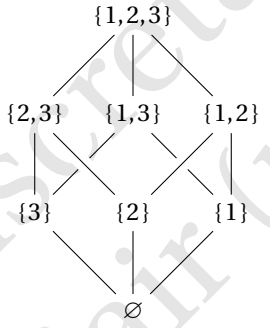


Figura 4.1: diagrama de Hasse de $\big(\wp\{1,2,3\}, \subseteq\big)$.

diagrama da ordem formada pelos divisores de 60 (em $\mathbb{N}$) com a ordem $|$.

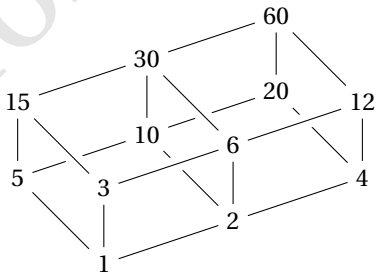


Figura 4.2: diagrama de Hasse dos divisores de 60 com a ordem $|$.

Elementos máximo, mínimo, maximal e minimal

Alguns elementos, quando existem, desempenham um papel especial numa ordem parcial $(A, \preccurlyeq)$. Temos que $x \in A$ é

minimal se, e só se, para todo $y \in A$,

$$y \preccurlyeq x \text{ implica } y = x.$$

mínimo se, e só se, para todo $y \in A$,

$$x \preccurlyeq y.$$

maximal se, e só se, para todo $y \in A$,

$$x \preccurlyeq y \text{ implica } y = x.$$

máximo se, e só se, para todo $y \in A$,

$$y \preccurlyeq x.$$

Há ordens parciais onde não ocorrem nenhum desses casos como, por exemplo, em $(\mathbb{Z}, \leqslant)$. Também, um conjunto parcialmente ordenado pode ter vários elementos minimais e vários elementos maximais. Por exemplo, o conjunto formado por todos os subconjuntos de A com k elementos, para algum $0 < k < n$, parcialmente ordenados por $\subseteq$ é formado por elementos incomparáveis entre si, todos os elementos são maximais e todos são minimais; não há máximo e não há mínimo.

No conjunto dos divisores *próprios* de 60 (em N) com a ordem de divisibilidade, que tem uma representação dada pelo diagrama da figura 4.3, percebemos que essa ordem parcial não tem máximo nem mínimo. Os elementos $12, 20, 30$ são elementos

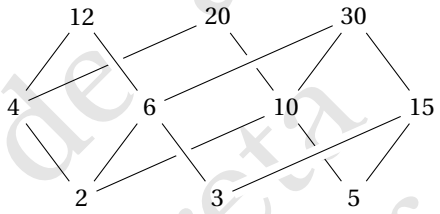


Figura 4.3: diagrama de Hasse dos divisores próprios de 60.

maximais $2, 3, 5$ são minimais. Se consideramos todos os divisores (figura 4.2), notamos que 1 é mínimo e 60 é máximo.

Exemplo 131. Dado um conjunto A com n elementos, tomamos $\wp(A) \setminus \{\varnothing, A\}$, isto é, os **subconjuntos próprios** de A, parcialmente ordenados por pela relação de inclusão. Nesse caso há n elementos maximais e n minimais (justifique essa afirmação).

Quando A é um conjunto de conjuntos e a relação de ordem é a inclusão $(\subseteq)$ um elemento minimal de $(A, \subseteq)$ é um conjunto que não contém propriamente nenhum outro elemento de A; um elemento maximal de $(A, \subseteq)$ é um conjunto que não está contido propriamente nenhum outro elemento de A. Por exemplo, se $A = \{\{2\}, \{1,2\}, \{1,3\}, \{1,2,4\}, \{3,4,5\}\}$ então $\{1,2,4\}$ não é minimal pois contém propriamente $\{1,2\} \in A$. São os elementos minimais: $\{2\}$, $\{1,3\}$ e $\{3,4,5\}$. O elemento $\{2\}$ não é maximal, nem $\{1,2\}$. Os elementos maximais do conjunto A são $\{1,3\}$, $\{1,2,4\}$ e $\{3,4,5\}$.

Exemplo 132. Para o conjunto $A = \{1,2,3,4,5,6\}$ munido da relação de ordem $\preccurlyeq$ dada por

$$\{(1,3),(2,3),(1,4),(2,4),(3,4),(5,6),(1,1),(2,2),(3,3),(4,4),(5,5),(6,6)\}$$

o número $2 \in A$ é um elemento *minimal* de pois não existe nenhum par $(a,2)$, $a \neq 2$, na relação. Os elementos minimais $(A, \preccurlyeq)$ são 1, 2 e 5. Quais são os maximais? Há máximo? Há mínimo? A figura 4.4 é uma representação dessa ordem parcial.

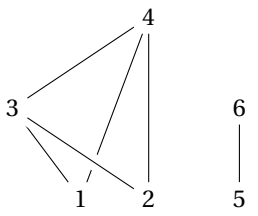


Figura 4.4: diagrama de Hasse do exemplo 132.

Exemplo 133. Tomemos $\mathbb{N}\setminus\{0,1\}$ com a relação de divisibilidade (denotada $|$). O número 21 não é minimal pois, por exemplo, $3|21$. O número 17 é minimal pois não existe a tal que $a|17$ (a única possibilidade seria o 1 que não está no conjunto). Note que os elementos minimais de $(\mathbb{N}\setminus\{0,1\},\preccurlyeq)$ são os números primos.

Já em $(\mathbb{N}\setminus\{0\},|)$, o 1 é o único minimal, que também é mínimo.

PROPOSIÇÃO 134 *Numa ordem parcial, se existe mínimo então ele é único e se existe máximo ele também é único.*

DEMONSTRAÇÃO. Seja $(A,\preccurlyeq)$ uma ordem parcial. Suponha que x_1 e x_2 sejam mínimos dessa ordem. Como x_1 é mínimo, $x_1 \preccurlyeq x_2$; analogamente $x_2 \preccurlyeq x_1$, portanto, $x_1 = x_2$ pela propriedade antissimétrica.

A demonstração para máximo é análoga. □

Exemplo 135. Considere o conjunto $\wp^{\leqslant 3}(\mathbb{N})$ de todos os subconjuntos de $\mathbb{N}$ com no máximo três elementos e ordenados por inclusão $\subseteq$. O (único) mínimo dessa ordem parcial é o $\varnothing$. Todos os subconjuntos de 3 elementos são maximais pois não há subconjuntos com 4 elementos de modo que, por exemplo, nenhum elemento de $\wp^{\leqslant 3}(\mathbb{N})$ contém $\{0,1,2\}$, nem $\{1,2,3\}$. Como consequência de haver dois elementos maximais inferimos que não há máximo nessa ordem parcial.

Cadeias

Numa ordem parcial podem ocorrer subconjuntos nos quais quaisquer dois elementos são comparáveis. É o caso, por exemplo de $\{1,2,10,30,60\}$ na ordem dos divisores de 60. Noutros, quais quaisquer dois elementos são incomparáveis, como $\{4,5,6\}$ na ordem dos divisores de 60.

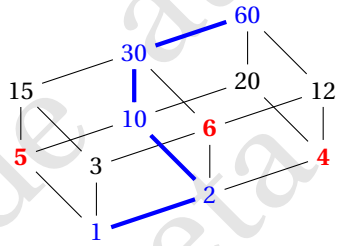


Figura 4.5: Uma cadeia em azul e uma anticadeia em vermelho.

Definição 136. Seja $(A,\preccurlyeq)$ um ordem parcial. Se $B \subseteq A$ é tal que quaisquer $x, y \in B$ vale $x \prec y$ ou $y \prec x$, dizemos que B é uma **cadeia**. Se para quaisquer $x, y \in B$ vale $x \not\prec y$ e $y \not\prec x$, dizemos que B é uma **anticadeia**.

Se a ordem parcial $(A,\preccurlyeq)$ é uma cadeia então dizemos que $(A,\preccurlyeq)$ é uma **ordem total**.

4.2.1 Boa ordem e Indução

Uma ordem parcial $(A,\preccurlyeq)$ é dita **boa ordem** se, e só se, $\preccurlyeq$ é uma ordem total e todo subconjunto não vazio de A tem mínimo com respeito a essa ordem, ou seja, existe $m \in A$ tal que $m \preccurlyeq x$ para todo $x \in A$.

O exemplo canônico de boa ordem é os naturais com a ordem usual $\leqslant$. Não é difícil provar que um subconjunto de um conjunto bem ordenado também é bem ordenado.

Exemplo 137. A seguinte relação $\preccurlyeq$ é um exemplo de boa ordem nos inteiros: $x \preccurlyeq y$ se, e somente se, uma das seguintes condições vale

1. $x = 0$
2. $0 < x$ e $y < 0$
3. $0 < x$ e $0 < y$ e $x \leqslant y$
4. $x < 0$ e $y < 0$ e $|x| \leqslant |y|$.

Nesse caso, por exemplo, $1 \prec -1$, $1 \prec -2$, $2 \prec -2$; no caso geral $0 \prec 1 \prec 2 \prec \cdots \prec -1 \prec -2 \prec \cdots$.

Exemplo 138. Outra relação para boa ordenação dos inteiros é a seguinte: $x \preccurlyeq y$ se, e somente se,

1. $|x| < |y|$ ou
2. $|x| = |y|$ e $x \leqslant y$.

Nesse caso $0 \prec -1 \prec 1 \prec -2 \prec 2 \prec \cdots$.

Uma propriedade muito interessante de uma boa ordem é que ela implica um princípio indutivo. Um princípio de indução completo para uma boa ordem é como segue.

TEOREMA 139 (PRINCÍPIO DE INDUÇÃO COMPLETO PARA BOA ORDEM) *Sejam $(A, \preccurlyeq)$ uma boa ordem e P um predicado sobre A.*

Suponha que, para todo $y \in A$, $P(y)$ é verdadeiro sempre que $P(x)$ seja verdadeiro para todo $x \prec y$. Então $P(x)$ é verdadeiro para todo $x \in A$.

De modo sintético, em símbolos, a sentença $\forall a \in A,\ P(a)$ é consequência lógica de

$$\forall y \in A\Big(\big(\forall x \in A(x \prec y \to P(x))\big) \to P(y)\Big) \tag{4.3}$$

DEMONSTRAÇÃO. A prova é por contradição. Sejam $(A, \preccurlyeq)$ uma boa ordem e P um predicado sobre A. Assumamos que (4.3) é verdadeiro, i.e., para todo $y \in A$ é verdadeiro:

$$\big(\forall x \in A(x \prec y \to P(x))\big) \to P(y) \tag{4.4}$$

e suponhamos que existe $a \in A$ tal que $P(a)$ não é verdadeiro. Assim, não é vazio o conjunto

$$S \coloneqq \{a \in A\colon \text{não } P(a)\}.$$

Façamos $y \coloneqq \min(S)$, o menor elemento de S com respeito a ordem $\preccurlyeq$, que existe pois o conjunto é bem ordenado.

De (4.4) verdadeiro e $P(y)$ falso, pois $y \in S$, segue que é verdadeira a sentença

$$\forall x \in A,\ x \prec y \to P(x)$$

portanto, por (4.4), $P(y)$ é verdadeiro, o que é uma contradição. □

Usamos esse princípio para provar que todo elemento de um conjunto bem ordenado tem uma dada propriedade. Para isso precisamos provar que (4.3) é verdadeira para tal conjunto e tal propriedade. Para isso, fixamos um y qualquer e provamos que $P(y)$ é verdadeiro sempre que $\forall x \in A,\ x \prec y \to P(x)$ é verdadeiro.

Percebamos que o caso quando y não tem predecessores por $\prec$ (o mínimo de A) e nesse caso a sentença $\forall x \in A, x \prec y \to P(x)$ é verdadeira por vacuidade, portanto, para valer (4.3) temos que verificar que $P(y)$ é verdadeiro, a propriedade vale no menor elemento da boa ordem. Usualmente, chamamos essa tarefa de *base da indução*.

Vamos a um exemplo. O conjunto $\mathbb{N} \times \mathbb{N}$ com a ordem lexicográfica $\trianglelefteq$, isto é,

$$(x, y) \trianglelefteq (a, b) \text{ se, e só se } x < a \text{ ou } (x = a \text{ e } y \leqslant b) \tag{4.5}$$

e $(x, y) = (a, b)$ se e só se $x = a$ e $y = b$. Agora, defina a função $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ por $f(0,0) = 0$ e nos outros casos

$$f(m,n) = \begin{cases} f(m-1,n)+1 & \text{se } n = 0 \text{ e } m > 0 \\ f(m,n-1)+n & \text{se } n > 0 \end{cases}$$

A relação $\trianglelefteq$ bem ordena o conjunto $\mathbb{N} \times \mathbb{N}$. Vamos provar por indução que $f(m,n) = m + n(n+1)/2$. Começamos provando

$$\big(\forall x \in \mathbb{N} \times \mathbb{N}(x \triangleleft y \to P(x))\big) \Rightarrow P(y) \tag{4.6}$$

para todo $y \in \mathbb{N} \times \mathbb{N}$ em que o predicado $P(y)$ é a igualdade "$f(m,n) = m + n(n+1)/2$" quando $y = (m,n)$.

Para $y = (0,0)$ temos $P(y)$ verdadeiro, pela definição $f(0,0) = 0$ e pela fórmula $f(0,0) = 0$, portanto (4.6) vale trivialmente. Tome $y = (a,b) \neq (0,0)$ arbitrário e assuma que para todo $x \triangleleft y$ vale $P(x)$, ou seja, assuma que $P((a-1,b))$ e $P((a,b-1))$ valem (de (4.5) temos $(a-1,b) \triangleleft (a,b)$ e $(a,b-1) \triangleleft (a,b)$), de modo que

$$\begin{aligned} &\text{se } b = 0,\ f(a,b) = f(a-1,b) + 1 = a - 1 + b(b+1)/2 + 1 = a + b(b+1)/2 \\ &\text{se } b > 0,\ f(a,b) = f(a,b-1) + b = a + b(b-1)/2 + b = a + b(b+1)/2 \end{aligned}$$

e em ambos os casos $P((a,b))$, é verdadeiro.

4.2.2 (opcional) O teorema de Dilworth

O seguinte resultado é equivalente a vários teoremas importantes em combinatória, como o teorema de Hall[1] e o teorema de Birkhoff–Von Neumann[2], também é uma generalização do teorema de Erdős–Szekeres sobre subsequências monótonas[3].

TEOREMA 140 (TEOREMA DE DILWORTH) *Numa ordem parcial finita A, o menor número m de cadeias tal que todo elemento de A pertence a alguma dessas cadeias é igual ao número máximo de elementos M em uma anticadeia de A.*

DEMONSTRAÇÃO. Vamos provar que $m \leqslant M$. A prova é por indução completa em $n = |A|$.

Se $n = 1$, então $m = M$. Seja $k \geqslant 1$ um natural arbitrário e assuma que para toda ordem parcial com $\leqslant k$ elementos o teorema é verdadeiro.

Tome $(A, \preccurlyeq)$ uma ordem parcial com $k+1$ elementos e considere C uma cadeia maximal (com respeito a inclusão) em A.

Se toda anticadeia em $A \setminus C$ tem no máximo $M-1$ elementos, então $A \setminus C$ pode ser escrito como união de no máximo $M-1$ cadeias, por hipótese da indução, que com a cadeia C formam no máximo M cadeias tal que todo elemento de A pertence a alguma dessas cadeias. Portanto $m \leqslant M$.

Agora suponha que X seja uma anticadeia em $A \setminus C$ com M elementos e defina os conjuntos

$$X^- = \{x \in A \colon x \preccurlyeq a \text{ para algum } a \in X\}$$
$$X^+ = \{x \in A \colon a \preccurlyeq x \text{ para algum } a \in X\}$$

de $|X| = M$, o tamanho máximo de uma anticadeia, $A = X^- \cup X^+$, caso contrário haveria z incomparável como os elementos de X e $X \cup \{z\}$ seria uma anticadeia.

Se $|X^+|, |X^-| < |A|$ então, pela hipótese da indução, $|X^+|$ pode ser escrito como união de $\leqslant M$ cadeias cujos mínimos estão em X e $|X^-|$ pode ser escrito como união de $\leqslant M$ cadeias cujos máximos estão em X. Portanto P é união de $\leqslant M$ cadeias.

Resta verificar que $|X^+|, |X^-| < |A|$. Isso segue do fato de $\max(C) \notin X^-$ e $\min(C) \notin X^+$. Portanto, pelo PIFc, para todo natural n, o teorema vale para uma ordem parcial com n elementos. □

Exercício 141 (**teorema de Erdős–Szekerés**). Seja $a_1, a_2, \ldots, a_{n^2+1}$ uma sequência de números reais. Uma subsequência $i_1 < i_2 < \cdots < i_k$ é dita *monótona crescente* (respec., monótona decrescente) se $a_{i_1} \leqslant a_{i_2} \leqslant \cdots \leqslant a_{i_k}$ (resp. $a_{i_1} \geqslant a_{i_2} \geqslant \cdots \geqslant a_{i_k}$). A sequência é *monótona* se for monótona crescente ou monótona decrescente.

Use o teorema de Dilworth para provar a seguinte afirmação, o teorema de Erdős–Szekerés: toda sequência $a_1, a_2, \ldots, a_{n^2+1}$ de números reais contém uma subsequência monótona de comprimento $n+1$.

Exercícios

1. Prove que numa ordem parcial um elemento mínimo é minimal e um máximo é maximal. Construa exemplos onde a recíproca não vale.
2. Determine os elementos maximais/minimais/máximo/mínimo em $(\mathbb{Z}^+, |\,)$.
3. Prove que se $(A, \preccurlyeq)$ tem máximo então ele é único.
4. Desenhe um diagrama de Hasse para o conjunto dos subconjuntos próprios de $\{1,2,3,4\}$ com a ordem da inclusão. Quais são as anticadeias dessa ordem parcial?
5. Determine os elementos maximais e minimais de $(\{2,4,5,10,12,20,25\}, |)$.
6. Determine as cadeias e as anticadeias de $(2^{\{1,2,3\}}, \subseteq)$.
7. Prove que numa ordem parcial finita e não vazia há elementos maximais e minimais.
8. Considere o conjunto $A = \{1,2,3,4\}$. Determine todas as relações de ordem total. Quantas são?
9. Seja $\mathscr{S}$ o conjunto das sequências binárias finitas. Seja $l(u) \in \mathbb{N}$ o comprimento (em quantidade de bits) da sequência $u \in \mathscr{S}$ (supomos uma sequência vazia, sem símbolos, de comprimento zero). Dadas duas sequências u, v defina uma relação R em $\mathscr{S}$ da seguinte forma:
$$(u, v) \in R \iff l(u) \leqslant l(v).$$
Trata-se de uma relação de ordem? Justifique.

[1] O teorema de Hall dá uma condição necessária e suficiente para poder selecionar elementos distintos de cada conjunto de uma família de conjuntos finitos.

[2] Toda matriz duplamente estocástica (cada linha e cada coluna somam 1) pode ser escrita como combinação convexa de matrizes de permutação (matriz quadrada 0-1 com um único 1 em cada linha e em cada coluna).

[3] Toda sequência de $mn+1$ números reais possui uma subsequência crescente de $m+1$ termos ou uma subsequência decrescente $n+1$ termos.

10. Defina a relação R sobre $\mathbb{Z}\times\mathbb{Z}$ pela regra $(a,b)\ R\ (c,d) \leftrightarrow a \leqslant c$ ou $b \leqslant d$. A relação é uma ordem parcial sobre $\mathbb{Z}\times\mathbb{Z}$?

11. Defina a relação R sobre $\mathbb{Z}\times\mathbb{Z}$ pela regra $(a,b)\ R\ (c,d) \leftrightarrow a = c$ ou $b = d$. A relação é uma ordem parcial sobre $\mathbb{Z}\times\mathbb{Z}$?

12. Dado um conjunto A considere o conjunto de partes com a relação de inclusão $(\mathscr{P}(A),\subseteq)$ e prove que trata-se de uma relação de ordem. Determine a existência, ou não, de mínimo e máximo.

13. Determine a veracidade das seguintes proposições:

    (a) Uma relação não pode ser simultâneamente de ordem e de equivalência.

    (b) Em um conjunto totalmente ordenado todo subconjunto não vazio tem mínimo.

14. Sejam $(A_1,\leq_1)$ e $(A_2,\leq_2)$ conjuntos com respectivas relações de ordem. Definimos a **ordem lexicografica** no produto $A_1\times A_2$ por $(x_1,x_2)\trianglelefteq(y_1,y_2)$ se, e somente se,

$$(x_1 \leq x_2 \text{ e } x_1 \neq x_2) \text{ ou } (x_1 = x_2 \text{ e } y_1 \leq y_2).$$

    - Prove que de fato temos uma relação de ordem.
    - No caso usual de $(\mathbb{R},\leq)$, considere a ordem lexicográfica no plano $\mathbb{R}\times\mathbb{R}$. Escolha um elemento qualquer $p=(p_1,p_2)\in\mathbb{R}\times\mathbb{R}$ e desenhe o conjunto $\{x\in\mathbb{R}\times\mathbb{R}\colon x\trianglelefteq p\}$.

15. Seja $(P,\leq)$ uma ordem parcial finita. Defina

$$K := \max\{|A|\colon A\subset P,\ \text{cadeia}\}.$$

    (a) Prove que existe uma partição de P em K conjuntos, $P=\{L_1,L_2,\ldots,L_K\}$, tais que se $x\in L_i$ e $y\in P$ é tal que $y\leq x\wedge y\neq x$ então $y\in L_1\cup\cdots\cup L_{i-1}$.

    (b) Observe que cada subconjunto L_i dos anteriores é, de fato, uma anti-cadeia.

    (c) Conclua que se $|P|=n$, então temos ou uma cadeia A de comprimento $|A|\geqslant\sqrt{n}$ ou temos uma anticadeia de cardinalidade $|L|\geqslant\sqrt{n}$.

16. Para cada $m\in\mathbb{N}$ denotamos por $[m]$ ao conjunto $\{0,1,\ldots,m-1\}$ com a ordem $\leqslant$ usual dos números inteiros. Dados $n,k\in\mathbb{N}$, considere o conjunto $P_{n,k}=[n]\times[k]$ com a **ordem produto**, ou seja, com a relação de ordem parcial em P definida do seguinte modo:

$$(x_1,x_2)\preccurlyeq(y_1,y_2) \text{ se, e só se, } x_1\leqslant y_1 \text{ e } x_2\leqslant y_2.$$

    (a) Prove que o comprimento da maior cadeia, C, de P é igual a $n+k-1$
    Dica: observe que existem máximo e mínimo (únicos).

    (b) Quantas cadeias de comprimento máximo tem-se?

17. Sejam $(A,\preccurlyeq)$ e $(B,\trianglelefteq)$ ordens totais. Uma função $f\colon A\to B$ é dita crescente[4] se, e só se, para todos $x,y\in A$, vale $x\prec y\to f(x)\triangleleft f(y)$. Dê uma prova ou um contraexemplo para a sentença: uma função crescente f de A em B é injetiva.

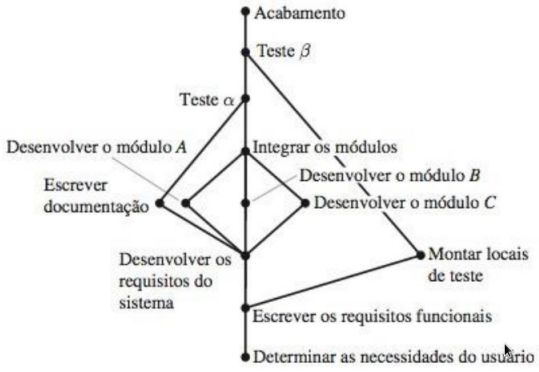
18. Uma **ordenação topológica** de uma ordem parcial $(A,\preceq)$ é uma sequência $a_1,a_2,\ldots,a_n$ com todos os elemento de A que é *compatível* com $\preceq$, isto é, se $i<j$ então $a_i\preceq a_j$, ou a_i e a_j são incomparáveis. Uma ordenação topológica de $(2^{\{1,2,3\}},\subseteq)$ é

$$\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}$$

    Escreva outras duas ordenações topológicas possíveis para $(2^{\{1,2,3\}},\subseteq)$.

19. (Ross) Seja S um conjunto de tarefas e $\preceq$ uma relação de ordem, de modo que $s\preceq t$ significa que s deve ser realizada antes de t. Uma ordenação topológica corresponde a uma sequência de realização de tarefas que é compatível com a ordem. Encontre uma ordem de tarefas para um projeto de software cuja ordem é representada pelo diagrama abaixo.

[4] É mais comum dizermos que f **preserva a ordem** ao invés de crescente. Note que usamos a ordem estrita.



20. Uma **linearização** de um conjunto parcialmente ordenado e finito $(P, \preccurlyeq)$ é uma enumeração dos elementos do conjunto, $x_1, x_2, \ldots, x_n$, de modo que $i < j$ implique $x_i \preccurlyeq x_j$ ou x_i e x_j incomparáveis.

    Seja $\mathscr{S}_3$ o conjunto das sequências binárias de 3 bits com a ordem produto, ou seja,

    $$a_0 a_1 a_2 \leq b_0 b_1 b_2 \text{ se,e somente se, } a_0 \preccurlyeq b_0 \text{ e } a_1 \preccurlyeq b_1 \text{ e } a_2 \preccurlyeq b_2.$$

    (a) Desenhe um diagrama de Hasse da ordem parcial, posicionando os elementos de $\mathscr{S}_3$ como os vértices de um cubo projetado contra o plano.

    (b) Verifique que a seguinte enumeração é de fato uma linearização: $000, 001, 010, 100, 011, 101, 110, 111$.

    (c) Prove que tem-se exatamente 6 formas de reordenar os elementos de $\mathscr{S}_3$ de modo à respeitar a ordem de $\mathscr{S}_3$ (ou seja, bijeções *monótonas*: $x \leq y \implies F(x) \leq F(y)$).
    Dica: Veja que estas devem respeitar a geometria do cubo...

    (d) Porem, o números de linearizações possíveis é bem maior. Verifique que tem-se 48 linearizações.
    Dica: $48 = 3! \cdot 3! + 3 \cdot 2 \cdot 2$.

    Obs.: ordenação topológica é outro nome para linearização, usado na computação.

21. Prove que todo subconjunto de um conjunto bem ordenado é bem ordenado.

22. Prove que são boas ordens as ordens parciais dos exemplos 137 e 138 e a ordem lexicográfica em $\mathbb{N} \times \mathbb{N}$.

23. Sejam $(A, \preccurlyeq)$ e $(B, \sqsubseteq)$ duas ordens parciais. Tome em $A \times B$ a ordem lexicográfica $\trianglelefteq$, isto é,

    $$(x, y) \trianglelefteq (a, b) \text{ se, e só se } x \prec a \text{ ou } (x = a \text{ e } y \sqsubseteq b)$$

    e $(x, y) = (a, b)$ se e só se $x = a$ e $y = b$. Prove que se $(A, \preccurlyeq)$ e $(B, \sqsubseteq)$ são boa ordem então $(A \times B, \trianglelefteq)$ é boa ordem.

24. Defina a relação $\trianglelefteq$ sobre o conjunto $\mathbb{Z}^-$ dos inteiros negativos por

    $$a \trianglelefteq b \text{ se, e somente se, } |a| \leqslant |b|.$$

    (a) Prove que $\trianglelefteq$ é uma boa ordem sobre $\mathbb{Z}^-$.

    (b) Defina $f : \mathbb{Z}^- \to \mathbb{Z}^-$ por

    $$f(-1) = -1 \; e \; f(n) = f(n+1) + n.$$

    Calcule $f(-2)$, $f(-3)$, $f(-4)$.
    Prove que f está bem definida.
    Use o princípio de Indução para conjuntos bem-ordenados para provar que

    $$f(n) = -\frac{|n|(|n|+1)}{2}.$$

25. A **relação de Stifel**, também conhecida como regra de Pascal, é a parte recursiva da definição da função $C\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ dada por

$$C(n,k) \coloneqq \begin{cases} 0 & \text{se } k > n \\ 1 & \text{se } k = n \text{ ou } k = 0 \\ C(n-1,k-1) + C(n-1,k) & \text{se } 0 < k < n. \end{cases}$$

Prove que C está bem definida.

26. Se uma função crescente f como definida no exercício 17, página 70, é uma bijeção então chamamos f de **isomorfismo** e as ordens totais $(A,\preccurlyeq)$ e $(B,\trianglelefteq)$ são ditas **isomorfas**. Prove que se duas boa ordens são isomorfas então há um único isomorfismo entre elas.

27. Seja $(A,\preccurlyeq)$ uma boa ordem e $B\subseteq A$. Prove que se $f\colon A\to B$ é um isomorfismo então $x\preccurlyeq f(x)$ para todo $x\in A$.

28. Sejam $(A,\preccurlyeq)$ uma ordem total. Um subconjunto $I\subseteq A$ é chamado de **segmento inicial** se para algum $x\in A$

$$I = \{y\in A\colon y\prec x\}$$

o qual é um **segmento inicial próprio** caso $I\neq A$. Prove que uma boa ordem não é isomorfa a um segmento inicial próprio dela.

29. Sejam $(A,\preccurlyeq)$ e $(B,\trianglelefteq)$ boas ordens. Prove que vale uma, e só uma, das seguintes afirmações.

    (a) $(A,\preccurlyeq)$ é isomorfa a um segmento inicial próprio de $(B,\trianglelefteq)$.

    (b) $(B,\trianglelefteq)$ é isomorfa a um segmento inicial próprio de $(A,\preccurlyeq)$.

    (c) $(A,\preccurlyeq)$ e $(B,\trianglelefteq)$ são isomorfas.

30. Na teoria e conjuntos ZFC, uma consequência do axioma da escolha é que todo conjunto admite uma boa ordenação. Seja $\preceq$ uma ordem parcial que bem ordena o $\mathbb{R}$. Tome $x_0 = \min\mathbb{R}$ e $x_1 = \min(\mathbb{R}\setminus\{x_0\})$. Demonstre que não há $x\in\mathbb{R}$ tal que $x_0\prec x\prec x_1$.

31. Seja S uma ordem parcial sem cadeias de comprimento maior que m. Prove que S pode ser coberto por no máximo m anticadeias. (*Dica*: indução em m. Para $m>1$, seja M o conjunto de todos os elementos maximais em S. Então $S\,M$ não tem cadeias de comprimento maior que $m-1$ e M é uma anticadeia.)

Complemento: Números naturais e ordinais

No uso comum a palavra ordinal é um adjetivo para *ordem, posição* como primeiro, segundo, terceiro e assim por diante. Em teoria dos conjuntos são *tipos de ordem*, duas boas ordens são do mesmo tipo se são isomorfas (veja os exercícios 17 ao 29).

O conjunto $\mathcal{N}$ dos **ordinais finitos de Von Neumann** são dados pela definição recursiva

1. $\varnothing\in\mathcal{N}$
2. se $x\in\mathcal{N}$ então $x\cup\{x\}\in\mathcal{N}$.

Com isso os números naturais são definidos na teoria dos conjuntos ZF

$$\begin{aligned} 0 &= \varnothing \\ 1 &= \{\varnothing\} = \{0\} \\ 2 &= \{\varnothing,\{\varnothing\}\} = \{0,1\} \\ 3 &= \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\} = \{0,1,2\} \end{aligned}$$

e assim por diante. Note que $0\in 1\in 2\in 3$. De fato $\in$ é uma relação bem fundada em $\mathcal{N}$.

Tomando a função sucessor $S(n) = n\cup\{n\}$, a estrutura $(\mathcal{N},0,S)$ em que 0 é constante dada pelo conjunto vazio, satisfaz os axiomas de Peano:

1. Todo número natural possui um único sucessor, que também é um número natural.
2. Existe um único número natural, o 0, que não é sucessor de nenhum outro.
3. Números naturais diferentes possuem sucessores diferentes.

4. Se um conjunto de números naturais contém o número 0 e, além disso, contém o sucessor de cada um dos seus elementos, então esse conjunto coincide com o conjunto dos números naturais.

Podemos ir além dos ordinais finitos. O conjunto $\omega = \bigcup_{n\in\mathcal{N}} n$ não é sucessor de outro ordinal e é o primeiro ordinal infinito (ou, não finito). A partir da podemos tomar sucessores (agora escrito como +1)

$$\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$$
$$\omega + 2 = \omega + 1 \cup \{\omega + 1\} = \{0, 1, 2, \ldots, \omega, \{\omega\}\}$$

e assim por diante, usando a definição recursiva acima e, em seguida, temos o próximo ordinal que não é sucessor de outro ordinal $\omega + \omega = \bigcup_{\alpha\in\omega+\omega} \alpha$.

Cada ordinal de von Neumann é o conjunto bem ordenado dos ordinais menores e pode-se provar que todo conjunto bem ordenado é isomorfo a um ordinal von Neumann. Eles podem ser construídos da seguinte forma:

1. 0 é o conjunto vazio ;
2. se α é ordinal então $\alpha + 1 = \alpha \cup \{\alpha\}$ é ordinal;
3. se A é um conjunto de ordinais então $\bigcup A$ é ordinal.

Os $\alpha + 1$ são **ordinais sucessores** e os $\bigcup A$ são **ordinais limites**, que não são sucessores de outro ordinal. Os ordinais de von Neumann têm a propriedade conveniente que, se $\alpha < \beta$ então $\alpha \in \beta$ e $\alpha \subsetneq \beta$.

Os números ordinais são $0, 1, 2, 3, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega, \omega + \omega + 1, \ldots$. Não há um maior ordinal, nem o conjunto de todos os ordinais.

Agora, podemos generalizar facilmente o conceito de sequência e de enumeração pois se α é um ordinal então uma **sequência transfinita** de elementos de X, denotado $(x_\beta)_{\beta\in\alpha}$ é uma função $x\colon \alpha \to X$.

Uma indução transfinita que funciona como o PIF também pode ser escrita para conjuntos bem ordenados quaisquer e, em particular, para ordinais infinitos. Ela é a seguinte generalização da indução:

> **Princípio de indução transfinita**. *Seja X um subconjunto se um conjunto A bem ordenado pela relação $<$ e denote por a_0 o elemento mínimo de A. Se (i) $a_0 \in X$ e (ii) para todo $a \in A$, se $\{t \in A\colon t < a\} \subseteq X$ implica $a \in X$, então $A = X$.*

Provas por indução transfinita em ordinais são frequentemente divididas em três casos: $P(0)$ é verdadeiro; para todo $\beta \in \alpha$ sucessor, se $P(\beta)$ então $P(\beta + 1)$ é verdadeiro; para todo β limite $P(\beta)$ é verdadeiro, então $P(\beta)$ é verdadeiro para todo $\beta \in \alpha$.

4.3 Relações bem fundadas

Definição 142. Uma relação $\prec$ sobre $A \neq \varnothing$ é dita **bem fundada** se todo subconjunto não vazio $S \subseteq A$ contém um elemento minimal com respeito $\prec$, ou seja, existe $m \in S$ tal que para qualquer $n \in S$ *não pode valer* $n \prec m$. Notemos que a relação deve ser irreflexiva, caso contrário teríamos $m \prec m$.

Equivalentemente, $\prec$ sobre $A \neq \varnothing$ é bem fundada se, e somente se, vale a **condição de cadeia descendente**: não existe uma sequência (x_n) de elementos de A tal que $x_{i+1} \prec x_i$ para todo i, ou seja, em A não há uma cadeia da forma $\cdots \prec x_2 \prec x_1 \prec x_0$.

Exercício 143. Verifique a equivalência das definições.

Toda ordem estrita de uma boa ordem é uma relação bem fundada. Isso decorre imediatamente das definições de cada um desses conceitos.

Exemplo 144. Em particular o $<$ sobre $\mathbb{N}$ é uma relação bem fundada, porém, o $\leqslant$ sobre $\mathbb{N}$ não é uma relação bem fundada.

Exemplo 145. A relação S sobre $\mathbb{N}$ dada por $n\ S\ m$ se e só se $m = n + 1$ é bem fundada pois qualquer $A \subseteq \mathbb{N}$ não vazio tem mínimo m pro qual não existe $n \in A$ tal que $n\ S\ m$.

Exemplo 146. Vamos tomar $X_0 \in 2^{\mathbb{N}}$ como o conjunto dos naturais múltiplos de seis. Definimos uma cadeia descendente com respeito a inclusão pondo $X_i = X_{i-1} \setminus \{2i\}$ para todo inteiro $i \geqslant 1$. Se $Y \in 2^{\mathbb{N}}$ é o conjunto dos naturais múltiplos de três ímpares então $Y \subset X_i$ para todo i, porém não é um mínimo da cadeia pois não pertence a ela.

Os inteiros positivos com a relação definida por $x \,\big|\, y$ e $x \neq y$ é relação bem fundada.

A relação de pertinência $\in_X := \{(a, b) \in X \times X\colon a \in b\}$ definida em um conjunto X é bem fundada. Isso decorre do axioma da fundação (ou regularidade, página 23). O axioma da fundação garante que não há uma sequência (x_n) de elementos tal que ocorra $\cdots \ni x_2 \ni x_1 \ni x_0$.

Também é uma relação bem fundada sobre o conjunto de todas as palavras[5] sobre um alfabeto fixo e totalmente ordenado com a ordem definida por: $w \prec w'$, para palavras w e w', se w é mais curta (tem menos letras) que w' e no caso de empate w é lexicograficamente menor que w'.

A relação $\prec$ sobre $\mathbb{N}\times\mathbb{N}$ dada por $(a,b) \prec (x,y)$ se, e só se, $a < x$ e $b < y$ é uma relação bem fundada. Tome X_1 o conjunto das primeiras coordenadas dos elementos de X, que pelo PBO admite um mínimo m_1. Tome X_2 o conjunto das segundas coordenadas dos elementos de X_1, que pelo PBO admite um mínimo m_2. O par (m_1, m_2) é um elemento minimal de X. De fato, $(m_1, m_2) \in X$ e se $(x,y) \in X$ então $m_1 \leqslant x$ e $m_2 \leqslant y$, por definição de m_1 e m_2.

Uma razão importante pela qual as relações bem fundadas são interessantes é porque vale um princípio de indução nelas. Os princípios indutivos e definições recursivas que vimos são casos especiais de um princípio geral denominado indução bem fundada. Em essência, a indução estrutural, que ainda veremos, funciona porque decompor uma estrutura (e.g. conjunto, função, relação, estrutura de dados, linguagem) em subestruturas não pode continuar para sempre, eventualmente, chegamos em estruturas atômicas que não podem ser mais decompostas. Se uma propriedade falha em ser herdada por subestruturas então ela deve falhar em alguma estrutura mínimal que, quando quebrada, produz subestruturas que satisfazem a propriedade. A característica essencial compartilhada tanto pela relação de subestrutura quanto pela relação de predecessor nos números naturais é que eles não dão origem a cadeias descendentes infinitas.

4.3.1 Indução bem fundada

O seguinte resultado é conhecido como **indução noetheriana**.

Teorema 147 (Princípio de indução completo para relação bem fundada) *Sejam A um conjunto, $\prec$ uma relação bem fundada sobre A e P uma propriedade de elementos de A. Todos os elementos de A têm a propriedade P sempre que*

para todo $y \in A$, se $P(x)$ é verdadeiro para todo $x \prec y$, então $P(y)$ é verdadeiro.

Dizendo de outro modo, em símbolos, $P(a)$ é verdadeira para todo $a \in A$ se é verdadeira a sentença

$$\forall y \in A\big(\forall x \in A(x \prec y \to P(x)) \to P(y)\big) \tag{4.7}$$

Na utilização desse resultado, a base da indução é o caso quando y não tem predecessores por $\prec$ e nesse caso a sentença $\forall x \in A(x \prec y \to P(x))$ é verdadeira por vacuidade, portanto, temos que verificar que $P(y)$ vale nos elementos minimais de A com respeito a ordem. No caso da relação $<$ em $\mathbb{N}$ (exemplo 144) temos de (4.7) o PIFc e no caso da relação de sucessor em $\mathbb{N}$, exemplo 145, em (4.7) temos o PIF.

Demonstração do teorema 147. Sejam A um conjunto, $\prec$ uma relação bem fundada sobre A e P uma propriedade de elementos de A. A demonstração é por contradição. Suponhamos que exista $a \in A$ para o qual não vale $P(a)$. Seja $X := \{x \in A\colon \text{não-}P(x)\}$ o conjunto não vazio dos contraexemplos de P.

De $\prec$ bem fundada temos que X tem um elemento mimimal m e, por definição, para todo $x \in A$ tal que $x \prec m$ a propriedade P vale, isto é, $P(x)$ é verdadeiro. Portanto, de (4.7) (para $y = m$) temos que $P(m)$ é verdadeiro, uma contradição. □

Um exemplo de demonstração na ordem estrita e bem fundada $(\mathbb{N}\setminus\{0,1\}, <)$ foi dada na página 52 quando provamos o teorema fundamental da aritmética. Reveja: Seja $P(n)$ a sentença *n é primo ou pode ser escrito como produto de primos.* 2 é primo, portanto $P(2)$ é verdadeiro. Seja $y > 2$ um natural arbitrário. Se y é primo então o $P(y)$ é verdadeiro, senão y é composto. Se para qualquer $x < y$ no domínio vale $P(x)$, então, como $y = a \cdot b$, para $a < y$ e $b < y$, temos que y é produto de primos pois $P(a)$ e $P(b)$ são verdadeiros. Por indução $P(n)$ é verdadeiro para todo n.

Exemplo 148 (**função de Ackermann**). A função de Ackermann $A\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ definida recursivamente por

$$A(x,y) = \begin{cases} y+1 & \text{se } x = 0 \\ A(x-1,1) & \text{se } x > 0 \text{ e } y = 0 \\ A(x-1, A(x,y-1)) & \text{c.c.} \end{cases}$$

é conhecida pela extraordinária velocidade com que cresce, $A(0,y) = y+1$, $A(1,y) = y+2$, $A(2,y) = 2y+3$, $A(3,y) = 2^{y+3} - 3$, $A(4,1) = A(5,0) = 65533$, $A(4,2) = 2^{65536} - 3$ e

$$A(4,y) = 2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}} - 3$$

onde as potências formam uma torre com $y+3$ ocorrências de 2's. Mais que isso, essa função é um contraexemplo importante para a conjectura de que toda função computável é primitiva recursiva.

[5] Dado um alfabeto Σ, uma palavra é uma cadeia finita $\ell_1\ell_2\ldots\ell_t$ de elementos (as letras) do alfabeto, $\ell_i \in \Sigma$.

Nesse caso devemos ter uma relação sobre os pares (x, y) com condição de cadeia descendente para garantir a condição de parada da recorrência da definição de A.

A função de Ackermann está bem definida, ou seja, existe e é única a imagem de cada par de naturais (x, y) pela função A que satisfaz 148. Considere a ordem lexicográfica estrita $\lhd$ sobre $\mathbb{N} \times \mathbb{N}$ que é bem fundada. O valor $A(0,0)$ está definido e é 1. Seja $(x, y) \neq (0,0)$ arbitrário e assuma que $A(x_0, y_0)$ está definido para todo $(x_0, y_0) \lhd (x, y)$. Vamos mostrar que $A(x, y)$ está definido em três casos: (1) $x = 0$; (2) $x \neq 0$ e $y = 0$; (3) $x, y \neq 0$.

No caso (1), se $x = 0$, então $A(0, y)$ está definido e vale $y + 1$. No caso (2), se $x \neq 0$ e $y = 0$, então em $(x-1, 1) \lhd (x, 0)$ a função está definida por indução, assim fica definido o valor $A(x, 0) = A(x-1, 1)$. No caso (3), se $x, y \neq 0$, então $(x, y-1) \lhd (x, y)$ de modo que $A(x, y-1)$ está definido por indução. Além disso, $(x-1, A(x, y-1)) \lhd (x, y)$, logo por indução $A(x-1, A(x, y-1)) = A(x, y)$ está definida. Portanto, a função está definida em todo par ordenado de números naturais.

Exemplo 149 (**teorema de Bachet–Bézout**). Vamos demostrar um teorema devido a Euclides (veja o exercício 79, página 42) usando indução bem fundada. O teorema enuncia que para todos os inteiros positivos m e n, existem inteiros x e y tais que $xm + yn = \text{mdc}(m, n)$. A prova é por indução em (m, n) usando a ordem lexicográfica estrita $\lhd$. Para o par $(1, 1)$, mais geralmente (m, n) para $m = n$, temos $x = 1$ e $y = 0$. Seja (m, n) um par de inteiros positivos, podemos assumir que $m \neq n$. Assumamos que o enunciado é verdadeiro para todos os pares de inteiros positivos lexicograficamente menores que (m, n) e que $m > n$.

Como $(m - n, n) \lhd (m, n)$ existem inteiros x_0 e y_0 tais que $x_0(m - n) + y_0 n = \text{mdc}(m - n, n)$. Notemos que um divisor de m e de n também divide $m - n$, assim $x_0(m - n) + y_0 n = \text{mdc}(m, n)$. Ademais $x_0(m - n) + y_0 n = x_0 m + (y_0 - x_0)n$ de modo que para $x = x_0$ e $y = y_0 - x_0$ temos $xm + yn = \text{mdc}(m, n)$.

Exercício 150. Seja $I \subset \mathbb{N}$ o conjunto definido recursivamente no exemplo 114. Defina em $\mathbb{N}$ a relação bem fundada $\prec$ por $a \prec b$ se, e só se, b pode ser obtido a partir de a por somas sucessivas de 2. Por exemplo, $1 \prec 3$ e $3 \prec 131$, mas $1 \not\prec 2$, $1 \not\prec 20$ e $3 \not\prec 8$.

1. Verifique que a relação é bem fundada.
2. Prove usando a indução noetheriana que I é o conjuntos dos naturais ímpares.

Estruturas definidas recursivamente e indução estrutural

A indução estrutural é uma generalização do PIFc e um caso da indução noetheriana para uma estrutura definida recursivamente, é usada para provar que alguma propriedade vale para todo elemento dessa estrutura que tem uma ordem bem fundada subjacente. Tais estruturas como, por exemplo, fórmulas, listas ou árvores são comuns em disciplinas da matemática discreta como a lógica, linguagens formais, teoria da computação e a teoria de grafos.

Exemplo 151. As fórmulas boolenanas formam um conjunto $\mathscr{F}$ das cadeias finitas de símbolos tomados do conjunto

$$\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow, (,), p_0, p_1, p_2, p_3, \ldots\}$$

chamado de alfabeto. O conjunto $\mathscr{F}$ é definido recursivamente por

1. para todo $i \in \mathbb{N}$, $p_i \in \mathscr{F}$;
2. se $\alpha, \beta \in \mathscr{F}$ então $(\neg\alpha) \in \mathscr{F}$ e $(\alpha \vee \beta) \in \mathscr{F}$ e $(\alpha \wedge \beta) \in \mathscr{F}$ e $(\alpha \rightarrow \beta) \in \mathscr{F}$ e $(\alpha \leftrightarrow \beta) \in \mathscr{F}$;
3. não há outros elementos em $\mathscr{F}$ além dos obtido pelo uso das regras 1 e 2 um número finito de vezes.

São exemplos de fórmulas p_1, $(\neg p_2)$ e $(p_3 \rightarrow (p_1 \wedge (\neg p_1)))$.

Nesse caso, consideramos a relação $\prec$ sobre $\mathscr{F}$ dada por $\alpha \prec \beta$ se, e só se, β pode ser obtida de α por uma aplicação da regra 2 acima. Por exemplo, $p_3 \prec (p_3 \rightarrow (p_1 \wedge (\neg p_1)))$, $(\neg p_1) \not\prec (p_3 \rightarrow (p_1 \wedge (\neg p_1)))$ e $(p_1 \wedge (\neg p_1)) \prec (p_3 \rightarrow (p_1 \wedge (\neg p_1)))$. Claramente vale a condição da cadeia descendente.

A indução noetheriana pode ser reescrita para fórmulas e obtemos o seguinte princípio de indução para fórmulas booleanas.

Teorema 152 *Seja P uma propriedade de fórmulas*

(1) se P é verdadeira para toda fórmula atômica e

(2) se P é verdadeira para α e β então também é verdadeira para $(\neg\alpha)$, para $(\alpha \wedge \beta)$, para $(\alpha \vee \beta)$, para $(\alpha \rightarrow \beta)$ e para $(\alpha \leftrightarrow \beta)$.

Então então P é verdadeira para toda $\alpha \in \mathscr{F}$.

O seguinte exemplo ilustra uma prova por indução.

Exemplo 153. Vamos provar usando a indução que *toda fórmula bem formada tem um quantidade par de parênteses.* Cada fórmula atômica tem 0 parênteses. Para todo α que tem um número par, digamos $2n$, de parênteses, $(\neg\alpha)$ tem $2n+2 = 2(n+1)$ parênteses, portanto par. Suponha que α e β tenham, respectivamente, $2n$ e $2m$ parênteses, então $(\alpha \wedge \beta)$ tem $2n+2m+2 = 2(n+m+1)$ parênteses (os casos $(\alpha \vee \beta)$, $(\alpha \to \beta)$ e $(\alpha \leftrightarrow \beta)$ são idênticos). Pelo Princípio de indução para fórmulas toda fórmula bem formada tem um quantidade par de parênteses.

O exemplo a seguir ilustra uma **definição recursiva** de uma função definida em $\mathscr{F}$. Pelo princípio de indução em fórmulas, precisamos defini-la para as fórmulas atômicas e, assumindo definida para α e β, escrever a definição para as fórmulas obtidas de α e β usando os conectivos.

Exemplo 154. As vezes é conveniente medir a complexidade de uma FBF pelo seu *grau* dado por:

1. $\text{grau}(\alpha) = 0$ se $\alpha = p_i$ para algum i;
2. $\text{grau}(\neg\alpha) = \text{grau}(\alpha) + 1$ e $\text{grau}(\alpha \square \beta) = \max\{\text{grau}(\alpha), \text{grau}(\beta)\} + 1$, onde $\square \in \{\wedge, \vee, \to, \leftrightarrow\}$.

Pelo princípio de indução a função grau está definida para toda fórmula de $\mathscr{F}$.

Exercício 155. Demonstre que para toda fórmula α vale que $\text{grau}(\alpha)$ é no máximo o número de conectivos lógicos que aparecem em α. Demonstre também que $\text{grau}(\beta) < \text{grau}(\alpha)$ para toda subfórmula própria β da fórmula α.

Exemplo 156 (**Árvore binária com raiz**). Uma árvore binária sobre $\mathbb{N}$ com raiz é uma tripla definida recursivamente por

1. se $r \in \mathbb{N}$ então $(, r,)$ é uma árvore binária com raiz r;
2. se E e D são árvores binárias com raiz, então (E, r, D) é uma árvore binária com raiz r. Nesse caso chamamos E de *subárvore esquerda* e D de *subárvore direita.*

Só consideraremos árvores obtidas por uma aplicação dessas regras um número finito de vezes.

Se T é uma árvore binária, as subárvores (binárias) da forma $(, r,)$ que ocorrem em T são chamadas de *folhas* de T. Os outros nós são ditos *internos.*

Um exemplo de árvore binária com raiz é $\big(\big((, 1,), 3, (, 2,)\big), 5, (, 4,)\big)$ que pode ser mais facilmente entendida pelo diagrama da figura 4.6 a seguir. As folhas são $(, 1,)$, $(, 2,)$ e $(, 4,)$, as quais denotamos simplesmente por 1, 2 e 4.

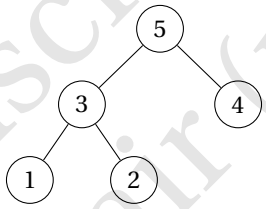


Figura 4.6: árvore binária

Outro exemplo de árvore binária com raiz é dado por $\big(\big((, 1,), 5, (, 2,)\big), 7, \big(, 3,), 6, (, 4,)\big)\big)$ representada na figura 4.7 As folhas são

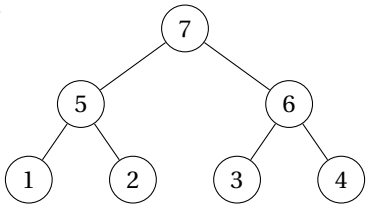


Figura 4.7: árvore binária

1, 2, 3 e 4.

A *quantidade de nós* de uma árvore binária T é definida recursivamente por

$$n(T) = \begin{cases} 1 & \text{se } T = (,r,) \\ 1 + n(E) + n(D) & \text{se } T = (E,r,D), \end{cases}$$

e a *altura* de uma árvore binária T é definida recursivamente por

$$h(T) = \begin{cases} 0 & \text{se } T = (,r,) \\ 1 + \max\{h(E), h(D)\} & \text{se } T = (E,r,D). \end{cases} \tag{4.8}$$

As duas árvores dos exemplos anteriores, figuras 4.6 e 4.7, têm altura 2. Na figura 4.8 representamos uma árvore de altura 3. As folhas são $1,2,3,5,6$.

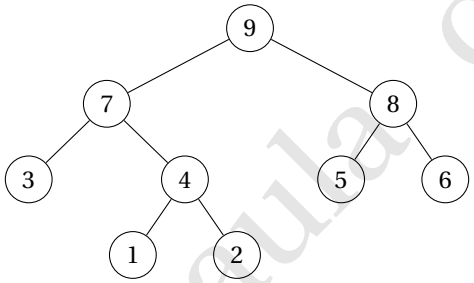


Figura 4.8: outra árvore binária

A relação $S \prec T$ definida por "S é a subárvore binária a esquerda ou a direita de T" é bem fundada, pela condição de cadeia descendente. Por exemplo,

$$\big(,1,\big),5,\big(,2,\big)\big) \prec \Big(\big(\big(,1,\big),5,\big(,2,\big)\big),7,\big(,3,\big),6,\big(,4,\big)\big)\Big).$$

Agora, vamos provar usando indução que o número de nós numa árvore binária T de altura $h(T)$ é

$$n(T) \leqslant 2^{h(T)+1} - 1 \tag{4.9}$$

Se $T = (,r,)$ então $h(T) = 0$ e $n(T) = 1$, o que satisfaz (4.9). Seja $T = (E,r,D)$ uma árvore binária arbitrária e assuma que (4.9) é verdadeira para E para D. Por hipótese $n(E) \leqslant 2^{h(E)+1} - 1$ e $n(D) \leqslant 2^{h(D)+1} - 1$, logo

$$n(T) = 1 + n(E) + n(D) \leqslant 1 + 2^{h(E)+1} - 1 + 2^{h(D)+1} - 1 \leqslant 2 \cdot \max\{2^{h(E)+1}, 2^{h(D)+1}\} - 1$$

mas $\max\{2^{h(E)+1}, 2^{h(D)+1}\} = 2^{\max\{h(E),h(D)\}+1}$ que, por (4.8), é $2^{h(T)}$, portanto, $n(T) \leqslant 2 \cdot 2^{h(T)} - 1 = 2^{h(T)+1} - 1$. Pela indução noetheriana (4.9) vale para toda árvore binária.

Como no caso do PIF e PBO temos uma estratégia de prova por contradição: assumindo que no conjunto de todas as estruturas de um certo tipo há aquelas que não têm uma determinada propriedade, então o subconjunto de contraexemplos não é vazio, portanto, deve ter um elemento *minimal*. A partir desse contraexemplo mínimo derivamos uma contradição. Vejamos um exemplo.

Definimos árvore binária *plena* como árvore binária em que os nós internos têm, obrigatoriamente, dois descendentes, ou seja, na formação da árvore (E,r,D) não podemos ter E vazia nem D vazia, exceto nos casos base onde ambas são vazias.

PROPOSIÇÃO 157 *Em qualquer árvore binária plena o número de folhas é um a mais que o número de nós internos.*

DEMONSTRAÇÃO. Suponha que haja um contraexemplo para tal afirmação. Então deve existir um contraexemplo T com $i(T)$ nós internos e $f(T) \geqslant 1$ folhas onde $i(T) + 1 \neq f(T)$ e $\prec$-minimal.

O contraexemplo T não é da forma $(,r,)$ porque tal árvore tem 0 nós internos e 1 folha, portanto, $T = (E,r,D)$ com $E, D \neq \varnothing$. Pela minimalidade de T temos $i(E) + 1 = f(E)$ e $i(D) + 1 = f(D)$. Assim

$$f(T) = f(E) + f(D) = i(E) + i(D) + 2 = i(T) + 1$$

pois $i(E) + i(D) + 1 = i(T)$, contrariando o fato de T ser um contraexemplo. □

Uma demonstração alternativa da proposição acima usando o PBO é como segue. Suponha que haja um contraexemplo para tal afirmação. O contraexemplo T não é da forma $(,r,)$, logo tem pelo menos uma folha f cujo nó pai p é um nó interno. Exclua essa folha f e seu pai p da árvore, promovendo o nó irmão da folha f para a posição ocupada por seu pai (nó imediatamente acima no diagrama). Por exemplo, essa operação no nó 5 da árvore da figura 4.8 resulta na árvore da figura 4.9). O resultado dessa operação é uma árvore binária plena T' com uma folha e um nó interno a menos, portanto, $i(T')+1 \neq f(T')$ e, portanto, é um contraexemplo menor, uma contradição.

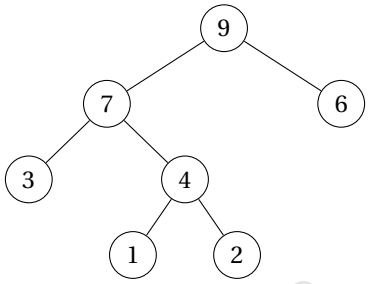


Figura 4.9: árvore binária plena obtida da árvore binária plena da figura 4.8 por remoção de uma folha (5) e seu pai (8).

Exercícios

1. Prove usando a condição de cadeia descendente que $\sqrt{4n-1}$ não é racional para todo $n \geqslant 1$ inteiro.

2. Sejam $(A, \prec)$ e $(B, \sqsubset)$ duas ordens estritas. Tome em $A \times B$ a ordem lexicográfica estrita $\lhd$, isto é,

$$(x,y) \lhd (a,b) \text{ se, e só se } x \prec a \text{ ou } (x = a \text{ e } y \sqsubset b).$$

   Prove que se $(A, \prec)$ e $(B, \sqsubset)$ são bem fundadas então $(A \times B, \lhd)$ é bem fundada.

3. Prove que a relação binária $\{(m, m+1) : m \in \mathbb{N}\}$ é uma ralação de ordem bem fundada sobre $\mathbb{N}$. Reescreva o princípio de indução para ordens bem fundadas para esse caso específico. É um resultado conhecido?

4. Prove que a relação de ordem estrita usual sobre $\mathbb{N}$ é bem fundada. Reescreva o princípio de indução para ordens bem fundadas para esse caso específico. É um resultado conhecido?

5. Prove que a relação de inclusão estrita de conjuntos é bem fundada se, e só se, o universo donde são tomados os subconjuntos é finito.

6. Prove que as três relações da seção 4.3.1, a saber $\alpha \prec \beta$ em fórmulas e "é uma subárvore binária própria de" e "tem menos nós" sobre árvores binárias, são relações bem fundadas.

7. **(Fechos de uma relação)** Seja $R \subseteq A \times A$ uma relação qualquer. Se S e T são duas relações reflexivas sobre A então $S \cap T$ também é uma relação reflexiva sobre A.

   (7.1) Demonstre que a interseção de duas relações reflexivas sore o mesmo conjunto é uma relação reflexiva.

   Ademais, se $R \subseteq S$ e $R \subseteq T$ então $R \subseteq S \cap T$. Podemos formar o conjunto $\mathscr{R}$ de todas as relações reflexivas que contêm R de modo que

$$\bigcap \mathscr{R}$$

   é uma relação reflexiva que contém R, é a "menor" ($\subset$-minimal) relação com essa propriedade, chamada de **fecho reflexivo** de R. Por exemplo, o fecho reflexivo de $<$ sobre $\mathbb{N}$ é $\leqslant$.

   (7.2) Demonstre que não existe relação reflexiva S que contém R tal que $S \subsetneq \bigcap \mathscr{R}$.

   Analogamente, a interseção de relações transitivas sobre um conjunto A resulta numa relação transitiva, assim podemos formar o conjunto $\mathscr{T}$ de todas as relações transitivas que contêm R de modo que

$$\bigcap \mathscr{T}$$

é a "menor" ($\subset$-minimal) relação transitiva que contém R, chamada de **fecho transitivo** de R.

(7.3) Demonstre os análogos de (7.1) e (7.2) para o fecho transitivo.

Ainda, podemos formar o conjunto de todas as relações reflexivas e transitivas que contém R, tomar a interseção que resultada no fecho reflexivo e transitivo da relação R.

(7.4) Demonstre os análogos de (7.1) e (7.2) para o fecho reflexivo e transitivo.

(7.5) Seja $\prec$ uma relação bem fundada sobre um conjunto A. Demonstre que

(a) o fecho transitivo de $\prec$ é uma relação bem fundada;

(b) o fecho reflexivo e transitivo de $\prec$ é uma ordem parcial.

8. Prove usando indução que na linguagem livre de contexto S $\rightarrow$ ab | aSb | SS todas as palavras têm a mesma quantidade de símbolos a e b.

9. Prove usando indução as seguintes propriedades da função de Ackermann A

(a) para todo $n \geqslant 0$, $A(1,n) = n+2$;

(b) para todo $n \geqslant 0$, $A(2,n) = 2n+3$;

(c) para todo $n \geqslant 0$, $A(3,n) = 2^{n+3} - 3$;

(d) para todos $m, n \geqslant 0$, $A(m,n) > n$.

Complemento: Lema de Zorn e teorema da boa ordem

"The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?" — Jerry Bona

Para encerrar essa seção enunciaremos dois resultados bem conhecidos e importantes para, por exemplo, provar que todo espaço vetorial tem base, o teorema de Hahn–Banach da análise funcional e o teorema de Tychonoff da topologia. O lema de Zorn é útil quando precisamos iterar algum tipo de operação "infinitamente muitas vezes" de maneira rigorosa.

TEOREMA 158 (LEMA DE ZORN) *Seja $A \neq \varnothing$ um conjunto parcialmente ordenado tal que toda cadeia em A tem um limitante superior. Então A tem um elemento maximal.* □

TEOREMA 159 (TEOREMA DA BOA ORDEM) *Para todo conjunto A não vazio, existe uma ordem $\preccurlyeq$ tal que $(A, \preccurlyeq)$ é bem-ordenado.* □

O lema de Zorn e o Teorema da boa-ordem podem ser demonstrados na teoria ZFC de conjuntos usando o axioma da escolha. De fato, as três sentenças, Axioma da Escolha, Lema de Zorn e Teorema da Boa Ordem, são equivalentes no sentido que na teoria dos conjuntos assumindo os axiomas de ZF, se acrescentamos a boa-ordem aos axiomas, então provamos escolha e Zorn e se acrescentamos Zorn então provamos escolha e boa ordem . Por, exemplo, da boa ordem é fácil provar o "axioma" da escolha, a função escolha é $f(y) = \min(y)$.

Exercício 160. Deduza do lema de Zorn o **lema de Tukey**[6]: Seja $\mathscr{F}$ uma família de subconjuntos do conjunto não vazio X com a propriedade de que se

$$F \in \mathscr{F} \text{ se e somente se cada subconjunto finito de } F \text{ está em } \mathscr{F}.$$

Então $\mathscr{F}$ tem um elemento máximal.

[6] John Wilder Tukey é matemático e cunhou o termo *bit* para dígito binário.

Capítulo 5

Contagem

5.1 Princípios de contagem: bijeção e cardinalidade

Uma característica importante dos números naturais é que eles constituem o modelo matemático que torna possível o processo de contagem e respondem a pergunta *quantos elementos tem esse conjunto*? Contagem é, em última instância, o processo de criar uma bijeção entre um conjunto que queremos contar e algum conjunto cujo "tamanho" já sabemos. Esse "tamanho" de um conjunto é chamado de cardinalidade, e é intuitivamente clara no caso de conjuntos finitos: a cardinalidade de um conjunto finito é a quantidade de elementos no conjunto expressa por um número natural. Cardinalidade é um conceito que a teoria dos conjuntos estende para qualquer conjunto. Os números cardinais transfinitos descrevem os tamanhos de conjuntos infinitos e há uma sequência transfinita de números cardinais

$$0,1,2,3,\ldots,n,\ldots,\aleph_0,\aleph_1,\aleph_2,\ldots,\aleph_\omega,\aleph_{\omega+1},\ldots,\aleph_{\omega+\omega},\ldots,\aleph_{\omega^2},\ldots,\aleph_{\omega^\omega},\ldots,\aleph_\alpha,\ldots.$$

Na verdade, a ideia de cardinalidade torna-se bastante sutil quando os conjuntos são infinitos.

Numa contagem, geralmente, não fornecemos uma bijeção explícita para calcular o tamanho de um conjunto, mas nos baseamos em princípios de contagem derivados dos processos de construção de conjuntos. O ramo da matemática que estuda,dentre outro temas, conjuntos construídos pela combinação de outros conjuntos é chamado de combinatória e a subárea que estuda os métodos de contagem é chamada de combinatória enumerativa. Também na teoria dos conjuntos estuda-se extensões das ideias e técnicas da combinatória para conjuntos infinitos, esse ramo da matemática é chamado de combinatória infinitária.

5.1.1 Bijeções

Para contar os elementos de um conjunto usamos a noção de correspondência biunívoca, ou bijeção, ou função bijetiva. Dois conjuntos têm a mesma cardinalidade se, e somente se, há uma correspondência um-para-um (bijeção) entre os elementos dos dois conjuntos. Lembremos que uma função $f : X \to Y$ é bijetiva se, e só se, para todo $y \in Y$, existe um único $x \in X$ tal que $f(x) = y$.

Dois conjuntos A e B têm a **mesma cardinalidade** e, por abuso de notação[1], denotamos isso por

$$|A| = |B|$$

se, e somente se, existe uma bijeção $f : A \to B$. Lê-se $|A|$ como **cardinalidade** de A.

Como de uma função bijetiva $f : A \to B$ temos que a sua inversa $f^{-1} : B \to A$ também é bijetiva então dizer que dois conjuntos têm a "mesma cardinalidade" está bem definido. Ademais, $|A| = |A|$ pois a função identidade $\mathrm{id} : A \to A$, dada por $\mathrm{id}(x) = x$ para todo x, é bijetiva

Exercício 161. Prove que se $|A| = |B|$ e $|B| = |C|$ então $|A| = |C|$.

Exemplo 162. A função $f : (0,+\infty) \to (0,1)$ nos reais, dada por $f(x) = \frac{x}{x+1}$ é bijetiva. A função é injetiva pois

$$\frac{x}{x+1} = \frac{y}{y+1} \Rightarrow yx + y = yx + x \Rightarrow x = y$$

e é sobrejetiva pois para todo $y \in (0,1)$

$$f(\frac{y}{1-y}) = y.$$

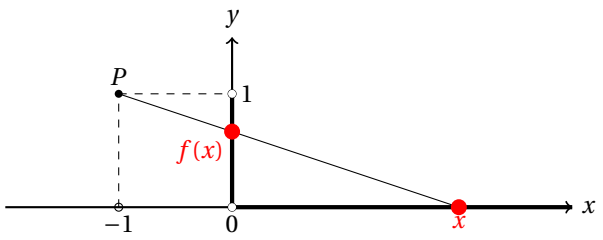


Figura 5.1: interpretação geométrica de $f(x) = x(x+1)^{-1}$

Essa função f tem a seguinte interpretação gráfica (veja a figura 5.1) no plano cartesiano. Para cada $x \in (0,+\infty)$ o valor $f(x)$ é dado pela intersecção com o eixo y da reta que passa por $(x,0)$ e por $P = (-1,1)$. Usando semelhança de triângulos temos

$$\frac{1}{x+1} = \frac{f(x)}{x}$$

donde tiramos a expressão para $f(x)$. Segue desse exercício que

$$|(0,+\infty)| = |(0,1)|.$$

Notemos que os conjuntos acima têm a mesma cardinalidade e a diferença $(0,+\infty) \setminus (0,1)$ não é vazia, muito pelo contrário é $[1,+\infty)$ e tem a mesma cardinalidade dos outros dois (verifique).

A função

$$\begin{aligned} g : \mathbb{R} &\to (0,+\infty) \\ x &\mapsto 2^x \end{aligned} \tag{5.1}$$

é bijetiva, logo pelo exercício 161 $|(0,+\infty)| = |\mathbb{R}|$ e $f \circ g : \mathbb{R} \to (0,1)$ é uma bijeção que certifica tal fato, dada por

$$f \circ g(x) = \frac{2^x}{2^x+1}.$$

Definição 163. Abusando da notação, escrevemos

$$|A| \leq |B|$$

para abreviar que existe $f : A \to B$ injetiva e escrevemos

$$|A| < |B|$$

para abreviar que existe $f : A \to B$ injetiva e não existe uma tal função bijetiva.

Nos casos em que $A \subseteq B$ temos uma função injetiva trivial de A para B, a função identidade, portanto vale o seguinte resultado.

Proposição 164 *Para todo $\varnothing \neq A \subseteq B$ vale $|A| \leqslant |B|$.*

Notemos que quando se trata de cardinalidade $\leq$ *não deve ser confundido com a relação de ordem* $\leqslant$ que usamos nos conjuntos numéricos, por exemplo. Veremos mais pra frente (na página 85) que essa definição estende, num certo sentido, a relação de ordem porém, ressaltamos que $\leq$ como definido aqui não é uma relação. Entretanto, temos que para quaisquer conjuntos não vazios A, B e C valem: (1) $|A| \leq |A|$ pois a função identidade $\mathrm{id} : A \to A$ é injetiva; (2) se $f : A \to B$ é injetiva e $g : B \to C$ é injetiva, então $g \circ f : A \to C$ é injetiva (exercício 11, página 26), portanto, se $|A| \leq |B|$ e $|B| \leq |C|$ então $|A| \leq |C|$.

Surpreendentemente, vale também a antissimetria, mas a prova não é tão simples. O seguinte resultado é bastante famoso na teoria dos conjuntos e não trivial no caso de conjuntos infinitos. A utilidade deste resultado vem do fato que, em geral, estabelecer uma bijeção que comprove $|A| = |B|$ pode ser muito difícil enquanto que estabelecer funções injetivas que comprovem $|A| \leq |B|$ e $|B| \leq |A|$ é mais fácil. Por exemplo, para provar que a cardinalidade do intervalo $[0,1)$ é a mesma do intervalo $(0,1)$ basta exibirmos uma $f : [0,1) \to (0,1)$ injetiva, pois pelo outro lado temos $\mathrm{id} : (0,1) \to [0,1)$, conforme proposição 164 acima. O leitor pode verificar que $f(x) = 1/4 + x/2$ é uma função que faz esse papel, portanto, $|[0,1)| \leqslant |(0,1)|$ e como $|(0,1)| \leqslant |[0,1)|$ o teorema 165 abaixo nos dá a equipotência.

Uma demonstração do seguinte teorema será dada adiante, no final desse capítulo.

Teorema 165 (Teorema de Cantor–Schröder–Bernstein) *Se $|A| \leq |B|$ e $|B| \leq |A|$ então $|A| = |B|$.*

[1] $|A|$ não está definido, e $|A| = |B|$ não é uma igualdade, é uma abreviação para o significado que lhe foi dado.

Alguns exemplos importantes

Vejamos algumas comparações entre a cardinalidade de alguns conjuntos conhecidos.

1. $|\mathbb{N}| = |\mathbb{Z}|$: uma ideia para estabelecermos uma bijeção entre esses conjuntos é olharmos para uma boa ordem de $\mathbb{Z}$ e tentar escrever $\mathbb{Z}$ como uma sequência dada pela ordenação. Na boa ordenação dos inteiros dada no exemplo 138, $0 \prec -1 \prec 1 \prec -2 \prec 2 \prec \cdots$

$$\begin{array}{lccccccc} (\mathbb{Z},\prec): & 0 & -1 & 1 & -2 & 2 & -3 & \cdots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\ (\mathbb{N},<): & 0 & 1 & 2 & 3 & 4 & 5 & \cdots \end{array}$$

   para mostrar que $|\mathbb{N}| = |\mathbb{Z}|$ definimos a função $f : \mathbb{Z} \to \mathbb{N}$ dada por

$$f(z) = \begin{cases} 2z, & \text{se } z \geqslant 0 \\ 2(-z)-1, & \text{se } z < 0 \end{cases}$$

   que leva os inteiros não negativos nos naturais pares e o negativos nos ímpares.

   Dado $n \in \mathbb{N}$, se n é par então $n = 2z$ para algum $z \in \mathbb{N}$, portanto $f(z) = n$; senão n é ímpar, $n = 2z-1$ para algum $z \in \mathbb{Z}^+$, portanto $f(-z) = 2(-(-z))-1 = n$. Assim f é sobrejetora. Agora, se $f(z_1) = f(z_2)$ então $2z_1 = 2z_2$ ou $2(-z_1)+1 = 2(-z_2)-1$ e em ambos os casos $z_1 = z_2$. Portanto a função é bijetora.

2. $|\mathbb{N}| = |\mathbb{N}\times\mathbb{N}|$: pelo teorema fundamental da aritmética todo número natural pode ser escrito de modo único como $2^k\ell$ com ℓ ímpar, portanto da forma $2m+1$ para algum natural m. Defina a função $f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ por $f(0,0) = 0$ e, nos outros casos $f(n,m) = 2^n(2m+1)$. Essa função é sobrejetiva pelo teorema fundamental da aritmética, como foi explicado acima. Se $2^x(2y+1) = 2^n(2m+1)$ então $2y+1 = 2^{n-x}(2m+1)$ e como o lado esquerdo é ímpar, $n = x$ e disso $m = y$. Portanto a função é injetiva.

3. $|\mathbb{N}| = |\mathbb{Q}|$: pela proposição 164 $|\mathbb{N}| \leq |\mathbb{Q}|$. Para mostrar que $|\mathbb{Q}| \leq |\mathbb{N}|$ consideremos os racionais expressos na forma canônica reduzida, isto é, são as frações

$$\frac{p}{q},\ p \in \mathbb{Z} \text{ e } q \in \mathbb{N}\setminus\{0\},\ \text{mdc}(p,q) = 1$$

   agora, definimos $g : \mathbb{Q} \to \mathbb{N}$ por

$$g\left(\frac{p}{q}\right) = \begin{cases} 0, & \text{se } p = 0 \\ 2^p 3^q, & \text{se } p > 0 \\ 5^{-p}3^q, & \text{se } p < 0 \end{cases}$$

   que é injetiva. É possível exibir um bijeção entre $\mathbb{Q}$ e $\mathbb{N}$ mas isso é mais trabalhoso para descrever.

4. $|R| = |(0,1)|$: do exemplo 162 e equação (5.1) temos as bijeções f e g cuja composição $f \circ g : \mathbb{R} \to (0,1)$ estabelece essa igualdade, como já observamos.

5. $|\mathbb{N}| < |\mathbb{R}|$: neste exemplo temos a famosa demonstração de Cantor por diagonalização. Como $\mathbb{N} \subset \mathbb{R}$, temos $|\mathbb{N}| \leq |\mathbb{R}|$ logo precisamos mostrar que $|\mathbb{N}| \neq |\mathbb{R}|$. Para tal, mostraremos que $|\mathbb{N}| \neq |(0,1)|$. Suponha que exista $f : \mathbb{N} \to (0,1)$ bijetiva, de modo que podemos escrever uma sequência de todos os elementos do intervalo

$$\begin{aligned} f(0) &= 0{,}d_{0,0}d_{0,1}d_{0,2}d_{0,3}d_{0,4}\ldots d_{0,n}\ldots \\ f(1) &= 0{,}d_{1,0}d_{1,1}d_{1,2}d_{1,3}d_{1,4}\ldots d_{1,n}\ldots \\ f(2) &= 0{,}d_{2,0}d_{2,1}d_{2,2}d_{2,3}d_{2,4}\ldots d_{2,n}\ldots \\ &\vdots \\ f(n) &= 0{,}d_{n,0}d_{n,1}d_{n,2}d_{n,3}d_{n,4}\ldots d_{n,n}\ldots \\ &\vdots \end{aligned}$$

   com $d_{i,j} \in \{0,1,2,3,4,5,6,7,8,9\}$. Consideremos o número real

$$\alpha = 0{,}d_0d_1d_2d_3\ldots d_n\ldots \text{ com } d_i \in \{0,1,2,3,4,5,6,7,8,9\}\setminus\{0,9,d_{i,i}\}$$

   para todo i. Esse número α pertence ao intervalo $(0,1)$ pois $d_i \neq 0$, logo α é diferente de $0 = 0{,}00000\ldots$, e $d_i \neq 9$ logo α é diferente de $1 = 0{,}9999\ldots$. Ademais, $\alpha \neq f(i)$ pois $d_i \neq d_{i,i}$ para todo $n \in \mathbb{N}$, uma contradição. Portanto, não existe $f : \mathbb{N} \to (0,1)$ bijetiva, tampouco $f : \mathbb{N} \to \mathbb{R}$ bijetiva.

6. $\left|\mathbb{R}^2\right| = |R|$: ou seja, o plano cartesiano tem tantos pontos quantos um de seus eixos. Aqui é suficiente mostrarmos que $|(0,1)\times(0,1)| \leq |(0,1)|$ pois temos $|(0,1)| \leq |(0,1)\times(0,1)|$ por $f(x) = (x,x)$ para todo x, bijetiva. Um ponto no quadrado $(0,1)\times(0,1)$ é da forma (x,y) com $x = 0,a_1a_2a_3\ldots$ e $y = 0,b_1b_2b_3\ldots$ (se tiver mais de uma representação[2] tomamos a finita) e uma função injetiva sobre $(0,1)$ é dada quando mapeamos o ponto (x,y) em $0,a_1b_1a_2b_2a_3b_3\ldots$ de $(0,1)$.

7. $\left|2^{\mathbb{N}}\right| = |\mathbb{R}|$: o conjunto das partes de $\mathbb{N}$ tem tantos elementos quanto $\mathbb{R}$. Vamos assumir que $|\mathbb{R}| = |[0,1)|$. Que $\left|2^{\mathbb{N}}\right| \leq |[0,1)|$: um subconjunto $B \subseteq \mathbb{N}$ pode ser representado por uma sequência binária infinita $b_0b_1b_2\ldots$ em que $b_i = 1$ se, e só se, $i \in B$, para todo $i \in \mathbb{N}$. Essa sequência é mapeada na representação binária $0,b_0b_1b_2\ldots$ de um número real do intervalo $[0,1)$; tal função é injetora. Agora, que $|[0,1)| \leq \left|2^{\mathbb{N}}\right|$: defina $f(0,d_1d_2d_3,\ldots) = \{10d_1, 10^2d_2, 10^3d_3,\ldots\}$ e verifique que f é injetiva (se $0,d_1d_2d_3\ldots$ for um real com mais de uma representação tomamos a finita).

5.1.2 Conjuntos finitos

Intuitivamente, um conjunto é finito quando tem uma quantidade de elementos descrita por um número natural, ou seja, A finito significa que $|A| \in \mathbb{N}$.

Definição 166. Definimos

$$[n] = \{0,1,\ldots,n-1\}$$

para todo natural n.

A **cardinalidade** de A é 0 se, e só se, A é vazio

$$|\varnothing| = 0.$$

Se $A \neq \varnothing$ então

$$|A| = n$$

se, e só se, existe uma bijeção $f\colon [n] \to A$.

Para um conjunto não vazio, a cardinalidade está bem definida, não é possível que um conjunto A esteja em correspondência biunívoca com $[n]$ e $[m]$ para dois números naturais diferentes m e n, isso implicaria numa bijeção entre $[m]$ e $[n]$ o que não é possível pelo princípio das gavetas: *se m objetos são distribuídos em n < m gavetas, então alguma gaveta guarda mais que um objeto.*

TEOREMA 167 (PRINCÍPIO DAS GAVETAS (PG)) *Se $1 \leqslant n < m$ então não existe função $f\colon [m] \to [n]$ injetiva.*

DEMONSTRAÇÃO. A prova é por indução em n. Vamos demonstrar que vale a seguinte propriedade, que denotamos por $P(n)$, para todo $n \geqslant 1$:

Para todo natural $m \geqslant 1$, se $f\colon [m] \to [n]$ é injetiva, então $m \leqslant n$.

Podemos assumir $m > 1$, no caso $m = 1$ a sentença acima é verdadeira trivialmente.

A base é o caso $n = 1$. Nesse caso a função é constante $f\colon [m] \to \{0\}$, portanto, se $m > 1$ então há $x \neq y$ em $[m]$ tal que $f(x) = f(y) = 0$, logo f não é injetiva e a sentença vale por vacuidade.

Para provar o passo, seja $k \geqslant 1$ um natural arbitrário e vamos provar que $P(k)$ implica $P(k+1)$. Assumamos que

para todo natural $m \geqslant 1$, se $f\colon [m] \to [k]$ é injetiva, então $m \leqslant k$

é verdadeiro. Tomemos $m > 1$ e $f\colon [m] \to [k+1]$ arbitrários, respectivamente, um natural e uma função injetiva.

Se $k+1 \notin \mathrm{Im}(f)$ então $g\colon [m] \to [k]$ dada por $g(x) = f(x)$ está bem definida e é injetiva. Pela hipótese de indução temos $m \leqslant k$ portanto $m < k+1$.

Agora, se $k+1 \in \mathrm{Im}(f)$, continuamos a demonstração em 2 casos: $f(m) = k+1$ ou $f(j) = k+1$ para algum j, com $1 \leqslant j < m$.

Caso 1: Definimos $g\colon [m-1] \to [k]$ por $g(x) = f(x)$. De f injetiva e $f(m) = k+1$ temos que g está bem definida e é injetiva. Pela hipótese de indução $m-1 \leqslant k$, portanto, $m \leqslant k+1$, ou seja, $P(k+1)$ é verdadeiro.

Caso 2: Nesse caso vamos construir uma $h\colon [m] \to [m]$ tal que $f \circ h\colon [m] \to [k+1]$ recaia no caso anterior. Seja $j \in [m]$ tal que $j < m$ e $f(j) = k+1$. Defina h por

$$h(x) = \begin{cases} x & \text{se } x \neq j, m \\ m & \text{se } x = j \\ j & \text{se } x = m \end{cases}$$

e temos que $f \circ h(m) = f(j) = k+1$. Pelo caso 1 $P(k+1)$ é verdadeiro. Portanto, pelo PIF, $P(n)$ é verdadeiro para todo $n \geqslant 1$. □

O princípio das gavetas também é conhecido como princípio da casa dos pombos.

[2] E.g., 0,5 = 0,49999…; esse fenômeno não ocorre com irracionais. Todo real tem no máximo duas representações e uma delas é finita

Exercício 168. Deduza PIF do PG.

O seguinte corolário do PG estabelece que a cardinalidade de qualquer conjunto A está bem definida quando $|A| \in \mathbb{N}$.

COROLÁRIO 169 *Se $A \neq \varnothing$ é conjunto e $f\colon [n] \to A$ e $g\colon [m] \to A$ são bijeções então $m = n$.*

Definição 170. A é **finito** se, e só se, $|A| = n$ para algum $n \in \mathbb{N}$.

A é **infinito** se, e só se, não é finito.

A relação $\leq$ entre cardinais no caso finito concorda com a representação conjuntista de número natural, os números ordinais de von Neumann, que apresentamos na página 72: $0 = \varnothing$, $1 = \{\varnothing\}$, $2 = \{0,1\}, \ldots, n = \{0,1,\ldots,n-1\}$,e assim por diante. Assim $3 \leq 4$ pois existe $f : \{0,1,2\} \to \{0,1,2,3\}$ injetiva, a saber $f(n) = n$.

Definição 171. Se $A \neq \varnothing$ é finito então uma bijeção f que prova a finitude é chamada de **enumeração** ou **contagem** dos elementos de A. Desse modo,

$$A = \{f(0), f(1), \ldots, f(n-1)\}$$

e dizemos que A tem n elementos.

Princípios de contagem

As seguintes propriedades de conjuntos finitos definem dois princípios básicos de contagem.

TEOREMA 172 (PRINCÍPIO ADITIVO) *Se A e B são conjuntos finitos e disjuntos, então $|A \cup B| = |A| + |B|$.*

DEMONSTRAÇÃO. Sejam A e B conjuntos disjuntos com cardinalidade n e m, respectivamente. Se um deles for vazio então o teorema vale como pode ser verificado facilmente. Vamos supor $m, n > 0$ e vamos mostrar uma bijeção $h : [n+m] \to A \cup B$.

Se $f : [n] \to A$ e $g : [m] \to B$ são bijeções então definimos h por

$$h(x) = \begin{cases} f(x) & \text{se } 0 \leqslant x < n \\ g(x-n) & \text{se } n \leqslant x < n+m. \end{cases}$$

h é sobrejetora: se $y \in A \cup B$, então $y \in A$ ou $y \in B$, mas não em ambos já que são disjuntos. Se $y \in A$ então $f(x) = y$ para algum $x \in [n]$, portanto $h(x) = y$. Se $y \in B$ então $g(x) = y$ para algum $x \in [m]$, portanto, $h(x+n) = g(x)$. Ainda, h é injetora: como A e B são disjuntos, se $h(x) = h(y)$ então $f(x) = f(y)$ ou $g(x) = g(y)$, em ambos os casos $x = y$. □

Exercício 173. Prove usando indução em n que se $A_1, \ldots, A_n$ são conjuntos dois-a-dois disjuntos então

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

TEOREMA 174 (PRINCÍPIO MULTIPLICATIVO (PM)) *Se A e B são conjuntos finitos e não vazios, então $|A \times B| = |A| \cdot |B|$.*

DEMONSTRAÇÃO. Seja $n = |A|$ e $A = \{f(1), f(2), \ldots, f(n)\}$ para alguma enumeração f de A. Definimos os conjuntos dois-a-dois disjuntos

$$E_i = \{(f(i), b) \in A \times B : b \in B\}$$

de modo que $|E_i| = |B|$, para todo i, pela bijeção $g_i : E_i \to B$ dada por $g_i\big((f(i), b)\big) = b$ para todo i.

Assim, $E_1, \ldots, E_n$ satisfaz a hipótese do exercício anterior e $\bigcup_i E_i$ é $A \times B$ (verifique), logo

$$|A \times B| = \left| \bigcup_{i=1}^{n} E_i \right| = \sum_{i=1}^{n} |B| = |A||B|$$

onde a segunda igualdade segue do exercício 173. □

Exercício 175. Prove o teorema acima usando exibindo uma bijeção entre $\big[|A||B|\big]$ e $A \times B$.

Exercício 176. Prove por indução em n que para todo $n \geqslant 1$, $|\{0,1\}^n| = 2^n$.

TEOREMA 177 *Todo conjunto A de cardinalidade $n \in \mathbb{N}$ tem 2^n subconjuntos distintos, isto é,*

$$\left|2^A\right| = 2^{|A|}.$$

DEMONSTRAÇÃO. Seja A um conjunto de cardinalidade n. Se $n = 0$ então $A = \varnothing$ é o único subconjunto dele mesmo e $2^0 = 1$. Senão $n \geqslant 1$, então existe uma bijeção $f : [n] \to A$. Como $A = \{f(0), f(1), f(2), \ldots, f(n-1)\}$, cada subconjunto $B \subset A$ corresponde a uma, e só uma, sequência binária $\mathbf{b}(B) = (b_0, b_1, \ldots, b_{n-1}) \in \{0,1\}^n$ dada por

$$b_i = 1 \text{ se, e só se } f(i) \in B$$

para cada $i \in [n]$, ou seja

$$\begin{aligned} \mathbf{b} : 2^A &\to \{0,1\}^n \\ B &\mapsto \mathbf{b}(B) \end{aligned}$$

assim definida é bijetiva (verifique), de modo que $|2^A| = |\{0,1\}^n| = 2^n$. □

5.1.3 Conjuntos enumeráveis

O conjunto $\mathbb{N}$ dos números naturais não é finito. De fato, se houvesse uma bijeção $f : [n] \to \mathbb{N}$ então tomaríamos o número natural $m = f(0) + f(1) + \cdots + f(n-1)$ de modo que m pertenceria à imagem de f contradizendo que $m > f(i)$ para todo $i \in [n]$.

Na definição 171 colocamos que se $A \neq \varnothing$ é finito então seus elementos podem ser enumerados $f(0), f(1), \ldots, f(n-1)$, o mesmo vale quando $|A| = |\mathbb{N}|$ pois a bijeção f que estabelece a igualdade define uma sequência $f_0, f_1, \ldots$. Nesses dois casos dizemos que A é enumerável. Vimos que $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ são enumeráveis e que $\mathbb{R}$ não é enumerável.

Definição 178. O conjunto A é dito **enumerável** se é finito ou se tem a mesma cardinalidade de $\mathbb{N}$.

A cardinalidade de $\mathbb{N}$ e, portanto, do conjuntos enumeráveis infinitos, é denotada por $\aleph_0$ (álefe-zero) e é o menor cardinal não finito.

5.1.4 Conjuntos infinitos

Vimos acima que $|\mathbb{R}|$, cuja cardinalidade é denotada por $\mathfrak{c}$ e chamada de **cardinalidade do contínuo**, é maior que $\aleph_0$. No caso de conjuntos infinitos não se pode falar em quantidade de elementos e, além disso, dizer simplesmente que são infinitos elementos não diz muita coisa desde que Cantor nos mostrou a possibilidade de vários "tamanhos" de infinito, como veremos a seguir.

TEOREMA 179 (TEOREMA DE CANTOR) *Para todo conjunto A, $|A| < |2^A|$.*

DEMONSTRAÇÃO. Se A é finito então $|A| < 2^{|A|}$. Seja A um conjunto infinito e vamos mostrar que $|A| \leq |2^A|$ e que $|A| \neq |2^A|$. A função

$$\begin{aligned} f : A &\to 2^A \\ a &\mapsto \{a\} \end{aligned}$$

é injetiva, portanto $|A| \leq |2^A|$.

Para mostrar que $|A| \neq |2^A|$ provaremos (por contradição) que não há sobrejeção $g : A \to 2^A$. Suponhamos que $g : A \to 2^A$ é sobrejetiva. Definimos

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

$B \subset A$ e g sobrejetiva implica que $B = g(b)$ para algum b. Se $b \in B$ então $b \notin g(b) = B$, pela definição do conjunto B. Também, se $b \notin B$ então $b \in g(b) = B$, ou seja, $b \notin B \Leftrightarrow b \in B$, uma contradição. □

Em particular, temos

$$|\mathbb{N}| < \left|2^{\mathbb{N}}\right| < \left|2^{2^{\mathbb{N}}}\right| < \left|2^{2^{2^{\mathbb{N}}}}\right| < \cdots$$

Uma dúvida que pode ter surgido nesse capítulo é saber se vale a lei de tricotomia para cardinalidades, ou seja, para quaisquer A e B, ou $|A| < |B|$, ou $|A| = |B|$, ou $|B| < |A|$. De fato, vale tal lei se assumirmos que vale o axioma da escolha. Nesse caso, vale que para qualquer conjunto A

1. se $|A| < |\mathbb{N}|$ então A é finito e enumerável;
2. se $|A| = |\mathbb{N}|$ então A é infinito e enumerável;
3. se $|A| > |\mathbb{N}|$ então A é infinito e não enumerável.

A hipótese do contínuo

Cantor conjeturou que não há um cardinal entre $\aleph_0$ e $\mathfrak{c}$. Por quase um século após a descoberta de Cantor de que há diferentes infinitos muitos matemáticos atacaram o problema de descobrir se existe um conjunto A tal que $|\mathbb{N}| < |A| < |2^{\mathbb{N}}|$. Suspeitava-se que tal conjunto não existiria e a sentença que *não existe tal A* é conhecida como **hipótese do contínuo**. Gödel, nos anos 1930, provou que a negação da hipótese do contínuo não pode ser provada a partir dos axiomas ZFC. Em 1964, Paul Cohen descobriu que nenhuma prova pode deduzir a hipótese do contínuo a partir dos axiomas de ZFC. Tomados em conjunto, os resultados de Gödel e Cohen significa que dos axiomas padrão da Teoria dos Conjuntos não se pode decidir se a hipótese do contínuo é verdadeira ou falsa; nenhum conflito lógico surge a partir da afirmação ou negação da hipótese do contínuo. Dizemos que a hipótese do contínuo é independente de ZFC. Assumindo a hipótese do contínuo temos $\aleph_0 = |\mathbb{N}|$ e $\aleph_1 = |2^{\aleph_0}| = \mathfrak{c}$. De modo geral, para α ordinal, $\aleph_{\alpha+1} = |2^{\aleph_\alpha}|$.

5.1.5 O princípio das gavetas revisitado

O princípio das gavetas (ou da casa dos pombos), teorema 167, é outro princípio muito útil em demostrações: *se $m > 1$ objetos são guardados em $n < m$ gavetas então alguma gaveta tem mais que um objeto.*

Vejamos uns exemplos de aplicação. Dado $m \in \mathbb{N}$, existem números inteiros positivos a e b, com um $a \neq b$, tal que $m^a - m^b$ é divisível por 10. Considere os seguintes 11 números

$$m^1,\ m^2,\ m^3,\ m^4,\ m^5,\ m^6,\ m^7,\ m^8,\ m^9,\ m^{10},\ m^{11}$$

como há 10 possibilidades para o algarismo da unidade, dois desses números, digamos m^a e m^b com $a \neq b$, termina com o mesmo algarismo de modo que $m^a - m^b$ é divisível por 10.

Agora, seja n um natural. Em qualquer escolha de mais do que n números do conjunto $\{1,2,\ldots,2n\}$ haverá dois números dentre os escolhidos tais que um é múltiplo do outro. Pelo teorema fundamental da aritmética, todo $r \in \{1,2,\ldots,2n\}$ é de forma $r = 2^a t$ com únicos $a, t \in \mathbb{N}$ e t ímpar. De $r \leqslant 2n$ temos $t \leqslant n$. Logo, em mais do que n números dois deles terão o mesmo divisor ímpar, digamos $r = 2^a t$ e $s = 2^b t$. O maior deles é múltiplo do menor.

Exercício 180. Prove que se os pontos do plano euclidiano são pintados usando duas cores, então existem dois pontos de mesma cor que distam 1.

Solução: Fixe uma coloração qualquer dos pontos do plano com duas cores e tome um triângulo equilátero de lado 1 qualquer (figura 5.2). Dos 3 vértices, 2 devem ter a mesma cor pelo PG. □

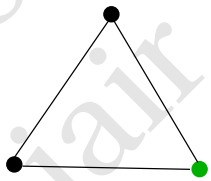


Figura 5.2: triângulo equilátero de lado 1

Exercício 181. Prove que se os pontos do plano euclideano são pintados usando três cores, então existem dois pontos de mesma cor que distam 1.

Solução. Tome uma circunferência Γ de centro C e raio $\sqrt{3}$. Se os pontos de $\Gamma \cup \{C\}$ recebem a mesma cor então há uma corda de comprimento 1 cujas extremidades têm a mesma cor. Senão em Γ há um ponto D de cor diferente da cor de C. Construa as circunferências de raio 1 centradas em C e em D (figura 5.3). O encontro delas em A e B define dois triângulos equiláteros ABC e ABD. Dentre os 4 vértices equidistantes haverá 2 da mesma cor pelo PG. □

TEOREMA 182 (PRINCÍPIO DAS GAVETAS GENERALIZADO) *Para quaisquer naturais r e $t_1, t_2, \ldots, t_r$ vale o seguinte. Em toda distribuição de $(t_1 - 1) + (t_2 - 1) + \cdots + (t_r - 1) + 1$ objetos em r gavetas, existe um $i \in \{1,2,\ldots,r\}$ tal que na i-ésima gaveta há pelo menos t_i objetos.*

DEMONSTRAÇÃO. A prova é por contradição, assuma que na gaveta i ficam no máximo $t_i - 1$ objetos, para todo i. Então o número total de objetos é $(t_1 - 1) + (t_2 - 1) + \cdots + (t_r - 1)$, que é uma contradição. □

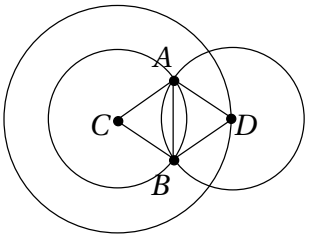


Figura 5.3: dentre os 4 pontos equidistantes A, B, C, D há 2 de mesma cor

Fazendo $t_i = t$ para todo i no teorema obtemos o seguinte resultado.

COROLÁRIO 183 *Em toda distribuição de $r(t-1)+1$ objetos em r gavetas há pelo menos t objetos numa mesma gaveta.*

Como aplicação desse resultado vejamos o seguinte, que é um teorema conhecido numa disciplina da combinatória conhecida como Teoria de Ramsey.

TEOREMA 184 (PRINCÍPIO DAS GAVETAS ORDENADO) *Toda sequência de $mn+1$ números reais possui uma subsequência crescente de $m+1$ termos ou uma subsequência decrescente $n+1$ termos.*

DEMONSTRAÇÃO. Sejam $a_1, a_2, \ldots, a_{mn+1}$ uma sequência numérica. Para cada a_i, seja C_i o número de termos da maior subsequência crescente começando em a_i. Se $C_i > m+1$, para algum i, então temos uma subsequência crescente de tamanho $m+1$. Senão, suponha $C_i \leqslant m$ para todo i e defina a função

$$\begin{aligned} \varphi\colon \{a_1, \ldots, a_{mn+1}\} &\to \{1, 2, \ldots, m\} \\ a_i &\mapsto C_i. \end{aligned}$$

Pelo corolário 183, em toda distribuição de $mn+1$ objetos em m gavetas haverá alguma gaveta com pelo menos $n+1$ objetos, digamos $G = \{a_{j_1}, a_{j_2}, \ldots a_{j_{n+1}}\}$ com, s.p.g., $j_1 < j_2 < \cdots < j_{n+1}$.

Se, para algum k, vale $a_{j_k} < a_{j_{k+1}}$, então teríamos um sequência crescente de comprimento m começando em $a_{j_{k+1}}$ (por hipótese) e, consequentemente, uma sequência crescente de tamanho $s+1$ começando em a_{j_k}, o que dá uma contradição pois a cor de a_{j_k} é s.

Desse modo, concluímos que $a_{j_1} \geqslant a_{j_2} \geqslant \cdots \geqslant a_{j_{n+1}}$, i.e., é uma subsequência decrescente com $n+1$ termos. □

Agora, considere que n objetos são distribuídos aleatoriamente, de modo uniforme e independente, em r gavetas. Isso pode ser entendido de duas maneiras essencialmente equivalentes do ponto de vista probabilístico: (1) para cada objeto sorteamos com probabilidade $1/r$ uma das gavetas para guardá-lo ou (2) sorteamos uma das r^n funções φ do conjunto de objetos para o conjunto de gavetas com cada função tendo a mesma probabilidade de ser sorteada.

Denote por C a quantidade de pares de objetos que caem numa mesma gaveta. Note que isso é mais interessante se $n \leqslant r$, nesse caso, há $r(r-1)(r-2)\cdots(r-n+1)$ modos diferentes de distribuir os n objetos sem repetir gaveta.

Se $(\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_n))$ é uma escolha aleatória dentre as r^n funções então nessa escolha

$$\mathbb{P}[C=0] = \frac{r(r-1)(r-2)\cdots(r-n+1)}{r^n} = \prod_{j=1}^{n-1}\left(1-\frac{j}{r}\right)$$

agora, usamos que $1-x < \exp(-x)$ e obtemos

$$\mathbb{P}[C=0] < \exp\left(-\frac{1}{r}\right)\exp\left(-\frac{2}{r}\right)\cdots\exp\left(-\frac{n-1}{r}\right) = \exp\left(-\frac{n(n-1)}{2r}\right).$$

TEOREMA 185 (PRINCÍPIO DAS GAVETAS PROBABILÍSTICO) *Numa distribuição ao acaso, em r gavetas, de $n \leqslant r$ objetos a probabilidade com que exista pelo menos dois objetos numa mesma gaveta é maior que*

$$1 - \exp\left(-\frac{n(n-1)}{2r}\right).$$

O conhecido *paradoxo dos aniversários* é o caso $n = 23$ e $r = 365$ na equação acima: $\mathbb{P}[C > 0] > 0{,}5$, ou seja, apenas 23 pessoas são suficientes para que duas delas façam aniversário no mesmo dia com probabilidade maior que $1/2$, supondo que os nascimentos ocorram uniformemente ao longo do ano. Para 75 ou mais pessoas, a probabilidade é maior do que 99,9%.

O paradoxo do aniversário é contra-intuitivo e só é chamado de "paradoxo" por causa do estranhamento causado pelo fato de que "apenas" 23 pessoas são necessárias para se obter 50% de probabilidade para duas pessoas nascerem no mesmo dia.

PG prova o PIF

Agora, para explorar o força do PG, vejamos que o PIF é uma consequência do PG na teoria dos conjuntos. Como provamos o PG do PIF, segue que tais princípio são logicamente equivalentes. Seja P um predicado dos números naturais e assuma

(i) $P(0)$ é verdadeiro e

(ii) $\forall n \in \mathbb{N}(P(n) \to P(n+1))$ é verdadeiro.

Vamos demonstrar que $P(n)$ vale para todo n por contradição.

Suponha que existe $m \in \mathbb{N}$ tal que não-$P(m)$. De (i) temos $m \geqslant 1$ e assim podemos definir uma função $\varphi\colon [m] \to [m-1]$ por

$$\varphi(i) = \begin{cases} i & \text{se } P(i) \\ i-1 & \text{se não-}P(i). \end{cases}$$

Tal função está bem definida. Pelo PG existem $i \neq j$ no domínio da φ tais que $\varphi(i) = \varphi(j)$, pois $\varphi\colon [m] \to [m-1]$ não pode ser injetiva.

De $i \neq j$, $\varphi(i) = \varphi(j)$ e da definição da φ temos que

$$\varphi(i) = i = j-1 = \varphi(j) \quad \text{ou} \quad \varphi(i) = i-1 = j = \varphi(j).$$

No primeiro caso, $j = i+1$, vale $P(i)$ mas não vale $P(j) = P(i+1)$ contrariando a hipótese de $P(i) \to P(i+1)$ verdadeiro. No segundo caso a dedução é análoga e contraria $P(j) \to P(j+1)$ verdadeiro. Com isso, a hipótese assumida de haver $m \in \mathbb{N}$ tal que não-$P(m)$ não pode ser verdadeira, ou seja, $P(n)$ vale para todo natural n. □

5.1.6 Demonstração do Teorema de Cantor–Schröder–Bernstein

Antes de demonstrar o teorema vamos adotar a seguinte convenção notacional: $\overline{A}^X = X \setminus A$.

DEMONSTRAÇÃO. Sejam A e B conjuntos tais que $|A| \leq |B|$ e $|B| \leq |A|$ e vamos mostrar que $|A| = |B|$. Sejam $f : A \to B$ e $g : B \to A$ funções injetivas, que existem por hipótese. Vamos mostrar que existe uma bijeção $h : A \to B$.

Definimos, para todo $X \subset A$

$$F(X) = A \setminus g(B \setminus f(X)) = A \setminus g\left(\overline{f(X)}^B\right) = \overline{g\left(\overline{f(X)}^B\right)}^A$$

onde $f(X)$ é o subconjunto de B formado pela imagem dos elementos de X. Vamos mostrar que existe $A_0 \subset A$ tal que $F(A_0) = A_0$. Primeiro, notemos que par uma sequência qualquer $(A_i : i \geqslant 1)$ de subconjuntos de A temos

$$\begin{aligned}
F\left(\bigcap_{i\geqslant 1} A_i\right) &= \overline{g\left(\overline{f(\bigcap_{i\geqslant 1} A_i)}^B\right)}^A && \text{por definição} \\
&= \overline{g\left(\overline{\bigcap_{i\geqslant 1} f(A_i)}^B\right)}^A && \text{pois f é injetiva} \\
&= \overline{g\left(\bigcup_{i\geqslant 1} \overline{f(A_i)}^B\right)}^A && \text{por De Morgan} \\
&= \overline{\bigcup_{i\geqslant 1} g\left(\overline{f(A_i)}^B\right)}^A && \text{pois g é injetiva} \\
&= \bigcap_{i\geqslant 1} \overline{g\left(\overline{f(A_i)}^B\right)}^A && \text{por De Morgan} \\
&= \bigcap_{i\geqslant 1} F(A_i) && \text{por definição de F.}
\end{aligned}$$

Tomemos

$$A_0 = A \cap F(A) \cap F^2(A) \cap F^3(A) \cap \cdots$$

onde $F^n(A) = F(F^{n-1}(A))$ donde temos

$$F(A_0) = F\Big(A \cap F(A) \cap F^2(A) \cap F^3(A) \cap \cdots\Big) = F(A) \cap F(F(A)) \cap F(F^2(A)) \cap F(F^3(A)) \cap \cdots$$

logo $F(A_0) = F(A) \cap F^2(A) \cap F^3(A) \cap F^4(A) \cap \cdots = A_0$ pois $A \supset F(A) \supset F^2(A) \supset \cdots$.

Desse modo $h : A \to B$ dado por

$$h(x) = \begin{cases} f(x), & \text{se } x \in A_0 \\ g^{-1}(x), & \text{caso contrário, isto é } x \in g\left(\overline{f(A_0)}^B\right) \end{cases}$$

é uma bijeção. Que é sobrejetiva: seja $y \in B$. Se $y \in f(A_0)$, então $y = f(x)$ para $x \in A_0$, portanto $y = h(x)$; senão, $y \notin f(A_0)$, ou seja $y \in \overline{f(A_0)}^B$, logo $g(y) \notin A_0$ logo $h(g(y)) = g^{-1}(g(y)) = y$, portanto h é sobrejetora. Que é injetiva: sejam $x, y \in A$ com $x \neq y$. A demonstração segue em três casos; (i) se $x, y \in A_0$ então $h(x) = f(x) \neq f(y) = h(y)$; (ii) se $x \in A_0$, então $h(x) = f(x) \in f(A_0)$, e se $y \notin A_0$, ou seja $y \in g\left(\overline{f(A_0)}^B\right)$, então $h(y) = g^{-1}(y) \in g^{-1}\left(g\left(\overline{f(A_0)}^B\right)\right) = \overline{f(A_0)}^B$, portanto $h(x) \neq h(y)$; (iii) se $x, y \notin A_0$ então $h(x) = g^{-1}(x) \neq g^{-1}(y) = h(y)$. Em todos os casos $h(x) \neq h(y)$, logo h é injetora. □

Exercícios

1. Verifique que $g : \mathbb{R} \to (0, +\infty)$, dada por $g(x) = 2^x$ é bijetiva.

2. Verifique que $g : \mathbb{Q} \to \mathbb{N}$ por

$$g\left(\frac{p}{q}\right) = \begin{cases} 0, & \text{se } p = 0 \\ 2^p 3^q, & \text{se } p > 0 \\ 5^{-p} 3^q, & \text{se } p < 0 \end{cases}$$

   é bijetiva.

3. Seja A um conjunto de cardinalidade n e f uma enumeração de A. Dado $B \subseteq A$, defina $b_i \in \{0,1\}$ para todo $i \in [n]$, por $b_i = 1$ se, e só se, $f(i) \in B$. Verifique que a função

$$\begin{array}{rccc} \mathbf{b}: & 2^A & \to & \{0,1\}^n \\ & B & \mapsto & (b_0, b_2, \ldots, b_{n-1}) \end{array}$$

   é bijetiva.

4. A **função de pareamento de cantor** é uma função que atribui números naturais consecutivos a pontos ao longo das diagonais no plano (veja a figura 5.4). A função é $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por

$$f(u, v) = \frac{(u+v)(u+v+1)}{2} + u.$$

   Prove que essa função é uma bijeção e determine a inversa.

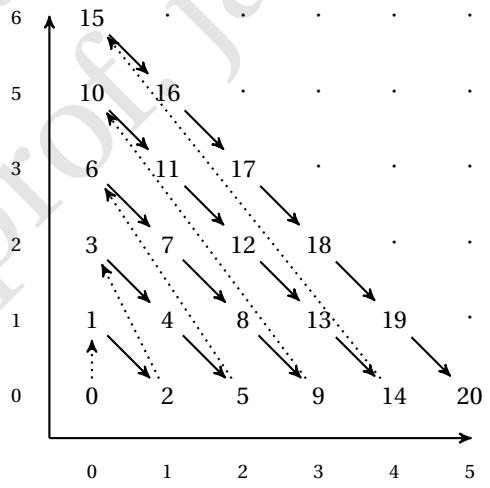


Figura 5.4: função de pareamento de Cantor

5. Prove ou dê um contraexemplo para a seguinte sentença: A é infinito se, e somente se, $|A| \geqslant n$ para todo $n \in \mathbb{N}$.

6. Sejam $A_1, A_2, \ldots, A_n$ conjuntos finitos e não vazios. Prove usando indução que

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

7. Seja $A \subset \mathscr{U}$ tal que $|2^A| = n$. Determine $|2^B|$ se

   (a) $B = A \cup \{x\}$ para algum $x \in \mathscr{U} \setminus A$;

   (b) $B = A \cup \{x, y\}$ para algum $x, y \in \mathscr{U} \setminus A$;

   (c) $B = A \cup \{x_1, x_2, \ldots, x_k\}$ para $x_1, x_2, \ldots, x_k \in \mathscr{U} \setminus A$.

8. Mostre que o conjunto dos inteiros ímpares (números da forma $2k+1$ com $k \in \mathbb{Z}$) tem a mesma cardinalidade que $\mathbb{N}$.

9. Verifique se é verdadeira ou falsa cada uma das afirmações a seguir. No caso de ser falsa, apresente um contra-exemplo.

   (a) se A e B são infinitos então $A \cap B$ é infinito;

   (b) se B é infinito $A \subseteq B$ então A é infinito;

   (c) se B é finito $A \subseteq B$ então A é finito;

   (d) se A é finito $A \subseteq B$ então B é finito.

10. Use o argumento da diagonal de Cantor para mostrar quer $\wp(\mathbb{N})$ não é enumerável.

11. Prove que acrescentar um novo elemento a um conjunto finito resulta num conjunto finito.

12. Prove que remover um elemento de um conjunto infinito resulta num conjunto infinito

13. Prove que todo subconjunto de um conjunto finito também é finito.

14. Prove que todo conjunto infinito contém um subconjunto infinito enumerável.

15. Prove que todo conjunto infinito contém um subconjunto próprio de mesma cardinalidade.

16. Prove ou refute: se A não é enumerável então $|A| = |\mathbb{R}|$.

17. Prove ou refute: Se $A \subseteq B \subseteq C$ e A e C infinitos e enumeráveis então B é infinito enumerável.

18. Prove ou refute : Todo conjunto infinito é subconjunto de um conjunto infinito enumerável.

19. Prove ou refute : Se $A \subseteq B$ e A é infinito e enumerável e B não enumerável, então $B \setminus A$ não é enumerável.

20. Prove que se A e B são enumeráveis então $A \cup B$ é enumerável e $A \times B$ é enumerável.

21. Um conjunto A é chamado de Peano-finito se e somente se existe um natural n e uma bijeção entre A e $[n]$, e é chamado de Peano-infinito se e somente se A não é Peano-finito.

    Um conjunto A é Dedekind-infinito se há uma bijeção entre A e algum subconjunto próprio de A; caso contrário é Dedekind-finito.

    Prove por indução que se um conjunto é Peano-finito, então é Dedekind-finito. Usando o Princípio de Boa Ordem provar que se um conjunto é Peano-infinito, então é Dedekind-infinito.

22. Prove que o PM é equivalente ao PIF, portanto ao princípio da descida infinita de Fermat, ao PBO e ao PG (*sugetão*: PM⇒PG e PIF⇒PM).

23. Enuncie formalmente e dê uma prova para o **princípio das gavetas infinitário**: *se todo número natural é guardado em alguma dentre r gavetas então alguma gaveta tem um quantidade infinita enumerável de números naturais.*

24. Demonstre usando o princípio da casa dos pombos as afirmações abaixo.

    (a) Para quaisquer seis (ou mais) usuários do *facebook*, há sempre três deles amigos entre si ou há três deles desconhecidos entre si.

    (b) Em grupo com 17 (ou mais) pessoas, podemos encontrar três pessoas que se amam entre si, três que se odeiam entre si ou três que são indiferentes entre si.

(c) Em qualquer escolha de mais do que n números do conjunto $[2n]$ haverão dois deles primos entre si.

(d) Se escolhemos 13 pontos no interior de um retângulo 3×4, então existem dois pontos tais que sua distância é menor ou igual a $\sqrt{2}$.

(e) $(a-b)(a-c)(b-c)$ é par, para quaisquer a, b e c inteiros.

(f) Chico e sua esposa foram a uma festa com três outros casais. No encontro deles houveram vários apertos de mão. Ninguém apertou a própria mão ou a mão da(o) esposa(o), e ninguém apertou a mão da mesma pessoa mais que uma vez. Após os cumprimentos Chico perguntou para todos, inclusive para a esposa, quantas mãos cada um apertou e recebeu de cada pessoa uma resposta diferente. Quantas mãos Chico apertou?

(g) Os pontos de uma reta são coloridos com 12 cores. Prove que existem dois pontos com a mesma cor tal que a distância entre eles é um número inteiro.

(h) Suponha que o conjunto $\{1,2,\ldots,2n\}$ foi dividido em dois subconjuntos com n elementos cada. Os elementos do primeiro conjunto foram ordenados em ordem crescente, $a_1 < a_2 < \cdots < a_n$, e os do segundo conjunto ordenados em ordem decrescente, $b_1 > b_2 > \cdots > b_n$. Prove que $\sum_{i=1}^{n} |a_i - b_i| = n^2$ (*dica*: para cada i, de a_i e b_i, um pertence a $\{1,2,\ldots,n\}$ o outro não).

25. Cada estrada na Bozolândia é de mão única e cada par de cidades é conectada por exatamente uma estrada. Prove que existe uma cidade que pode ser alcançada a partir de qualquer outra cidade ou diretamente ou indo através de no máximo uma outra cidade.

26. Num torneio de queda-de-braço no sistema de todos contra todos exatamente uma vez, cada jogo termina em uma vitória ou uma derrota. Prove que se são n competidores então podemos rotulá-los $P_1, P_2, \ldots, P_n$ de tal forma que P_1 derrotou P_2, P_2 derrotou P_3, e assim por diante até, P_{n-1} derrotou P_n.

Complemento: O problema de Hadwiger–Nelson (1950)

Qual é o menor número de cores necessárias para colorir os pontos do plano euclidiano de modo que não existam dois pontos da mesma cor que distam 1*, quatro, cinco ou seis?*

Pelo exercício 180 acima, são necessárias pelo menos 3 cores e pelo exercício 181, são necessárias pelo menos 4 cores. O exercício 181 pode ser resolvido por um método ao do exercício 180: fixe uma 3-coloração do plano e tome uma realização do grafo de Moser, cujo diagrama está mostrado na figura 5.5, no plano e com todas arestas de comprimento 1. No grafo de Moser qualquer 3-coloração dos vértices implica em dois vértices adjacentes monocromáticos (verifique). A 3-coloração do plano induz

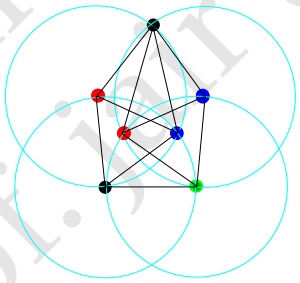


Figura 5.5: grafo de Moser com vértices adjacentes equidistantes e 4-coloridos

uma 3-coloração nos vértices grafo de Moser e dois deles, adjacentes, devem receber a mesma cor. Tais vértices distam 1 e são monocromáticos. Essa estratégia foi usada por Aubrey de Grey, um matemático amador, que em 2018 provou que não é possível colorir o plano com 4 cores. Agora, a construção é muito grande e a verificação foi feita por computador.

Um ladrilhamento do plano com hexágonos regulares prova que com sete cores nenhum par de pontos que distam 1 recebem a mesma cor. Essa solução é atribuída ao matemático John R. Isbell. As regiões hexagonais são 7-coloridas de modo que os seis vizinho de um hexágono têm seis cores diferentes e diferente do hexágono central (figura 5.6). Para hexágonos regulares de lado 0,45, o diâmetro é 0,9, e não há pontos da mesma cor que distam menos que 1,19.

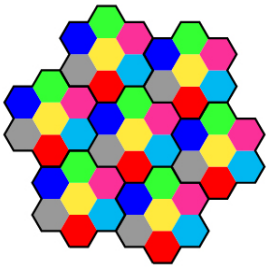


Figura 5.6: ladrilhamento 7-colorido do plano

5.2 Princípios de contagem: combinatória

Uma interpretação para o princípio aditivo, que vimos anteriormente, é: suponha que o evento E pode ocorrer n maneiras e o evento F de m maneiras distintas das outras n. Então, o número de maneiras de ocorrer o evento "E ou F" é $n+m$. No caso geral, se $A_1, \ldots, A_n$ são conjuntos dois-a-dois disjuntos então

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Por exemplo, há quantas possibilidades de escolher um inteiro entre 1 e 16 que é múltiplo de 3 ou de 7? Devemos determinar a cardinalidade do conjunto de inteiros entre 1 e 16 que são múltiplos de 3 ou múltiplos de 7, tais conjuntos são disjuntos pois $\text{mmc}(3,7) = 21$. Os múltiplos de 3 são cinco, os múltiplos de 7 são dois, portanto, os múltiplos de ambos são $5+2=7$. O evento *múltiplo de* 3 *ou múltiplo de* 7 ocorre de 7 modos distintos. E se contássemos os múltiplos de 2 e 3 entre 1 e 16? O princípio aditivo não se aplica pois alguns números são contados duas vezes, como o 6 e o 12.

Teorema 186 (Princípio de Inclusão–Exclusão) *Se E e F são conjuntos finitos (não necessariamente disjuntos) então*

$$|E \cup F| = |E| + |F| - |E \cap F|.$$

Demonstração. Sejam E e F conjuntos finitos. Podemos escrever $E = (E \cap F) \cup (E \setminus F)$, uma união disjunta (verifique). Logo, podemos usar o princípio aditivo e escrever, rearranjando os termos, que

$$|E \setminus F| = |E| - |E \cap F|. \tag{5.2}$$

Agora, escrevemos $E \cup F$ como a seguinte união de subconjuntos disjuntos (verifique) $E \cup F = (E \setminus F) \cup (F \setminus E) \cup (E \cap F)$ e, pelo princípio aditivo e (5.2), temos $|E \cup F| = |E| + |F| - |E \cap F|$. □

Por inclusão–exclusão o número de possíveis resultados que são múltiplo de 2 ou de 3 no lançamento de uma dado é dado por: os múltiplos de 2 definem o subconjunto $E = \{2,4,6\}$, os múltiplos de 3 definem o subconjunto $F = \{3,6\}$, portanto,

$$|E \cup F| = |E| + |F| - |E \cap F| = 4.$$

Exercício 187. Prove que se A, B e C são conjuntos finitos então

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|.$$

Exercício 188. Conjecture uma expressão para o princípio de inclusão–exclusão para a cardinalidade da união de n conjuntos finitos.

Em uma turma de Matemática Discreta, há 43 estudantes que fazem aula de Análise de Algoritmos, 57 estudantes que fazem Análise Real e 29 estudantes que tomam aula de Análise na Educação Básica. Há 10 alunos em Análise de Algoritmos e Análise real, 5 em Análise Real e Análise na Educação Básica, 5 em Análise de Algoritmos e Análise na Educação Básica e 2 tendo todos os três cursos. Quantos alunos estão fazendo pelo menos dos cursos de análises? Vamos indicar por C, P e E os conjuntos de alunos que fazem Análise de Algoritmos, Análise Real e Análise na Educação Básica, respectivamente. Queremos calcular $|C \cup P \cup E|$. Aplicamos inclusão–exclusão $|C \cup P \cup E| = |C| + |P| + |E| - |C \cap P| - |P \cap E| - |C \cap E| + |C \cap P \cap E| = 111$.

Exercício 189. De quantas maneiras podemos escolher um número em $\{1,2,\ldots,100\}$ que não é divisível por 2, 3 ou 5?

Podemos interpretar o princípio multiplicativo da seguinte forma: se um experimento pode ser descrito em duas etapas de modo que há n desfechos possíveis para a 1ª etapa e há m desfechos possíveis para a 2ª etapa, então o número de possíveis desfechos para o experimento é $n \cdot m$. De um modo geral, se $E_1, \ldots, E_r$ representam r etapas de experimento composto, então o números de modos distintos de realizar o experimento é

$$\left| \prod_{i=1}^{r} E_i \right| = |E_1| \cdot |E_2| \cdots |E_r|$$

que pode ser demonstrado usando princípio da indução.

Exemplo 190. Uma placa de carro é uma sequência de 3 letras seguidas por 4 dígitos. Qual é a quantidade de placas distintas que podemos obter?

Tomamos os conjuntos $E_i = \{A, B, \ldots, Z\}$ das letras do alfabeto com $i = 1,2,3$, para cada letrada placa, e os dígitos $E_i = \{0,1,2,3,4,5,6,7,8,9\}$ para $i = 4,5,6,7$, cada número da placa. Assim, a quantidade de placas distintas que podemos obter é $\left|\prod_{i=1}^{8} E_i\right| = 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 26^3 10^4 = 175.760.000$.

Exemplo 191. Cada posição da memória (célula de memória) de um computador tem um endereço que é uma sequência binária. As arquiteturas com processadores 32-bits tem capacidade para endereçamento de $2^{32} = 4.294.967.296$ posições de memória, aproximadamente 4 Gigabytes. As arquiteturas com processadores 64-bits tem capacidade para endereçamento de

$$2^{64} = 18.446.744.073.709.551.616$$

posições de memória, aproximadamente 16 Exabytes (16 milhões de Terabytes). Suponhamos que um dispositivo de 1 Gigabyte ocupe um dispositivo de dimensões 1 mm × 1 mm × 1 mm. Para guardar 16 Exabytes precisaríamos de uma quarto de dimensões 2,5 m × 2,5 m × 2,5 m.

Definição 192. Sejam A e B conjuntos não vazios. O conjunto de todas as funções de A em B é denotado por B^A.

No caso em que A e B são conjuntos finitos B^A pode ser identificado com o conjuntos de todas as sequências $(b_1, \ldots, b_{|A|})$ de comprimento $|A|$ formada por elementos de B: fixamos uma enumeração de de A e, com isso, b_1 é a imagem do *primeiro* elemento de A, b_2 é a imagem do *segundo* elemento de A, e assim por diante. Pelo princípio multiplicativo

$$\left|B^A\right| = |B|^{|A|}. \tag{5.3}$$

Notemos que essa notação estende a notação 2^A que usamos para o conjunto das partes. A definição conjuntista usual para o ordinal 2 é $2 = \{0,1\}$ e um subconjunto de A é naturalmente identificado com uma função $A \to \{0,1\}$ (veja o exercício 3, página 90 e a demonstração do teorema 177, página 85).

A seguir destacamos alguns casos particulares do princípio multiplicativo. Essencialmente, são modos de contagem do número de maneiras diferentes para selecionarmos objetos: *arranjos*, quando a ordem da seleção importa, e *combinações* quando a ordem não importa.

5.2.1 Arranjo

Uma disposição de $r \geqslant 1$ elementos tomados de um conjunto A de $n \geqslant r$ elementos em que a ordem importa é um **arranjo simples**. Cada arranjo corresponde univocamente a uma sequência $(a_1, a_2, \ldots, a_r)$ de elementos não repetidos de A.

Para formar um arranjo, temos n elementos para a primeira posição, temos $n-1$ elementos para a segunda, e assim por diante até $n-r+1$ elementos para a última posição, ou seja, uma arranjo é um elemento de $X_1 \times X_2 \times \cdots \times X_r$ com X_i um conjunto que depende de $X_1, \ldots, X_{i-1}$ e de cardinalidade $|X_i| = n - i + 1$. Pelo princípio multiplicativo temos que $|X_1, \ldots, X_{i-1}| = n \cdot (n-1) \cdots (n-r+1)$.

Proposição 193 *A quantidade de arranjos simples de r elementos tomados de um conjunto de n elementos ($1 \leqslant r \leqslant n$) é o número $(n)_r$ dado por*

$$(n)_r := n(n-1)(n-2)\cdots(n-r+1).$$

Convencionamos que $(n)_0 = 1$ para todo natural n.

A quantidade de arranjos simples de r elementos tomados de um conjunto de n elementos ($1 \leqslant r \leqslant n$) é dada pela definição recursiva (verifique):

$$(n)_r = \begin{cases} 1, & \text{se } r = 0 \\ n \cdot (n-1)_{r-1}, & \text{se } n \geqslant r \geqslant 1. \end{cases}$$

Por exemplo, de quantas maneiras podemos escolher um inteiro entre 000 e 999 (inclusive e com 3 dígitos) com todos os dígitos distintos? O conjunto tem 1.000 elementos e a quantidade deles sem dígitos repetidos é $(10)_3 = 10 \cdot 9 \cdot 8 = 720$.

Exercício 194. Sejam A e B conjuntos finitos com $|A| \leqslant |B|$. Há quantas funções injetivas de A em B?

Arranjo com repetição

Um arranjo em que é permitido repetição é chamado **arranjo com repetição**.

PROPOSIÇÃO 195 *A quantidade de arranjos com repetição de r elementos tomados de um conjunto de n elementos é n^r.*

DEMONSTRAÇÃO. Um arranjo com repetição de r elementos tomados do conjunto A pode ser identificado como uma sequência s de comprimento r de elementos de A

$$s\colon [r] \to A.$$

A quantidade de tais sequências é $\left| A^{[r]} \right| = |A|^r$ por (5.3). □

Retomando o paradoxo do aniversário (página 88), com que probabilidade ocorre que num grupo com 25 pessoas 2 ou mais pessoas façam aniversário no mesmo dia? Os aniversários de 25 pessoas pode ocorrer, pelo princípio multiplicativo, de 365^{25} modos diferentes. Os aniversários de 25 pessoas sem que nenhum deles coincida pode ocorrer de $(365)_{25}$ modos diferentes, portanto, há $365^{25} - (365)_{25}$ possibilidades diferentes para o aniversário de 25 pessoas com pelo menos duas aniversariando no mesmo dia. A probabilidade desse evento é

$$\frac{365^{25} - (365)_{25}}{365^{25}} = 1 - \frac{(365)_{25}}{365^{25}} > 0{,}56.$$

Quando é dito simplesmente **arranjo** entende-se arranjo simples.

Permutação

Um arranjo simples com $r = n$ é chamado **permutação**.

De quantas maneiras diferentes 8 alunos podem se sentar numa sala com 8 cadeiras? O primeiro aluno tem 8 opções, o segundo tem 7, o terceiro tem 6, o quarto tem 5, o quinto tem 4, o sexto tem 3, o sétimo tem 2 e para o oitavo resta 1 opção. Logo há $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 40320$ maneiras dos 8 alunos sentarem nas 8 cadeiras.

Uma permutação de elementos de um conjuntos A pode ser identificado com uma sequência dos elementos de A sem repetição. O número de permutações dos elementos de um conjunto de $n \geqslant 0$ elementos é $n!$, definido recursivamente para todo natural n por

$$n! = \begin{cases} 1, & \text{se } n = 0 \\ n(n-1)!, & \text{se } n \geqslant 1. \end{cases}$$

Exemplo 196. A quantidade de permutações que podem ser formadas com as letras da palavra *"livros"* é $6! = 720$. A quantidade de permutações que podem ser formadas com as letras da palavra *"teclado"* é $7! = 5.040$. A quantidade de permutações que podem ser formadas com as letras da palavra *"discreta"* é $8! = 40.320$. A quantidade de permutações que podem ser formadas com as letras da palavra *"universal"* é $9! = 362.880$. A quantidade de permutações que podem ser formadas com as letras da palavra *"pernambuco"* é $10! = 3.628.800$. A quantidade de permutações que podem ser formadas com as letras da palavra *"seminublado"* é $11! = 39.916.800$. A quantidade de permutações que podem ser formadas com as letras da palavra *"configuravel"* é $12! = 479.001.600$.

O fatorial de n cresce bastante rápido com n: $11!$ é mais que a quantidade de segundos de 1 ano inteiro; $12!$ é mais que a quantidade de segundos de 12 anos e $13!$ é mais que a quantidade de segundos que passam em 1.000 anos.

Exercício 197. Verifique que

$$(n)_r = \frac{n!}{(n-r)!}. \tag{5.4}$$

5.2.2 Combinação

Tomemos um arranjo de r elementos escolhidos de um conjunto com n elementos. A quantidade de arranjos *que têm os mesmos r elementos* é $r!$ pois a única diferença entre eles é a ordem com que se apresentam os r elementos. Por exemplo, se selecionamos sequencialmente e sem reposição 3 cartas de um baralho então temos $52 \cdot 51 \cdot 50$ arranjos distintos, um dos quais é $(K\heartsuit, 5\clubsuit, Q\diamondsuit)$. Agora, se selecionamos três cartas de uma só vez as $3!$ permutações de $(K\heartsuit, 5\clubsuit, Q\diamondsuit)$ correspondem a mesma seleção. A quantidade de seleções distintas é

$$\frac{52 \cdot 51 \cdots 50}{3!} = \frac{52!}{49!3!}.$$

Uma **combinação** de $r \geqslant 0$ elementos escolhidos de um conjunto A com $n \geqslant r$ elementos é uma seleção sem ordem e sem repetição de r elementos tomados de n ou, simplesmente, um subconjunto com r elementos de A.

PROPOSIÇÃO 198 *A quantidade de subconjuntos de A com r elementos, para $0 \leqslant r \leqslant n$, é*

$$\frac{n!}{r!(n-r)!}.$$

DEMONSTRAÇÃO. Dados um conjunto A de cardinalidade n e $0 \leqslant r \leqslant n$, seja $C(n,r)$ a quantidade de subconjuntos de A com cardinalidade r.

Um único subconjunto de tamanho r determina $r!$ arranjos de r elementos de A. Subconjuntos distintos determinam arranjos distintos, portanto, $C(n,r)\cdot r! = (n)_r$, ou seja, $C(n,r) = (n)_r / r!$. Usando (5.4)

$$C(n,r) = \frac{n!}{r!(n-r)!}.$$

□

O **coeficiente binomial** $\binom{n}{r}$ para todo $n \geqslant r \geqslant 0$ é dado por

$$\binom{n}{r} := \frac{n!}{r!(n-r)!}.$$

Convencionamos que $\binom{n}{r} = 0$ se $n < r$.

Em combinatória entendemos $\binom{n}{r}$ como a quantidade de subconjuntos de r elementos que podem ser formados a partir de um conjunto com n elementos.

Exemplo 199. A Mega-Sena é um jogo de apostas que consiste em acertar 6 dezenas escolhidas dentre 60. O número de possíveis resultados distinto para a Mega-Sena é $\binom{60}{6} = 50.063.860$. Se uma aposta em seis números demorar 1 segundo para ser registrada, então registrar 50.063.860 demoraria um ano e meio, aproximadamente. A probabilidade de acertar os seis números é

$$\frac{1}{\binom{60}{6}} = \frac{1}{50.063.860} \approx 2\times 10^{-8}.$$

A chance de morrer por raio no Brasil em 2010 era[3] $0{,}8\times 10^{-6}$ (40 vezes maior).

Exemplo 200. Numa população com n elementos, n_1 são azuis e $n_2 = n - n_1$ são verdes. De quantas maneiras podemos escolher k elementos com r deles azuis? ($0 \leqslant r \leqslant \min\{n_1, k\}$) O número de maneiras de escolher $k-r$ verdes é $\binom{n_2}{k-r}$. O número de maneiras de escolher r azuis é $\binom{n_1}{r}$. Pelo Princípio Multiplicativo, o número de maneiras de escolher r azuis e $k-r$ verdes é $\binom{n_2}{k-r}\binom{n_1}{r}$.

Exemplo 201. Três bolas são retiradas aleatoriamente de uma caixa com 6 bolas brancas e 5 bolas pretas. Com que probabilidade a escolha resulta em 1 branca e 2 pretas?

No total são 11 bolas das quais escolhemos 3. O número de possíveis resultados é $\binom{13}{3}$. "6 bolas brancas e 5 bolas pretas" ocorre de $\binom{6}{1}\binom{5}{2}$ modos diferentes, pelo exercício anterior. Portanto a probabilidade é $\frac{\binom{6}{1}\binom{5}{2}}{\binom{13}{3}}$.

Exercício 202. Prove que as seguintes identidades

$$\begin{aligned} \binom{n}{r} &= \binom{n}{n-r} \\ i\binom{n}{i} &= n\binom{n-1}{i-1}. \end{aligned} \tag{5.5}$$

Exercício 203. Verifique que o coeficiente binomial $\binom{n}{k}$ é uma solução para a equação de recorrência

$$C(n,k) := \begin{cases} 0 & \text{se } k > n \\ 1 & \text{se } k = n \text{ ou } k = 0 \\ C(n-1,k-1) + C(n-1,k) & \text{se } 0 < k < n. \end{cases}$$

(veja o exercício 25, página 72). Conclua que para $n > k > 0$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \tag{5.6}$$

e dê uma justificativa para essa igualdade usando a interpretação combinatória de $\binom{n}{k}$ (quantidade de subconjuntos).

[3] esse número é uma média no sentido de que considera que todos têm a mesma chance de ser atingido por um raio ao acaso, o que não é real.

Combinação com repetição

Se escolhemos uma peça de dominó ao acaso, com que probabilidade obtemos a peça [•|••] ?

As peças de dominós são formadas por dois números tomados dos números de 0 a 6 podendo haver repetição. Os dominós com pares de números diferentes são $\binom{7}{2} = 21$, mais os $\binom{7}{1} = 7$ pares repetidos resultam em $\binom{7}{2} + \binom{7}{1} = \binom{8}{2} = 28$ peças de dominós, portanto, são 28 combinações de 2 objetos tomados dentre 7 com repetição. Assim a probabilidade de ocorrer a peça [••|••] num sorteio é $1/28$.

Agora, vamos imaginar um dominó com três pontas, cada uma com um número de 0 a 6 de modo que em cada trio de números pode haver repetições e, ademais, cada trio aparece numa única peça na coleção de peças desse jogo.

Observação 204. Com os números 1, 3 e 4 poderíamos ter duas peças como na figura 5.7 abaixo, que são diferentes como podemos observar lendo-as no sentido horário a partir da mesma ponta. Entretanto consideramos apenas uma delas na coleção.

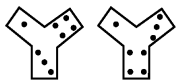


Figura 5.7: dominó de 3 pontas

São $\binom{7}{3}$ peças com três números distintos e $\binom{7}{1}$ peças com três números iguais. Para os outras peças temos $\binom{7}{2}$ modos de escolher dois números distintos e repetimos um deles para formar uma peça, logo são $2\binom{7}{2}$ peças. O total é de 84 peças. Observamos que da relação de Stifel, equação (5.6), podemos reorganizar a soma $\binom{7}{3} + 2\binom{7}{2} + \binom{7}{1}$ como

$$\left[\binom{7}{3} + \binom{7}{2}\right] + \left[\binom{7}{2} + \binom{7}{1}\right] = \binom{8}{3} + \binom{8}{2} = \binom{9}{3}.$$

Essa estratégia de contagem não é facilmente generalizável, o leitor pode tentar contar o número de peças de dominós de 5 pontas com 7 possíveis números diferentes para se convencer de que a quantidade de padrões de repetição dos números nas pontas das peças começa a fugir do controle.

Como vimos acima há $\binom{8}{2}$ dominós de duas pontas e $\binom{9}{3}$ dominós de três pontas. Ingenuamente podemos conjecturar que são $\binom{10}{4}$ de quatro pontas e $\binom{11}{5}$ de cinco pontas. Indo um pouco mais adiante, conjecturamos que são $\binom{7+p-1}{p}$ dominós de p pontas.

De fato, essa conjectura se verifica e uma estratégia alternativa de contagem mais simples que a usada acima é contar *quantas vezes podemos repetir cada um dos sete número de modo que a soma total das repetições é três.* Se x_i é quantas vezes o $i \in \{0,1,\ldots,6\}$ é repetido, temos $x_i \in \{0,1,2,3\}$ e devemos ter $x_0 + x_1 + \cdots + x_6 = 3$. Veremos a seguir como contar o número de soluções em $\mathbb{N}$ de tais equações.

Para o caso geral vale que dentre n objetos, se queremos selecionar r podendo haver repetição e sem considerar ordem, então isso pode ser feito de

$$\left(\!\binom{n}{r}\!\right) := \binom{n+r-1}{r} \tag{5.7}$$

maneiras diferentes.

No caso dos dominós, por exemplo, são 7 números dos quais selecionamos 2, podendo repetir número

$$\left(\!\binom{7}{2}\!\right) = \binom{7+2-1}{2} = \binom{8}{2} = \frac{8!}{6!2!} = 28.$$

Como dissemos acima, uma maneira de modelar combinação com repetição para deduzir equação (5.7) é escrever uma equação com uma indeterminada para cada um dos n objetos, $x_1, x_2, \ldots, x_n$. A variável x_i indica quantas vezes o i-ésimo objeto será selecionado, portanto $x_1 + x_2 + \cdots + x_n = r$. Assim, o número combinações com repetição é a quantidade de soluções inteiras de

$$x_1 + x_2 + x_3 + \cdots + x_n = r \text{ com } x_i \in \{0,1,2,\ldots\} \text{ para todo } i. \tag{5.8}$$

Soluções inteiras de equações lineares

Vamos começar com um caso simples, estudaremos o número de soluções de

$$x_1 + x_2 + x_3 = 6 \text{ com } x_i \in \{1,2,\ldots\} \text{ para todo } i. \tag{5.9}$$

Escrevemos

$$1+1+1+1+1+1=6$$

e uma solução da equação (5.9) corresponde a escolha de 2 operadores + dentre os 5 escritos na equação acima; por exemplo, se usamos $\oplus$ para representar as escolhas

$$\underbrace{1+1}_{x_1}\oplus\underbrace{1+1+1}_{x_2}\oplus\underbrace{1}_{x_3}=6$$

corresponde a $x_1=2$, $x_2=3$ e $x_3=1$, e

$$\underbrace{1+1}_{x_1}\oplus\underbrace{1+1}_{x_2}\oplus\underbrace{1+1}_{x_3}=6$$

corresponde a $x_1=2$, $x_2=2$ e $x_3=2$. Portanto essa equação tem $\binom{5}{2}$ soluções em $\mathbb{Z}^+$.

Agora, estudaremos o número de soluções de

$$x_1+x_2+x_3=6 \text{ com } x_i\in\{0,1,2,\ldots\} \text{ para todo } i.$$

Notemos que uma solução $(x_1,x_2,x_3)=(x,y,z)$ inteira e *positiva* da equação $x_1+x_2+x_3=6+3$ determina uma única solução inteira e *não-negativa* $(x-1,y-1,z-1)$ da equação $x_1+x_2+x_3=6$ e vice-versa, ou seja, as equações

$$\begin{aligned} x_1+x_2+x_3 &= 6+3 \quad \text{com } x_i\in\{1,2,3,\ldots\} \text{ para todo } i.\\ x_1+x_2+x_3 &= 6 \quad \text{com } x_i\in\{0,1,2,3,\ldots\} \text{ para todo } i. \end{aligned}$$

têm o mesmo número de soluções.

De volta ao problema que gerou essa discussão: o número de maneiras de selecionar r objetos, podendo haver repetição, dentre n objetos é igual ao número de soluções inteiras da equação (5.8), que é o mesmo número de soluções inteiras de

$$x_1+x_2+x_3+\cdots+x_n=n+r \text{ com } x_i\in\{1,2,\ldots\} \text{ para todo } i.$$

consideramos $1+1+1+\cdots+1=n+r$ e dos $n+r-1$ operadores + escolhemos $n-1$, ou seja, usando (5.5) são $\binom{n+r-1}{n-1}=\binom{n+r-1}{r}$ soluções inteiras.

Exercício 205. Escreva a partir das ideias acima uma demonstração para a afirmação de que o número de combinações com repetição é dada por (5.7).

Resumindo, a quantidade de maneiras diferentes de selecionarmos r elementos de um conjunto de n elementos é,

	sem repetição	com repetição
com ordem	$(n)_r=\frac{n!}{(n-r)!}$	n^r
sem ordem	$\binom{n}{r}=\frac{(n)_r}{r!}$	$\left(\!\binom{n}{r}\!\right)=\binom{n+r-1}{r}$

Bolas em caixas

Um outro modelo para problemas de contagem, além de contar soluções inteiras de equações, é considerar a distribuição de bolas em caixas. Consideramos os casos: *caixas distinguíveis* ou *caixas idênticas* e *bolas distinguíveis* ou *bolas idênticas*.

Por exemplo, há 8 modos de distribuir as bolas distinguíveis a,b,c em duas caixas distinguíveis, *esquerda* e *direita*

$$\begin{array}{cccc} abc| & ab|c & a|bc & |abc \\ ac|b & bc|a & b|ac & c|ab \end{array}$$

Se as caixas fossem idênticas, ou indistinguíveis, então $abc|$ e $|abc$ definem a mesma configuração, assim como $ac|b$ e $b|ac$, como $ab|c$ e $c|ab$, como $bc|a$ e $a|bc$. Não há ordem na disposição das bolas dentro da caixa. Portanto, há 4 modos de distribuir as bolas distinguíveis a,b,c em duas caixas indistinguíveis.

Se as bolas são idênticas, ou indistinguíveis, e as caixas não, são 4 modos

$$***| \qquad **|* \qquad *|** \qquad |***$$

Se caixas e bolas são indistinguíveis são 2 modos: $***|$ (ou, $|***$) e $**|*$ (ou, $*|**$).

Exemplo 206. De quantas maneiras distintas podemos distribuir 3 bolas distinguíveis em 4 caixas distinguíveis? Para cada uma das 3 bolas bola há 4 possíveis caixas, portanto temos um evento composto por uma sequência de 3 etapas em que cada um tem 4 possíveis resultados, portanto 4^3 maneiras distintas para distribuir as bolas nas caixas.

Exercício 207. De quantas maneiras podemos

1. distribuir r bolas distintas em n caixas distintas com qualquer número de bolas por caixa;
2. distribuir r bolas distintas em n caixas distintas com no máximo uma bola por caixa;
3. distribuir r bolas idênticas em n caixas distintas com no máximo uma bola por caixa;
4. distribuir r bolas idênticas em n caixas distintas com qualquer número de bolas por caixa.

O número de modos de distribuir n bolas distintas em n caixas idênticas é conhecido como número de Bell, do qual falaremos adiante.

Binômio de Newton

Se A é um conjunto com n elementos então a quantidade de subconjuntos de A de cardinalidade r é o número de maneiras distintas que podemos selecionar r elementos dentre os n do conjunto, isto é, são $\binom{n}{r}$ subconjuntos. Por outro lado, a bijeção que identifica subconjuntos de A com sequências binárias, exercício 3 na página 90 garante que há 2^n subconjuntos de A. Disso[4] concluímos que

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

Esse fato também é consequência de um resultado mais geral conhecido como Teorema Binomial.

TEOREMA 208 (TEOREMA BINOMIAL) *Para todo $n > 0$, vale*

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}.$$

Vejamos como o produto se desenvolve para valores pequenos de n. No caso $n = 2$ temos

$$\begin{aligned}(x+y)(x+y) &= (x+y)x + (x+y)y \\ &= xx + yx + xy + yy\end{aligned}$$

e multiplicado o resultado por $(x+y)$ obtemos o caso $n = 3$

$$\begin{aligned}(x+y)(x+y)(x+y) &= (x+y)(xx + yx + xy + yy) \\ &= (x+y)xx + (x+y)yx + (x+y)xy + (x+y)yy \\ &= xxx + yxx + xyx + yyx + xxy + yxy + xyy + yyy.\end{aligned}$$

Observemos que em ambos os casos temos uma soma monômios da forma $x^i y^j$ com $i + j = 3$ e as ocorrências das vaiáveis no monômio não repete cor. Isso porque na aplicação da propriedade distributiva cada um dos n termos $(x+y)$ contribui com uma das variáveis, x ou y. O caso $n = 4$

$$\begin{aligned}&(x+y)(x+y)(x+y)(x+y) \\ &\quad = (x+y)(xxx + yxx + xyx + yyx + xxy + yxy + xyy + yyy) \\ &\quad = xxxx + xyxx + xxyx + xyyx + xxxy + xyxy + xxyy + xyyy \\ &+ yxxx + yyxx + yxyx + yyyx + yxxy + yyxy + yxyy + yyyy\end{aligned}$$

DEMONSTRAÇÃO. Como $(x+y)^n =$

$$\underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ vezes}}; \tag{5.10}$$

desenvolvendo o produto usando a propriedade distributiva temos que cada variável de cada termo $(x+y)$ do produto será multiplicada por umá variável de cada outro termo do produto, de modo que o resultado é uma soma em que cada parcela é um monômio da forma $x^r y^{n-r}$, para $0 \leqslant r \leqslant n$ e precisamos determinar quantas vezes cada monômio ocorre nesse desenvolvimento.

Para cada r, o coeficiente de $x^r y^{n-r}$ é o número de maneiras de escolher o x de r fatores $(x+y)$ da equação (5.10); os $n-r$ fatores restantes contribuem com o y. O número de maneiras de escolher r fatores dentre n é $\binom{n}{r}$, portanto

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}$$

como queríamos. □

[4] Alguns textos denominam essa estratégia de demonstração de uma igualdade de **contagem dupla**: contando a quantidade de elementos de um conjunto de dois modos distintos os resultados devem ser iguais.

Exercício 209. Escreva uma prova do teorema binomial usando indução.

Exercício 210. Verifique se vale a igualdade

$$\sum_{r=0}^{n}\binom{n}{r}x^r y^{n-r} = \sum_{r=0}^{n}\binom{n}{r}x^{n-r}y^r.$$

A relação de Stifel (5.6) nos dá um algoritmo para encontrar os coeficientes do polinômio. Dispomos esses coeficientes num arranjo triangular cuja n-ésima linha são os coeficientes de $(x+y)^n$, chamado **triângulo de Pascal**:

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
\qquad
\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}$$

O 1 é o primeiro e o último número de cada linha. Os outros números é a soma dos outros dois logo acima a esquerda e acima a direita:

$$\begin{array}{ccccc}
\cdots & \binom{n-1}{k-1} & \binom{n-1}{k} & \cdots & \\
\cdots & \binom{n}{k} & \cdots & &
\end{array}$$

Vejamos um exemplo de aplicação do teorema binomial na prova de uma igualdade. Por um lado temos que

$$(1+x)^{2n} = \sum_{m=0}^{2n}\binom{2n}{m}x^m.$$

Por outro lado, temos que $(1+x)^n(1+x)^n$ é o produto

$$\left(\sum_{k=0}^{n}\binom{n}{k}x^k\right)\cdot\left(\sum_{\ell=0}^{n}\binom{n}{\ell}x^\ell\right) = \sum_{k=0}^{n}\sum_{\ell=0}^{n}\binom{n}{k}\binom{n}{\ell}x^{k+\ell} = \sum_{m=0}^{n}\left(\sum_{j=0}^{m}\binom{n}{j}\binom{n}{m-j}\right)x^m$$

e como $(1+x)^{2n} = (1+x)^n(1+x)^n$ os coeficientes dos dois polinômios devem ser iguais na mesma potência de x, ou seja, temos essa bela identidade

$$\binom{2n}{m} = \sum_{j=0}^{m}\binom{n}{j}\binom{n}{m-j}.$$

Exemplo 211. Se A, B e C são três subconjuntos de $X = \{1,2,\ldots,n\}$. Vamos contar o número de ternas (A,B,C) com $A\cap B\subset C$.

Primeiro, fixamos o conjunto $C\in S$ e o conjunto $A\in S$. Digamos que C tem cardinalidade c e $A\setminus C$ tem cardinalidade a, com $0\leqslant c\leqslant n$ e $0\leqslant a\leqslant n-c$. O número de possíveis $B\in S$ tais que $A\cap B\subset C$ é contado da seguinte maneira: para que $A\cap B$ seja subconjunto de C o conjunto B não pode ter elementos de $A\setminus C$, caso contrário teríamos $x\in A\cap B$ e $x\notin C$. Qualquer outro elemento de X pode estar em B logo temos 2^{n-a} possibilidades em S para o conjunto B.

Deixemos C fixado e vamos contar quantos $A\in S$ são possíveis com a elementos em $A\setminus C$. Um conjunto A com a elementos em $A\setminus C$ é formado por elementos de um subconjunto de a elementos escolhidos em $n-c$, ou seja $\binom{n-c}{a}$ possibilidades para $A\setminus C$ aos quais unimos um dos 2^c subconjuntos de C para formar A, pelo princípio multiplicativo são $2^{n-a}\binom{n-c}{a}2^c$ possibilidades para formar A. Assim o número de pares (A,B) cuja interseção está contida em C (fixo) é

$$\sum_{a=0}^{n-c}2^{n-a}\binom{n-c}{a}2^c = 2^c2^c\sum_{a=0}^{n-c}\binom{n-c}{a}2^{n-c-a} = 4^c(1+2)^{n-c} = 4^c3^{n-c} \tag{5.11}$$

na segunda igualdade usamos o teorema binomial.

Da equação (5.11) acima, são $4^c 3^{n-c}$ pares (A,B) cuja interseção está contida em qualquer $C \in S$ cuja cardinalidade é c. A quantidade de tais C é $\binom{n}{c}$, portanto, o número de ternas $(A,B,C) \in S \times S \times S$ tais que $A \cap B \subset C$ é

$$\sum_{c=0}^{n} \binom{n}{c} 4^c 3^{n-c} = (4+3)^n \tag{5.12}$$

novamente, na equação (5.12) usamos o teorema binomial para concluir o resultado. Portanto $|\{(A,B,C) \in S \times S \times S : A \cap B \subset C\}| = 7^n$.

Exercício 212. Escreva um equação de recorrência para resolver o problema do exercício anterior. Verifique usando indução que 7^n é uma solução.

5.2.3 Relações de equivalência e contagem

Uma permutação qualquer das letras de uma dada palavra é chamada de *anagrama* dessa palavra, mesmo que esta permutação não tenha sentido. Por exemplo, "lodo" é um anagrama de "dolo", bem como "odol" e "dool".

Quantos anagramas podem ser formados com as letras da palavra "ana"? Sabemos que são 3! permutações de 3 símbolos distintos, mas nesse caso há permutações que dão origem ao mesmo anagrama. As seis permutações de ana são:

ana ana aan aan naa naa

em cada duas permutações a palavra é a mesma, só muda (a cor) a ordem da letra repetida, portanto são

$$\frac{3!}{2} = 3$$

permutações distintas, ou 3 anagramas.

Exemplo 213. Quantos anagramas podem ser formados com as letras da palavra *"dado"*?

Da mesma maneira, diferenciamos artificialmente as letras iguais e olhamos para todas as sequências formadas por tais letras. O número de arranjos de quatro letras tomadas de $\{d_1, a, d_2, o\}$ é 4!; no entanto para cada arranjo há um único outro que dá origem ao mesmo anagrama, as saber o que troca as posições das duas letras "d" e deixa as outras letras na mesma posição. Desse modo cada anagrama é contado duas vezes, ou seja, são

$$\frac{4!}{2} = 12$$

anagramas distintos (veja a figura 5.8 abaixo).

(a,d_1,d_2,o) (a,d_2,d_1,o)	(o,d_1,d_2,a) (o,d_2,d_1,a)	(d_1,d_2,a,o) (d_2,d_1,a,o)	(d_1,a,d_2,o) (d_2,a,d_1,o)
(a,d_1,o,d_2) (a,d_2,o,d_1)	(o,a,d_1,d_2) (o,a,d_2,d_1)	(d_1,a,o,d_2) (d_2,a,o,d_1)	(d_1,d_2,o,a) (d_2,d_1,o,a)
(a,o,d_1,d_2) (a,o,d_2,d_1)	(o,d_1,a,d_2) (o,d_2,a,d_1)	(d_1,o,a,d_2) (d_2,o,a,d_1)	(d_1,o,d_2,a) (d_2,o,d_1,a)

Figura 5.8: anagramas de "dado"com os "d"'s diferenciados.

Temos quatro letras na palavra mas menos do 4! anagramas pois temos letras "d" repetidas. Distinguimos essas letras usando índices, d_1 e d_2, e assim temos o conjunto das letras $\{d_1, a, d_2, o\}$. Seja A o conjunto das permutações destas quatro letras

$$A = \{(x_1,x_2,x_3,x_4) : x_i \in \{d_1,a,d_2,o\} \text{ e } x_i \neq x_j \text{ sempre que } i \neq j,\ \forall i,j \in \{1,\ldots,4\}\}.$$

Definimos a relação binária $\backsim$ em A pondo $(x_1,x_2,x_3,x_4) \backsim (y_1,y_2,y_3,y_4)$ se, e só se, para cada $i \in \{1,\ldots,4\}$ vale que

$$x_i = y_i \text{ ou}$$
$$x_i, y_i \in \{d_1, d_2\}$$

isto é, duas permutações equivalentes de elementos de A têm o d_1 possivelmente trocado por d_2 e as demais letras nas mesmas posições. Por exemplo, $(d_1,a,o,d_2) \sim (d_2,a,o,d_1)$ e $(a,o,d_1,d_2) \backsim (a,o,d_2,d_1)$, enquanto que $(d_1,a,o,d_2) \not\backsim (a,o,d_1,d_2)$.

Os doze subconjuntos formados das permutações equivalentes entre si são representados na figura 5.8 acima, os doze quadros correspondem aos doze anagramas da palavra "dado" considerando as letras "d" como "diferentes". Cada um dos quadros é o que chamamos de classe de equivalência da relação de equivalência.

Exemplo 214. Um modo de contar quantos subconjuntos de cardinalidade r tem um conjunto de cardinalidade n é considerar o conjunto A dos arranjos simples de r elementos. Dados dois arranjos $\alpha, \beta \in A$ dizemos que eles são equivalentes se eles diferem apenas na ordem dos elementos, os elementos em si são os mesmos. Se α e β são equivalentes, escrevemos $\alpha \sim \beta$ que é uma relação de equivalência sobre A (verifique). Como α e β têm os mesmos elementos, α é uma permutação de β, assim a classe de equivalência $[\alpha]_\sim$ tem $r!$ elementos. Toda classe de equivalência tem $r!$ elementos, pelo mesmo argumento. Notemos que há tantos subconjuntos de cardinalidade r de um conjunto de cardinalidade n quantos são os elementos de $A/\sim$, o conjunto das classes de equivalência de $\sim$ sobre A. Lembremos o teorema 123, página 62, que diz que o conjunto quociente $A/\sim$, formado pelas classes de equivalência da relação $\sim$ sobre A, é uma partição de A de modo que $|A/\sim| \cdot r! = |A|$ pelo princípio aditivo. Finalmente, $|A/\sim|$, a quantidade de subconjuntos de cardinalidade r de um conjunto de cardinalidade n é

$$\frac{|A|}{r!} = \frac{(n)_r}{r!}.$$

É frequente precisar determinar a cardinalidade das classes de equivalência e do conjunto quociente nas aplicações.

Teorema 215 *Se A é finito e $\sim$ é uma relação de equivalência sobre A cujas classes de equivalência têm a mesma cardinalidade, digamos $k = |[a]_\sim|$, então*

$$\left|A/\sim\right| = \frac{|A|}{k}.$$

Demonstração. Se A é finito, então de (4.2), da proposição 119 (página 62) e do princípio aditivo temos

$$|A| = \sum_{[a]_\sim \in A/\sim} |[a]_\sim|.$$

Se ainda tivermos todos as classes de equivalência de mesma cardinalidade k então $|A| = k \cdot |A/\sim|$, donde segue o teorema. □

No exemplo dos anagramas de "dado", A é o conjunto de todas as permutações e cada classe de equivalência tem dois anagramas obtido um do outro pela permutação das duas letras "d", portanto, o quantidade de anagramas distintos sem diferenciar as letras "d" é $\left|A/\backsim\right| = 4!/2 = 12$.

Exemplo 216. Quantos anagramas podem ser formados com as letras da palavra *"banana"*? Como há letras repetidas vamos diferenciá-las usando cores. Como no caso de "dado", temos permutações que são diferentes quando diferenciamos as letras iguais, mas que não diferem na ordem, isto é, definem o mesmo anagrama. Por exemplo:

banana banana banana banana

são permutações diferentes que determinam o mesmo anagrama. As 3! permutações das letras a no mesmo anagrama são indistinguíveis, assim como as 2! da letras n, portanto, há $3! \cdot 2! = 12$ permutações em cada classe de equivalência, quando consideramos equivalentes dois anagramas com a mesma sequência de letras. Vejamos as dez classes de equivalência das permutações que começam com a letra "b"

banana	banana	banana	banana	banana	banana
banana	banana	banana	banana	banana	banana
banaan	banaan	banaan	banaan	banaan	banaan
banaan	banaan	banaan	banaan	banaan	banaan
baanna	baanna	baanna	baanna	baanna	baanna
baanna	baanna	baanna	baanna	baanna	baanna
baanan	baanan	baanan	baanan	baanan	baanan
baanan	baanan	baanan	baanan	baanan	baanan
bannaa	bannaa	bannaa	bannaa	bannaa	bannaa
bannaa	bannaa	bannaa	bannaa	bannaa	bannaa
bnaana	bnaana	bnaana	bnaana	bnaana	bnaana
bnaana	bnaana	bnaana	bnaana	bnaana	bnaana
bnaaan	bnaaan	bnaaan	bnaaan	bnaaan	bnaaan
bnaaan	bnaaan	bnaaan	bnaaan	bnaaan	bnaaan
bnanaa	bnanaa	bnanaa	bnanaa	bnanaa	bnanaa
bnanaa	bnanaa	bnanaa	bnanaa	bnanaa	bnanaa
bnnaaa	bnnaaa	bnnaaa	bnnaaa	bnnaaa	bnnaaa
bnnaaa	bnnaaa	bnnaaa	bnnaaa	bnnaaa	bnnaaa
baaann	baaann	baaann	baaann	baaann	baaann
baaann	baaann	baaann	baaann	baaann	baaann

A palavra tem 6 letras portanto são 6! = 720 permutações se considerarmos as letras distintamente e pelo teorema 215 o número de anagramas é 720/12 = 60.

Exemplo 217. Na relação binária sobre $\mathbb{R}$ dada por $x \sim y$ se, e só se, $x - y \in \mathbb{Z}$ não há $(x, y) \in [0,1) \times [0,1)$ com $x \neq y$ na relação $\sim$. Então a função $f\colon [0,1) \to \mathbb{R}/\sim$ dada por $f(x) = [x]_\sim$ é injetiva e, portanto, $\mathfrak{c} \leq \left|\mathbb{R}/\sim\right|$. Por outro lado, $\left|\mathbb{R}/\sim\right| \leq |\mathbb{R}| = \mathfrak{c}$, logo $\left|\mathbb{R}/\sim\right| = \mathfrak{c}$. Finalmente, se $x \in \mathbb{R}$, então $[x]_\sim = \{y \in \mathbb{R}\colon x - y \in \mathbb{Z}\} = \{z + x\colon z \in \mathbb{Z}\}$, portanto, $|[x]_\sim| = |\mathbb{Z}| = \aleph_0$, para todo $x \in \mathbb{R}$.

Permutação com repetição

De quantos modos podemos arranjar n objetos se esses são de r tipos diferentes e o no arranjo o objeto do tipo i ocorre k_i vezes para todo $i \in \{1, \ldots, r\}$, sendo que $k_1 + \cdots + k_r = n$?

Defina A como o conjunto das sequências de objetos $(o_1, o_2, \ldots, o_n)$ de acordo com as restrições do parágrafo anterior e com os objetos do mesmo tipo diferenciados por algum artifício, por exemplo, colorindo ou indexando os objetos. Agora, tome em A a relação de equivalência definida por $(o_1, o_2, \ldots, o_n) \backsim (p_1, p_2, \ldots, p_n)$ se, e só se, para todo $i \in \{1, \ldots, n\}$ os objetos o_i e p_i são do mesmo tipo.

Fixada uma sequência $(o_1, o_2, \ldots, o_n)$ de A, se permutamos os objetos do tipo i, porém preservando as posições relativas na sequência, obtemos uma sequência $(p_1, p_2, \ldots, p_n)$ equivalente a original pela relação $\backsim$. São $k_i!$ sequências $(p_1, p_2, \ldots, p_n)$ equivalentes a $(o_1, o_2, \ldots, o_n)$ quando só se permuta os objetos do tipo i. O número total de permutações que só mudam a posição entre objetos de mesmo tipo é $\prod_{i=1}^{r} k_i!$. O número de permutações distintas com repetição é dado pelo teorema 215.

Proposição 218 *Em n objetos no total, com r tipos diferentes de objetos e k_i objetos do tipo i, sujeitos a $1 \leqslant i \leqslant r$ e $n = k_1 + \cdots + k_r$, a quantidade de permutações de n objetos com repetição é dado pelo* ***coeficiente multinomial***

$$\binom{n}{k_1,\ k_2, \ldots,\ k_r} = \frac{n!}{k_1! k_2! \cdots k_r!}$$

Exemplo 219 (**mãos de bridge**). Numa mão de Bridge as 52 cartas de um baralho embaralhado são divididas igualmente entre 4 jogadores. O número de modos distintos com que isso é feito pode ser calculado da seguinte forma: uma distribuição de cartas corresponde a uma sequência de 52 objetos, os 13 primeiros objetos da sequência são as cartas do primeiro jogador, os 13 seguintes do segundo jogador, os próximos 13 do terceiro e os 13 últimos objetos da sequência são as cartas do quarto jogador. Há 52! sequências distintas de cartas. Entretanto, dessas 52! temos que, para cada jogador, 13! permutações correspondem a mesma sequência de cartas em sua mão, portanto, são

$$\binom{52}{13, 13, 13, 13} = 53.644.737.765.488.792.839.237.440.000$$

modos distintos de distribuir as cartas, ou mãos diferentes de início de jogo.

Com raciocínio análogo ao feito para o Teorema Binomial,

$$(x + y + z)^n = \sum_{\substack{k_1,\ k_2,\ k_3 \in \mathbb{N} \\ k_1 + k_2 + k_3 = n}} \binom{n}{r_1, r_2, r_3} x^{r_1} y^{r_2} z^{r_3}.$$

Exercício 220. Se numa mão de Bridge as 52 cartas de um baralho são divididas igualmente e aleatoriamente entre 4 jogadores. Com que probabilidade cada jogador recebe um ás?

Solução. Os 4 ases podem ser distribuídos de 4! modos distintos entregando um para cada jogador. As 48 cartas restantes são distribuídas pelos jogadores de $\binom{48}{12,12,12,12}$ maneiras distintas. Pelo princípio multiplicativo são $4!\binom{48}{12,12,12,12}$ modos distintos de os jogadores receberem um ás cada. Portanto a probabilidade é

$$\frac{4!\binom{48}{12,12,12,12}}{\binom{52}{13,13,13,13}}$$

que vale aproximadamente 0,0044. □

Exercício 221. Quantos são os anagramas formados com as letras da palavra *"matemática"*?

Exercício 222. Um sinal é composto por nove bandeiras alinhadas. Quantos sinais diferentes é possível formar quando há disponíveis 4 bandeiras brancas, três bandeiras vermelhas e duas bandeiras azuis? Bandeiras da mesma cor são idênticas.

Exercício 223. Formule o problema de contar o número de combinações usando relação de equivalência.

Permutação circular

De quantos modos 5 crianças, denominadas a, b, c, d, e podem formar uma roda de ciranda? Em fila, seriam 5! filas diferentes, entretanto, numa roda há vários arranjos que descrevem a mesma configuração circular, por exemplo, as rodas $abcde$, $eabcd$ e $deabc$ são iguais pois importa apenas a posição relativa das crianças. Assim, cada roda tem 5 descrições equivalentes dependendo do primeiro elemento da descrição, logo a resposta correta é $5!/5 = 4! = 24$.

PROPOSIÇÃO 224 *O número de permutações circulares de $n \geqslant 1$ objetos distintos é igual a*

$$\frac{n!}{n}$$

DEMONSTRAÇÃO. Exercício. □

Número de funções sobrejetivas

Sejam A, B dois conjuntos com cardinalidades m e n, respectivamente. Vimos que o número de funções $f\colon A \to B$ é n^m e que o número de funções injetivas é $(n)_m$. Quantas são as funções sobrejetivas $f\colon A \to B$? Essa pergunta só é interessante se $m \geqslant n \geqslant 1$.

Tome uma enumeração qualquer de B, digamos que $B = \{b_0, b_2, \ldots, b_{n-1}\}$. Denote, para cada $i \in [n]$, por A_i o conjunto da funções f de A em B tais que $b_i \notin \operatorname{Im}(f)$. O conjunto da funções sobrejetivas é

$$S = B^A \setminus \bigcup_{i=0}^{n-1} A_i.$$

Sabemos que $|B^A| = n^m$. Usando inclusão–exclusão, exercício 27, página 107,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{I\subseteq[n]} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right|$$

e $\bigcap_{i\in I} A_i$ é o conjunto das funções de A em B que deixam $\{b_i\colon i \in I\}$ de fora da imagem, logo para todo $I \neq \varnothing$

$$\left|\bigcap_{i\in I} A_i\right| = (n - |I|)^m$$

portanto

$$\begin{aligned}
|S| &= n^m - \sum_{\varnothing\neq I\subseteq[n]} (-1)^{|I|+1} (n - |I|)^m \\
&= n^m - \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} (n-i)^m \\
&= n^m + \sum_{i=1}^{n} (-1)^{i} \binom{n}{i} (n-i)^m \\
&= \sum_{i=0}^{n} (-1)^{i} \binom{n}{i} (n-i)^m
\end{aligned}$$

Número de partições

Se $f\colon A \to B$ é sobrejetiva e $|A| = m$ e $|B| = n$, então para cada $y \in B$ a pré-imagem $f^{-1}(y) \subseteq A$ é um subconjunto não vazio de modo que $\{f^{-1}(y)\colon y \in B\}$ é uma partição de A em n partes.

No conjunto de todas as funções sobrejetivas de A em B definimos uma relação de equivalência pondo para quaisquer funções f, g desse conjunto $f \equiv g$ se, e só se, elas definem a mesma partição de A, isto é, $\{f^{-1}(y)\colon y \in B\} = \{g^{-1}(y)\colon y \in B\}$.

Ainda, $\left|[f]_{\equiv}\right| = n!$ pois se $\mathscr{A}$ é uma partição de A em n partes então existem $n!$ bijeções $F\colon \mathscr{A} \to B$ e cada bijeção F define uma sobrejeção $f\colon A \to B$, portanto, são $n!$ sobrejeções que definem a mesma partição $\mathscr{A}$.

Definição 225. A quantidade de maneiras de particionar um conjunto de cardinalidade m em n partes é conhecida como **número de Stirling do segundo tipo** e é denotada por $\left\{{m \atop n}\right\}$ ou $S(m, n)$. Convencionamos que $\left\{{0 \atop 0}\right\} = 1$.

Pela definição acima e a discussão no parágrafo que a precede, usando o teorema 215 concluímos que o número de funções sobrejetoras é $n!\left\{{m \atop n}\right\}$, portanto

$$\left\{{m \atop n}\right\} = \frac{1}{n!} \sum_{i=0}^{n} (-1)^{i} \binom{n}{i} (n-i)^m. \tag{5.13}$$

Exercício 226. Justifique a seguinte equação de recorrência. Tome $\left\{ {n \atop 0} \right\} = \left\{ {0 \atop n} \right\} = 0$ e para $n > 0$ e todo m, vale que

$$\left\{ {m+1 \atop n} \right\} = \left\{ {m \atop n-1} \right\} + n \left\{ {m \atop n} \right\}. \tag{5.14}$$

Definição 227. O número de partições de um conjunto de cardinalidade m é

$$B_m = \sum_{n=0}^{m} \left\{ {m \atop n} \right\}$$

para todo $m \in \mathbb{N}$, chamado de m-ésimo **número de Bell**.

Exercícios

1. Quantos elementos há em $A_1 \cup A_2$ se $|A_1| = 12$, $|A_2| = 18$ e

   (a) A_1 e A_2 são disjuntos;

   (b) $|A_1 \cap A_2| = 6$;

   (c) $A_1 \subseteq A_2$.

2. Uma pesquisa revela que 96% das residência têm pelo menos um aparelho de TV; 98% em telefone e 95% das residências têm pelo menos uma TV e telefone. Qual a porcentagem de residências que não tem nem TV nem telefone?

3. Quantos naturais menores ou iguais a 100 são divisíveis por 5 ou por 7?

4. Quantos naturais menores ou iguais a 100 são ímpares ou quadrado de um inteiro?

5. Quantas sequências de 8 bits não contém seis zeros consecutivos?

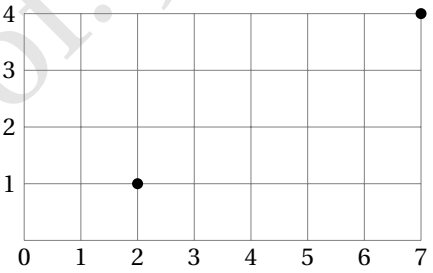
6. Uma sala tem 6 portas. De quantas maneiras é possível entrar e sair dessa sala? De quantas formas é possível entrar e sair da sala por portas distintas?

7. De quantas maneiras diferentes podemos distribuir seis brinquedos diferentes para três crianças de modo que cada uma receba pelo menos um brinquedo?

8. Quantos inteiros entre 10000 e 100000 existem cujos dígitos são somente 6, 7 ou 8? E quantos são os inteiros cujos dígitos são somente 0, 6, 7 ou 8?

9. Quantos inteiros entre 1000 e 9999 (inclusive) existem com todos os dígitos distintos? Desses quantos são ímpares? Desses quantos são pares?

10. Na figura abaixo, de quantas maneiras pode-se caminhar do ponto $(2,1)$ até o ponto $(7,4)$ se cada passo só pode ser para a direita ou para cima (ou seja, a partir do ponto (i, j) só se chega, em um passo, ao $(i+1, j)$ ou ao $(i, j+1)$)?



    De quantas maneiras pode-se caminhar do ponto $(0,0)$ até o ponto $(7,4)$? De quantas maneiras pode-se caminhar do ponto $(0,0)$ até o ponto $(7,4)$ passando pelo ponto $(2,1)$?

11. Prove que para quaisquer inteiros positivos n e k, se $n \geqslant 2k$ então a fração $n!/2^k$ resulta num inteiro.

12. Numa estante temos 13 livros: 6 de cálculo, 3 de geometria analítica e 4 de física básica. De quantas maneiras é possível ordenar os livros se:

(a) Não colocarmos nenhuma restrição.

(b) Se pedirmos para que os livros de cálculo sejam colocados primeiro, depois os de geometria analítica e por fim os de física básica.

(c) Se pedirmos para que os livros do mesmo assunto fiquem juntos.

(d) Considerando agora os 3 livros de cálculo são iguais, responda novamente cada um dos três itens anteriores.

13. Defina o domínio (nos naturais) das variáveis n e r para os quais valem as identidades e prove as identidades abaixo.

(a) $(n+1)_r = \frac{n+1}{n+1-r}(n)_r$.

(b) $\binom{n}{r} = \binom{n}{n-r}$.

(c) $n\binom{m+n}{m} = (m+1)\binom{m+n}{m+1}$.

14. Para jogar uma partida de futebol 22 crianças dividem-se em dois times de 11 cada. Quantas divisões diferentes são possíveis?

15. Um *byte* é uma sequência de 8 *bits*. Quantos *bytes* contém

(a) exatamente dois 1's;

(b) exatamente quatro 1's;

(c) exatamente seis 1's;

(d) pelo menos seis 1's.

16. Em uma caixa há 100 bolas enumeradas de 1 a 100. Cinco bolas são escolhidas ao acaso. Qual a probabilidade de que os números correspondentes as cinco bolas escolhidas sejam consecutivos?

17. Temos 20 mil reais que devem ser aplicados entre 4 carteiras diferentes. Cada aplicação deve ser feita em múltiplos de mil reais e os investimentos mínimos que podem ser feitos são de 2,2,3 e 4 mil reais. Quantas estratégias de aplicação diferentes existem se

(a) uma aplicação tiver que ser feita em cada carteira?

(b) aplicações tiverem que ser feitas em pelo menos 3 das quatro carteiras?

18. Formule os seguintes problemas em termos de soluções inteiras de equações.

(a) O número de maneiras de distribuir r bolas idênticas em n caixas distintas com pelo menos k bolas na primeira caixa.

(b) O número de maneiras de distribuir r bolas idênticas em n caixas distintas com nenhuma caixa com mais de duas bolas.

(c) O número de subconjuntos de $\{A, B, C, D, E\}$ com 3 elementos.

(d) O número de maneiras de distribuir r bolas idênticas em n caixas distintas tal que as duas primeiras caixas tenham juntas p bolas.

19. Formule os seguintes problemas em termos de soluções inteiras de equações e distribuição de bolas em caixas.

(a) Seleção de seis sorvetes a partir de 31 sabores

(b) Seleção de cinco camisas de um grupo de cinco vermelhas, quatro azuis e duas amarelas.

(c) Seleção de 12 cervejas de 4 tipos com pelo menos duas de cada tipo.

(d) Seleção de 20 refrigerantes de 4 tipos com número par de cada tipo e não mais que oito do mesmo tipo.

20. De quantas maneiras podemos dispor 8 peças brancas idênticas e 8 peças pretas idênticas num tabuleiro de xadrez (8×8)? Quantas são simétricas (a disposição ficará a mesma quando rotacionamos o tabuleiro de 180 graus)?

21. Sejam k, n, p números naturais com p primo.

(a) prove que $p|\binom{p}{k}$, sempre que $k < p$;

(b) prove que $p|\binom{n}{k}$ se, e somente se, $p|\lfloor n/p \rfloor$.

22. Quantas são as funções $f\colon [n] \to [n]$ não decrescentes, isto é, tais que se $i < j$ então $f(i) \leqslant f(j)$? (Dica: $x_0 = f(1), x(i) = f(i+1) - f(i), x_n = n - f(n)$, reformule em termos de soluções inteiras de equações lineares.)

23. Quantas soluções tem $x_1 + x_2 + x_3 = 13$ com $0 \leqslant x_i < 6$ para todo i?

24. Para que valores de n as equações

$$x_1 + x_2 + \cdots + x_{19} = n$$
$$y_1 + y_2 + \cdots + y_{64} = n$$

têm o mesmo número de soluções inteiras positivas?

25. Sejam n e m inteiros positivos, $m \geqslant n$. Prove que o número de maneiras de distribuir m bolas idênticas em n caixas distinguíveis sem que alguma caixa fique vazia é

$$\binom{m-1}{n-1}.$$

Prove que se cada caixa tiver que receber pelo menos r objetos, quando $m \geqslant rn$, então são

$$\binom{m-1+(1-r)n}{n-1}.$$

maneiras.

26. (**identidade de Vandermonde**) Prove

$$\binom{n+m}{k} = \sum_{r=0}^{k} \binom{m}{k-r}\binom{n}{r}.$$

27. (**Princípio de Inclusão–Exclusão**) Prove o caso geral do princípio de Inclusão–Exclusão

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{I\subseteq[n]} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right|.$$

28. Determine o número de primos menores que 200 usando o princípio de inclusão–exclusão.

29. Uma permutação dos números $[n]$ é dita **permutação caótica** se todos os números estão fora de suas posições originais. Por exemplo, para $n = 4$, a permutação 2413 é caótica, mas a permutação 2431 não é, pois o número 3 está na terceira posição. Quantas permutações caóticas há num conjunto com sete elementos?

30. Quantas permutações caóticas de $1,2,3,4,5,6$ começam com $1,2,3$ em qualquer ordem?

31. Prove que o número de permutações caóticas de $n \geqslant 1$ elementos é

$$D_n = n!\left(\frac{1}{0!} - \frac{1}{1!} + \cdots + \frac{(-1)^n}{n!}\right).$$

32. Use o teorema binomial para provar as identidades abaixo.

(a) $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

(b) $\sum_{k=0}^{n} (-1)^k k \binom{n}{k} = 0$.

(c) $\sum_{k=0}^{n} k(k-1)\binom{n}{k} = n(n-1)2^{n-2}$.

33. Prove a seguinte relação entre coeficientes binomiais e os números de Fibonacci

$$\sum_{k=0}^{\lfloor n/2\rfloor} \binom{n-k}{k} = F_{n+1}.$$

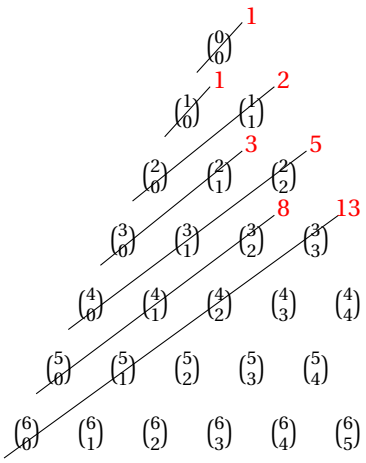


Figura 5.9: triângulo de Pascal e números de Fibonacci.

34. Prove que
$$\binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3}\cdots\binom{n-k_1-k_2-\cdots-k_{r-1}}{k_r} = \frac{n!}{k_1!k_2!\cdots k_r!}$$
para os valores de $n, k_1, \ldots, k_r$ nos quais os coeficientes binomiais estão definidos.

35. Prove que para todo $n \geqslant 1$
$$(x+y+z)^n = \sum_{\substack{k_1,\,k_2,\,k_3\in\mathbb{N}\\ k_1+k_2+k_3=n}} \binom{n}{k_1,\,k_2,\,k_3} x^{k_1} y^{k_2} z^{k_3}.$$

36. Prove o **teorema multinomial** de Leibniz: Para todo $n > 0$, vale
$$(x_1+x_2+\cdots+x_k)^n = \sum_{\substack{r_1,\ldots,r_k\in\mathbb{N}\\ r_1+r_2+\cdots+r_k=n}} \binom{n}{r_1, r_2, \ldots, r_k} x_1^{r_1} x_2^{r_2}\cdots x_k^{r_k}.$$

37. A soma dos números na diagonal do triângulo de Pascal é igual ao número abaixo do último somando. Por exemplo, $1+1=2$, $1+2=3$, $1+2+3=6$, $1+3=4$, $1+3+6=10$, etc.

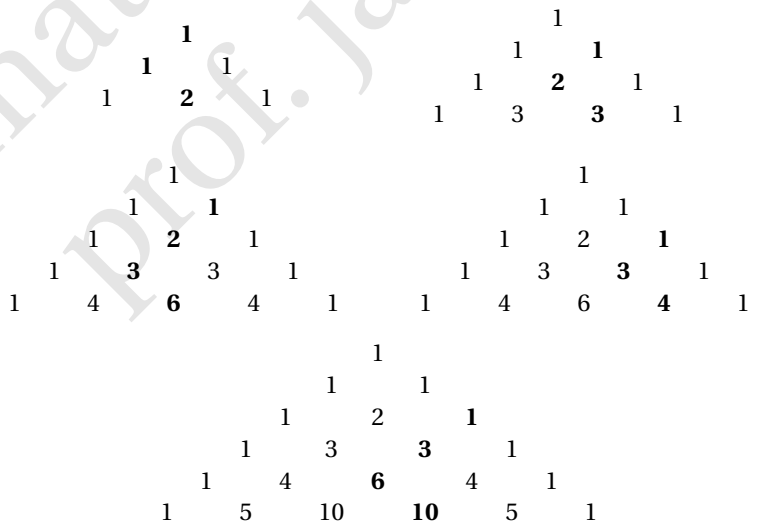


Figura 5.10: somas nas diagonais no triângulo de Pascal.

Use indução e a relação de Stifel para mostrar que

$$\sum_{i=0}^{k}\binom{n+i}{n}=\binom{n+k+1}{k+1}.$$

38. Uma caixa tem um número desconhecido de bolas idênticas, que denotamos por n e queremos estimá-lo. Para tal, selecionamos aleatoriamente n_1 bolas, cada uma recebe uma marca e é devolvida para a caixa.

    (a) De quantas maneiras podemos extrair r bolas de modo que k estarão marcadas?

    (b) Qual é o número de seleções de r bolas.

    (c) Defina o índice de acerto por $p_k(n)=\dfrac{\text{resultado do item (a)}}{\text{resultado do item (b)}}$.

    Mostre que $p_k(n)$ é

    i. crescente para os valores de n tais que $p_k(n)>p_k(n-1)$,

    ii. decrescente para os valores de n tais que $p_k(n)<p_k(n-1)$.

    Conclua que $\lfloor n_1 r/k\rfloor$ é ponto de máximo de $p_k(n)$. Qual é uma boa estimativa para n?

39. Dê uma demonstração combinatória (sem usar a recorrência (5.14) e sem usar (5.13)) para $\left\{{m \atop 2}\right\}=2^m-2$.

40. Justifique a seguinte equação de recorrência

$$B_{m+1}=\sum_{k=0}^{m}\binom{m}{k}B_k$$

    com $B_0=1$ (da convenção assumida na definição 225 temos que $B_0=1$).

41. De quantas maneiras podemos distribuir n bolas distintas em n caixas idênticas?

Complemento: Aproximação de Stirling e limitantes para coeficiente binomial

A fórmula de Stirling é uma boa aproximação para o fatorial. Uma primeira aproximação é dada por aproximação de uma soma por uma integral

$$\int_{k-1}^{k}\ln(x)\,\mathrm{d}x<\ln k<\int_{k}^{k+1}\ln(x)\,\mathrm{d}x$$

e de

$$\ln(n!)=\ln\left(\prod_{i=1}^{n}i\right)=\sum_{i=1}^{n}\ln(i)$$

de onde deduzimos que

$$\int_{0}^{n}\ln(x)\,\mathrm{d}x<\ln(n!)<\int_{1}^{n+1}\ln(x)\,\mathrm{d}x$$

ou seja,

$$n\ln(n)-n<\ln(n!)<(n+1)\ln(n+1)-n$$

A fórmula de Stirling, mais apurada, é assintótica. Duas sequências de números a_n e b_n são *assintoticamente iguais* e escrevemos $a_n\sim b_n$, se

$$\lim_{n\to\infty}\frac{a_n}{b_n}=1.$$

Frequentemente, é muito útil quanto trabalhamos com fatoriais a seguinte igualdade assintótica conhecida como fórmula de Stirling

$$n!\sim\left(\frac{n}{\mathrm{e}}\right)^n\sqrt{2\pi n}$$

n	$n!$	stirling	$\exp(n\ln n - n + 1)$
1	1	0.922137	1
2	2	1.919004	1.471517764685769
3	6	5.83621	3.654052647388543
7	5040	4980.396	2041.359003828341
10	3628800	3598696	1234098.0408668
20	$2.432902e+18$	$2.422787e+18$	$5.874957877287052e+17$
50	$3.041409e+64$	$3.036345e+64$	$4.656617903154618e+63$
75	$2.480914e+109$	$2.478159e+109$	$3.103152318837849e+100$
100	$9.332622e+157$	$9.324848e+157$	$1.01122149261047e+157$
142	$2.695364e+245$	$2.693783e+245$	$2.451449516100687e+244$

também valem os limitantes

$$\sqrt{2\pi n}\Big(\frac{n}{\mathrm{e}}\Big)^n \leqslant n! \leqslant \mathrm{e}\sqrt{n}\Big(\frac{n}{\mathrm{e}}\Big)^n$$

O coeficiente binomial tem os seguintes limitantes triviais

$$0 \leqslant \binom{n}{k} \leqslant 2^n.$$

Para um limitante inferior melhor podemos escrever

$$\binom{n}{k} = \prod_{j=0}^{k-1} \frac{n-j}{k-j} \geqslant \Big(\frac{n}{k}\Big)^k$$

e para um limitante superior usamos o teorema binomial de Newton e de $\mathrm{e}^x \geqslant (1+x)$

$$\mathrm{e}^{nx} \geqslant (1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i \geqslant \binom{n}{i} x^i$$

para todo $x > 0$ e todo $i \in \{0, 1, \ldots, n\}$. Logo

$$\binom{n}{i} \leqslant \mathrm{e}^{nx} x^{-i}.$$

Em particular, fazendo $x = i/n$, temos a segunda desigualdade de

$$\Big(\frac{n}{i}\Big)^i \leqslant \binom{n}{i} \leqslant \Big(\mathrm{e}\frac{n}{i}\Big)^i.$$

5.3 Funções geradoras

De quantas maneiras distintas podemos lançar uma dado quatro vezes de modo que os resultados somam 14?

O resultado do primeiro lançamento é representado por um polinômio da seguinte forma

$$x^1 + x^2 + x^3 + x^4 + x^5 + x^6 \tag{5.15}$$

O símbolo x aqui é chamado de *indeterminada*, o que significa que não é uma variável que assume valores em algum domínio, seu único papel é codificar uma enumeração e, neste papel, contém duas informações: (1) as potências de x representam as diferentes faces dos dados; (2) os coeficientes das potências de x, nesse caso todos 1, representam o número de ocorrências de cada face. Se as faces do dado fossem 1,2,2,2,5,5 então o polinômio seria

$$x^1 + 3x^2 + 2x^5. \tag{5.16}$$

Se o segundo lançamento é codificado pelo mesmo polinômio, então o produto é, pela regra de multiplicação de polinômios,

$$\begin{aligned}(x^1 + x^2 + x^3 + x^4 + x^5 + x^6)(x^1 + x^2 + x^3 + x^4 + x^5 + x^6) = \\ x^{12} + 2x^{11} + 3x^{10} + 4x^9 + 5x^8 + 6x^7 + 5x^6 + 4x^5 + 3x^4 + 2x^3 + x^2\end{aligned} \tag{5.17}$$

e nesse polinômio ax^k significa que há a maneiras de obtermos a soma k. O coeficiente a é o número de soluções de $i + j = k$ com $i, j \in \{1, \ldots, 6\}$. Por exemplo, só há uma maneira de obtermos 12, é como $6+6$, há 0 modos de obtermos soma 0 ou soma maior que 12, há 3 maneiras de obter soma 4 (a saber $1+3$, $2+2$ e $3+1$).

Exemplo 228 (dados de Sicherman). Um dado com faces 1, 2, 2, 3, 3, 4 e outro com faces 1, 3, 4, 5, 6, 8 quando são lançados tem as frequências das soma dadas por

$$(x^1+2x^2+2x^3+x^4)(x^1+x^3+x^4+x^5+x^6+x^8) = \\ x^{12}+2x^{11}+3x^{10}+4x^9+5x^8+6x^7+5x^6+4x^5+3x^4+2x^3+x^2$$

que é a mesma dos dados regulares (5.17).

Para três lançamentos usamos a expansão do polinômio ao (5.15) cubo para ter as quantidades de soluções de $i+j+k=m$ com $i,j,k \in \{1,\ldots,6\}$ e todo $m \in \mathbb{N}$. A resposta está codificada em

$$(x^1+x^2+x^3+x^4+x^5+x^6)^3 = x^{18}+3x^{17}+6x^{16}+10x^{15}+15x^{14}+21x^{13}+25x^{12}+27x^{11}+27x^{10}+25x^9+21x^8+15x^7+10x^6+6x^5 \\ +3x^4+x^3.$$

Para responder a pergunta inicial, precisamos conhecer o coeficiente de x^{14} na quarta potência de (5.15)

$$(x^1+x^2+x^3+x^4+x^5+x^6)^4 = x^{24}+4x^{23}+10x^{22}+20x^{21}+35x^{20}+56x^{19}+80x^{18}+104x^{17}+125x^{16}+140x^{15}+146x^{14}+140x^{13} \\ +125x^{12}+104x^{11}+80x^{10}+56x^9+35x^8+20x^7+10x^6+4x^5+x^4$$

portanto há 146 maneiras diferentes de obter a soma 14.

No exemplo do dado com faces 1,2,2,2,5,5 as somas de 4 lançamentos são dadas pela quarta potência do polinômio (5.16)

$$(x^1+3x^2+2x^5)^4 = 16x^{20}+96x^{17}+32x^{16}+216x^{14}+144x^{13}+24x^{12}+216x^{11}+216x^{10}+72x^9+89x^8+108x^7+54x^6+12x^5+x^4$$

portanto há 216 maneiras diferentes de obter a soma 14.

Exemplo 229. Um pai generoso deseja dividir R$20,00 entre seus três filhos de modo que cada um receba pelo menos R$5,00 e ninguém receba mais que R$10,00 e a quantia do filho mais velho é par. De quantas maneiras ele pode fazer essa divisão?

O filho mais velho recebe um valor de $\{6,8,10\}$ e os outros filhos de $\{5,6,7,8,9,10\}$, portanto, procuramos pelo coeficiente de x^{20} no polinômio

$$(x^6+x^8+x^{10})(x^5+x^6+x^7+x^8+x^9+x^{10})(x^5+x^6+x^7+x^8+x^9+x^{10}) = \\ x^{30}+2x^{29}+4x^{28}+6x^{27}+9x^{26}+12x^{25}+13x^{24}+14x^{23}+13x^{22}+12x^{21}+9x^{20}+6x^{19}+4x^{18}+2x^{17}+x^{16}.$$

Portanto, são 9 maneiras de realizar a divisão.

Exercício 230. Quantas soluções inteiras tem $x_1+x_2+x_3=11$ com $x_1 \in \{1,2,3\}$ e $x_2,x_3 \in \{4,5\}$?

Solução. O coeficiente de x^{11} em $(x^1+x^2+x^3)(x^4+x^5)(x^4+x^5)$. □

5.3.1 Série formal de potências

Imagine um país no qual há apenas três valores de moedas: 1 centavo, 2 centavos e 4 centavos. De quantas maneiras podemos formar 10.000 centavos?

Precisamos resolver a equação $a+2b+4c=10000$ para números inteiros não-negativos a,b,c. Os possíveis valores para a são codificados pelo "polinômio"

$$1+x+x^2+\cdots$$

os possíveis valores para b são codificados por

$$1+x^2+x^4+\cdots$$

e os possíveis valores para b são codificados por

$$1+x^4+x^8+\cdots$$

Agora, procuramos o coeficiente de x^{10000} no "polinômio"

$$P(x) = (1+x+x^2+\cdots)\cdot(1+x^2+x^4+\cdots)\cdot(1+x^4+x^8+\cdots)$$

Podemos multiplicar os termos e com alguma perseverança eventualmente encontramos o coeficiente de x^{10000}. Mas agora precisamos buscar um modo mais pragmático para essa tarefa.

Se $(a_0, a_1, a_2, \ldots)$ é uma sequência de números reais a **função geradora ordinária** $A(x)$ dessa sequência é dada pela série formal de potências

$$A(x) = \sum_{n \geqslant 0} a_n x^n \tag{5.18}$$

O **coeficiente** a_n de x^n é dado por

$$[x^n]A(x).$$

Duas séries formais de potências são iguais se, e só se, têm os mesmos coeficientes. Em nossas aplicações (contagem) os coeficientes da série (5.18) são inteiros, porém todas as propriedades discutidas são válidas para números complexos ou mesmo para coeficientes tomados de um anel comutativo com unidade.

A função geradora é dita *ordinária* para diferenciar de outros tipos de funções geradoras e a série é dita *formal* porque é definida como um conceito algébrico e não analítico.

Observação 231. No estudo analítico de séries de potências o x é uma variável que pode assumir valores reais (ou complexos) e as séries $\sum_n a_n x^n$ podem assumir um valor real (ou complexo), pois o somatório com infinitos termos é um limite de somas finitas parciais e tal limite pode existir ou não existir (que inclui ser $\pm\infty$). Quando o tal limite existe dizemos que a série **converge**. Damos mais detalhes adiante.

No caso formal não podemos atribuir valores a x porque não é uma variável, é um marcador de posição, de modo que $2x^n$, por exemplo, expressa o fato de que 2 é o n-ésimo termo de uma sequência. A expressão (5.18) *representa* a sequência $(a_n)_n$ de números reais. O conjunto de todas tais sequência com a soma e o produto dados por

$$(a_n)_n + (b_n)_n = (a_n + b_n)_n$$
$$(a_n)_n \cdot (b_n)_n = \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_n$$

forma um anel comutativo com unidade $(1,0,0,\ldots)$ que representamos pela série formal 1. Definindo, em séries formais, a soma e o produto que sejam compatíveis com a definição acima (veja tabela 5.1 na página 114) o conjunto das séries formais de potências munido dessas duas operações forma um anel comutativo com unidade.

Se os coeficientes a_n são não nulos apenas para um número finito de índices n então a série formal de potências é um polinômio pois *adotamos a convenção de que somar zeros infinitamente não tem efeito.* Por exemplo,

- o polinômio 1 é função geradora da sequência $(1,0,,0,0,\ldots)$,
- o polinômio $1-x$ é função geradora da sequência $(1,-1,0,0,\ldots)$ e
- $1+x+x^2+\cdots+x^n$ da sequência $(1,1,\ldots,1,0,0,\ldots)$.

Da definição de produto $(1-x)(1+x+x^2+\cdots+x^n) = 1-x^{n+1}$, o que escrevemos como

$$\frac{1-x^{n+1}}{1-x} = 1+x+x^2+\cdots+x^n$$

que é função geradora da sequência $(1,1,\ldots,1,0,0,0\ldots)$ com $n+1$ ocorrências de 1 e o restante é 0 (verifique). Também segue da definição de produto, usando indução em n, que

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{n}x^n$$

é função geradora da sequência $(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}, 0, 0, \ldots)$.

Da definição da multiplicação de séries formais temos $(1-x)(1+x+x^2+x^3+\cdots) = 1$ o que escrevemos como

$$\frac{1}{1-x} = 1+x+x^2+x^3+\cdots \tag{5.19}$$

que é a função geradora da sequência constante $(1,1,1,\ldots)$ e da multiplicação obtemos $(1-ax)\left(\sum_{n\geqslant 0} a^n x^n\right) = 1$ o que escrevemos como

$$\frac{1}{1-ax} = \sum_{n\geqslant 0} a^n x^n$$

que é a função geradora da sequência $(1, a, a^2, \ldots)$.

O **recíproco** da série formal $A(x) = \sum_{n\geqslant 0} a_n x^n$ é a série formal $B(x)$ tal que $A(x)\cdot B(x) = 1$. Quando existe, o recíproco é único e denotado por $\frac{1}{A(x)}$.

Em $\left(\sum_{n\geqslant 0} a_n x^n\right)\left(\sum_{n\geqslant 0} b_n x^n\right) = 1$, o termo independente é $a_0 b_0 = 1$, de modo que para haver recíproco de $A(x) = \sum_{n\geqslant 0} a_n x^n$ é necessário que $a_0 \neq 0$, pois só assim a_0 tem inverso multiplicativo em $\mathbb{R}$. Essa condição também é suficiente.

Exercício 232. Prove que, para $A(x) = \sum_{n\geqslant 0} a_n x^n$, se $a_0 \neq 0$ então $\frac{1}{A(x)}$ tem coeficientes dados por

$$b_0 = \frac{1}{a_0}$$
$$b_n = -b_0 \sum_{i=1}^{n} a_i b_{n-i}, \text{ para } n \geqslant 1.$$

Se $(a_0, a_1, \ldots)$ tem função geradora $A(x)$ então $x^k A(x)$ é função geradora de $(0,0,\ldots,0,a_0,a_1,\ldots)$ com k ocorrências de 0 no início da sequência. Em particular, $(0,0,0,1,1,1,1,\ldots)$ tem a função geradora

$$\frac{x^3}{1-x} = x^3 + x^4 + x^5 + \cdots.$$

No caso do produto de séries formais os coeficientes $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ dependem de um número finito de coeficientes $a_0,\ldots,a_n$ e $b_0,\ldots,b_n$. Agora, se $A_0, A_1, \ldots$ são série formais então $A_0(x) + A_1(x) + \cdots$ fará sentido se para cada potência n existe uma cota m tal que os n primeiros coeficientes de $A_i(x)$ é 0 para todo $i > m$, pois cada coeficiente resultante será a soma de um número finito de coeficientes não nulos. Pela mesma razão, a substituição (composição)

$$A(B(x)) = \sum_{n\geqslant 0} a_n (B(x))^n$$

está definida sempre que $b_0 = 0$, para que os coeficientes de $A(B(x))$ dependam de apenas um número finito de termos. Fixado um k natural, na expansão de

$$(b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots)^n$$

ocorre a potência x^k para todo $n \geqslant 1$ de modo que quando tomamos expandirmos $\sum_{n\geqslant 0} a_n (b_1 x + b_2 x^2 + b_3 x^3 + \cdots)^n$ haverá infinitas contribuições para o coeficiente de x^k que, portanto, não está determinado (a menos de convergência, que não consideramos em séries formais). Se $b_0 = 0$ temos

$$\begin{aligned} A(B(x)) &= \sum_{n\geqslant 0} a_n (B(x))^n \\ &= \sum_{n\geqslant 0} a_n (b_1 x + b_2 x^2 + b_3 x^3 + \cdots)^n \\ &= \sum_{n\geqslant 0} a_n (x(b_1 + b_2 x^2 + \cdots))^n \\ &= \sum_{n\geqslant 0} a_n x^n (b_1 + b_2 x^2 + \cdots)^n \end{aligned}$$

de modo que quando $n > k$ não haverá contribuições de $x^n(b_1 + b_2 x^2 + \cdots)^n$ para o coeficiente de x^k. Em particular,

$$A(bx^k) = \sum_{n\geqslant 0} a_n (bx^k)^n = \sum_{n\geqslant 0} a_n b^n x^{nk}.$$

Por exemplo, de $\frac{1}{1-x}$ função geradora da sequência $(1,1,\ldots)$ deduz-se que $\frac{1}{1-x^2}$ é função geradora da sequência $(1,0,1,0,1,0,\ldots)$ e que $\frac{1}{1+x} = \frac{1}{1-(-x)}$ é função geradora da sequência $(1,-1,1,-1,\ldots)$, de modo que

$$\frac{1}{1-x} + \frac{1}{1+x} = \frac{2}{1-x^2}$$

é função geradora da sequência $(2,0,2,0,2,\ldots)$.

Operações

Existem muitas operações com séries formais de potência o que as torna aplicável numa ampla variedade de problemas de contagem. Aqui definimos algumas delas. Sejam $A(x) = \sum_{n\geqslant 0} a_n x^n$ e $B(x) = \sum_{n\geqslant 0} b_n x^n$ funções geradoras, definimos:

soma	$A(x)+B(x)=\sum_{n\geqslant 0}(a_n+b_n)x^n$
produto	$A(x)B(x)=\sum_{n\geqslant 0}\left(\sum_{k=0}^{n}a_k b_{n-k}\right)x^n$
deslocamento a direita	$xA(x)=\sum_{n\geqslant 1}a_{n-1}x^n$
deslocamento a esquerda	$\frac{A(x)-a_0}{x}=\sum_{n\geqslant 0}a_{n+1}x^n$
diferenciação	$\frac{\mathrm{d}}{\mathrm{d}x}A(x)=\sum_{n\geqslant 0}(n+1)a_{n+1}x^n$
somas parciais	$\frac{A(x)}{1-x}=\sum_{n\geqslant 0}\left(\sum_{k=0}^{n}a_k\right)x^n$

Tabela 5.1: operações com séries formais de potências.

Função geradora da sequência de Fibonacci

A sequência de Fibonacci $(F_0,F_1,F_2,\ldots)$ é definida recursivamente por $F_0=0, F_1=1$ e $F_n=F_{n-1}+F_{n-2}$ para todo $n\geqslant 2$. Olhando de outro modo

$$0, F_0+1, F_1+F_0, F_2+F_1, F_3+F_2$$

é obtida da soma das três sequências

$$\begin{array}{cccccccc} 0, & 1\,, & 0\,, & 0\,, & 0\,, & 0, & \ldots \\ 0, & F_0, & F_1, & F_2, & F_3, & F_4, & \ldots \\ 0, & 0\,, & F_0, & F_1, & F_2, & F_3, & \ldots \end{array}$$

cujas funções geradoras são, respectivamente, x, $xF(x)$ e $x^2F(x)$, onde $F(x)=\sum_{n\geqslant 0}F_n x^n$ é a função geradora da sequência de Fibonacci. Logo $F(x)=x+xF(x)+x^2F(x)$ donde concluímos, resolvendo para $F(x)$, que

$$F(x)=\frac{x}{1-x-x^2}.$$

Notemos que $1-x-x^2=(1-\varphi x)(1-\bar{\varphi}x)$, onde $\varphi=(1+\sqrt{5})/2$ e onde $\bar{\varphi}=(1-\sqrt{5})/2$ são as raízes de $1-x-x^2$. Fazendo

$$\frac{x}{(1-\varphi x)(1-\bar{\varphi}x)}=\frac{A}{1-\varphi x}+\frac{B}{1-\bar{\varphi}x}$$

pois no lado direito sabemos escrever as séries de potências usando substituição em (5.19), resolvemos para A e para B e obtemos que $A=1/\sqrt{5}$ e $B=11/\sqrt{5}$ de modo que

$$\frac{x}{1-x-x^2}=\frac{1}{\sqrt{5}}\cdot\frac{1}{1-\varphi x}-\frac{1}{\sqrt{5}}\cdot\frac{1}{1-\bar{\varphi}x}.$$

Agora

$$\frac{1}{1-\varphi x}=\sum_{n\geqslant 0}(\varphi x)^n$$

e

$$\frac{1}{1-\bar{\varphi}x}=\sum_{n\geqslant 0}(\bar{\varphi}x)^n$$

portanto

$$\frac{x}{1-x-x^2}=\sum_{n\geqslant 0}\frac{1}{\sqrt{5}}(\varphi^n-\bar{\varphi}^n)x^n$$

de modo que os coeficientes F_n são, para todo n, dados por

$$[x^n]\frac{x}{1-x-x^2}=\frac{1}{\sqrt{5}}(\varphi^n-\bar{\varphi}^n)$$

como, aliás, já sabíamos desde o exemplo 101 na página 51.

5.3.2 Expansão de funções de geradoras

Dada uma *forma funcional* para uma função geradora, gostaríamos de um mecanismo para encontrar a sequência associada. Esse processo é chamado de *expandir* a função geradora. Muitas funções são facilmente manipuladas a partir do teorema de Taylor–Maclaurin

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \cdots = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!}x^n$$

de modo que

$$[x^n]f(x) = \frac{1}{n!}f^{(n)}(0)$$

sempre que diferenciação for possível.

Também, obtemos coeficientes por manipulações algébricas envolvendo as identidades básicas que já são conhecidas e transformações dadas nas tabelas acima. Por exemplo

$$[x^n]\frac{c}{1-bx} = cb^n$$

para quaisquer constantes b e c, pois de (5.19) temos

$$\frac{c}{1-bx} = c\sum_{n\geqslant 0}(bx)^n.$$

Exemplo 233. Consideremos o problema dos dados enunciado no início dessa seção: *De quantas maneiras distintas podemos lançar uma dado quatro vezes de modo que os resultados somam 14?* A função geradora é

$$\begin{aligned} D(x) &= (x+x^2+x^3+x^4+x^5+x^6)^4 \\ &= x^4(1+x^2+x^3+x^4+x^5)^4 \\ &= x^4\left(\frac{1-x^6}{1-x}\right)^4 \\ &= x^4\left(1-x^6\right)^4(1-x)^{-4} \end{aligned}$$

de modo que $[x^{14}]D(x) = [x^{10}]\left(1-x^6\right)^4(1-x)^{-4}$. Ainda,

$$\left(1-x^6\right)^4 = \sum_{j\geqslant 0}\binom{4}{j}(-x^6)^j = 1-4x^6+6x^{12}-4x^{18}+x^{24}$$

$$(1-x)^{-4} = \sum_{j\geqslant 0}\binom{4+j-1}{j}x^j = \sum_{j\geqslant 0}\binom{3+j}{j}x^j$$

Agora, $[x^{10}]\left(1-x^6\right)^4(1-x)^{-4}$ pode ser obtido de $[x^0]\left(1-x^6\right)^4 = 1$ e $[x^{10}](1-x)^{-4} = \binom{13}{10} = 286$ e ser obtido de $[x^6]\left(1-x^6\right)^4 = -4$ e $[x^4](1-x)^{-4} = \binom{7}{4} = 35$, logo temos $286 - 140 = 146$ modos distintos.

Exemplo 234. O coeficiente de $[x^{15}](x^2+x^3+x^4+\cdots)^4$:

$$[x^{15}](x^2+x^3+x^4+\cdots)^4 = [x^{15}]\left(x^2(1+x+x^3+\cdots)\right)^4$$

$$= [x^{15}]\left(\frac{x^2}{1-x}\right)^4 = [x^{15}]\left(\frac{x^8}{(1-x)^4}\right) = [x^7]\left(\frac{1}{(1-x)^4}\right)$$

e

$$\frac{1}{(1-x)^4} = \sum_{r\geqslant 0}\binom{-4}{r}(-x)^r = \sum_{r\geqslant 0}\binom{4+r-1}{r}x^r$$

portanto $[x^{15}](x^2+x^3+x^4+\cdots)^4 = \binom{4+7-1}{7}$.

Exemplo 235. *Quantos subconjuntos de* $\{1,2,\ldots,15\}$ *formado de 4 elementos não consecutivos existem?* Se $\{a,b,c,d\}$ é um tal subconjunto de modo que

$$1 \leqslant a < b < c < d \leqslant 15$$

então

$$\underbrace{(15-d)}_{x_1} + \underbrace{(d-c)}_{x_2} + \underbrace{(c-b)}_{x_3} + \underbrace{(b-a)}_{x_4} + \underbrace{(a-1)}_{x_5} = 14$$

portanto, queremos o número de soluções inteiras de

$$x_1 + x_2 + x_3 + x_4 + x_5 = 15$$

com $x_1, x_5 \geqslant 0$ e $x_2, x_3, x_4 \geqslant 2$, o qual é o coeficiente

$$[x^{14}](1+x+x^2+\cdots)^2(x^2+x^3+x^4+\cdots)^3 = [x^{14}]x^6(1-x)^{-5} = [x^8](1-x)^{-5} = \binom{5+8-1}{8} = 495.$$

Exemplo 236. De quantos modos podemos comprar n frutas de modo que (1) o número de maçãs é par, (2) o número de bananas é múltiplo de 5, (3) no máximo 4 laranjas, e (4) no máximo uma pêra.

$$f(x) = \frac{1}{1-x^2} \cdot \frac{1}{1-x^5} \cdot \frac{1-x^5}{1-x} \cdot (1+x)$$

$[x^n]f(x) = n+1$.

Frações parciais No caso de funções racionais podemos usar a técnica da frações parciais, por exemplo

$$\frac{x}{1-x-x^2} = \frac{x}{(1-\varphi x)(1-\bar{\varphi}x)}$$

onde $\varphi = (1+\sqrt{5})/2$ e onde $\bar{\varphi} = (1-\sqrt{5})/2$ são as raízes de $1-x-x^2$. Fazendo

$$\frac{x}{(1-\varphi x)(1-\bar{\varphi}x)} = \frac{A}{1-\varphi x} + \frac{B}{1-\bar{\varphi}x}$$

temos $A = 1/\sqrt{5}$ e $B = 11/\sqrt{5}$ de modo que

$$\frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}}\frac{1}{1-\varphi x} - \frac{1}{\sqrt{5}}\frac{1}{1-\bar{\varphi}x}$$

Agora

$$\frac{1}{\sqrt{5}}\frac{1}{1-\varphi x} = \frac{1}{\sqrt{5}}\sum_{n\geqslant 0}(\varphi x)^n$$

e

$$\frac{1}{\sqrt{5}}\frac{1}{1-\bar{\varphi}x} = \frac{1}{\sqrt{5}}\sum_{n\geqslant 0}(\bar{\varphi} x)^n$$

portanto $\frac{x}{1-x-x^2} = \sum_{n\geqslant 0}\frac{1}{\sqrt{5}}(\varphi^n - \bar{\varphi}^n)x^n$ de modo que

$$[x^n]\frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}}(\varphi^n - \bar{\varphi}^n)$$

Exemplo 237. O coeficiente de x^n na série de potências de

$$\frac{1}{x^3 - 7x^2 + 16x - 12}$$

Primeiro, temos que

$$x^3 - 7x^2 + 16x - 12 = (x-3)(x-2)^2$$

portanto devemos determinar constantes A, B, C tais que

$$\frac{1}{x^3 - 7x^2 + 16x - 12} = \frac{A}{x-3} + \frac{B}{x-2} + \frac{C}{(x-2)^2}$$

e temos que $A = 1$ e $B = C = -1$, logo

$$\frac{1}{x^3 - 7x^2 + 16x - 12} = \frac{1}{x-3} - \frac{1}{x-2} - \frac{1}{(x-2)^2}$$

Agora, reescrevemos cada fração para cairmos no caso $\frac{1}{1-ax}$

$$\frac{1}{x-3} = \frac{1}{-3(1-x/3)} = -\frac{1}{3}\frac{1}{1-x/3}$$

$$\frac{1}{x-2} = \frac{1}{-2(1-x/2)} = -\frac{1}{2}\frac{1}{1-x/2}$$

e no caso $\frac{1}{(1-ax)^2}$

$$\frac{1}{(x-2)^2} = \frac{-1}{4}\frac{1}{(1-x/2)^2}$$

logo

$$\begin{aligned}\frac{1}{x^3-7x^2+16x-12} &= -\frac{1}{3}\frac{1}{(1-\frac{x}{3})} + \frac{1}{2}\frac{1}{(1-\frac{x}{2})} + \frac{1}{4}\frac{1}{(1-x/2)^2} \\ &= -\frac{1}{3}\sum_{n\geqslant 0}\left(\frac{x}{3}\right)^n + \frac{1}{2}\sum_{n\geqslant 0}\left(\frac{x}{2}\right)^n + \frac{1}{4}\sum_{n\geqslant 0}\binom{-2}{n}\left(\frac{-x}{2}\right)^n \\ &= \sum_{n\geqslant 0}\left(\left(\frac{1}{2}\right)^{n+1} - \left(\frac{1}{3}\right)^{n+1} + \frac{1}{4}(-1)^n\binom{-2}{n}\right)x^n \\ &= \sum_{n\geqslant 0}\left(\left(\frac{1}{2}\right)^{n+1} - \left(\frac{1}{3}\right)^{n+1} + \frac{1}{4}(-1)^n\binom{n+3}{n}\right)x^n\end{aligned}$$

portanto

$$[x^n]\frac{1}{x^3-7x^2+16x-12} = \frac{1}{2^{n+1}} - \frac{1}{3^{n+1}} + \frac{(n+3)(n+2)(n+1)}{24}.$$

O número de funções sobrejetivas

Seja $S(n,k)$ o número de funções sobrejetivas $[n] \to [k]$ e dividir esse número em duas classes: a primeira é formada por aquelas onde a restrição da função a $[n-1]$ ainda teremos uma função sobrejetiva. Há $kS(n-1,k)$ delas. Por outro lado, se após restringir a $[n-1]$ a função não é mais sobrejetiva, então existem $kS(n-1,k-1)$ destas, porque para ter tal função escolhemos um elemento em $[k]$ que tem n mapeado para ele e, em seguida, uma função sobrejetiva de $[n-1]$ para os $k-1$ elementos restantes. Assim, temos a relação de recorrência:

$$S(n,k) = kS(n-1,k) + kS(n-1,k-1).$$

Escrevamos $A_k(x) = \sum_{n\geqslant 0} S(n,k)x^n$. Multiplicando a relação de recorrência por x^n e somando todos os n nos dá a relação

$$A_k(x) = \frac{kx}{1-kx}A_{k-1}(x).$$

Também temos $A_0(x) = 1$ porque o único termo diferente de zero em A_0 é $S(0,0)x^0$. Portanto, temos uma fórmula explícita para esta função geradora

$$A_k(x) = \frac{k!X^k}{(1-x)(1-2x)\cdots(1-kx)}.$$

Agora, se dividirmos essa fração usando frações parciais em uma soma da forma

$$\sum_{j=1}^{k}\frac{a_j}{1-jx}$$

nós encontramos

$$a_j = \frac{(-1)^{k-j}}{j!(k-j)!}.$$

Usando o fato de que $(1-jx)^{-1} = 1 + jx + j^2x^2 + \cdots$ e que $S(n,k)$ é por definição o coeficiente de x^n nesta série de potências, temos isso

$$S(n,k) = \sum_{j=1}^{k}\frac{(-1)^{k-j}k!j^n}{j!(k-j)!}.$$

Por exemplo, $S(n,3) = 3(3^{n-1} - 2^n + 1)$ de modo que $S(12,3) = 519156$.

Exercícios

1. Determine uma expressão para a função geradora de cada sequência

(a) $(2,2,2,2,2,2)$;
(b) $(0,2,2,2,2,2,2,\ldots)$;
(c) $(0,1,0,0,1,0,0,1,0,0,1,\ldots)$;
(d) $(2,4,8,16,32,64,\ldots)$;
(e) $(0,0,1,2,3,4,\ldots,)$
(f) $(a_n\colon n\in\mathbb{N})$ dada por $a_n = 5$;
(g) $(a_n\colon n\in\mathbb{N})$ dada por $a_n = 3^n$;
(h) $(a_n\colon n\in\mathbb{N})$ dada por $a_n = \binom{8}{n}$.

2. Que sequência é gerada pelas seguintes funções

(a) $(3x-4)^3$
(b) $(x^3+1)^3$
(c) $1/(1-2x^2)$
(d) $x^2/(1-x)^3$

3. Encontre $[x^{10}]$ em

(a) $(1+x^5+x^{10}+x^{15}+\cdots)^3$
(b) $(x^3+x^4+x^5+x^6+\cdots)^3$
(c) $(x^3+x^4+x^5+x^6)(x^3+x^4+x^5+x^6+x^7)\frac{1}{1-x}$
(d) $(x^2+x^4+x^6+x^8+\cdots)(x^3+x^6+x^8+x^{12}+\cdots)(x^4+x^8+x^{12}+\cdots)$
(e) $1/(1-2x)$
(f) $1/(1-x)^3$
(g) $1/(1+x)^2$
(h) $1/(1+2x)^4$
(i) $x^4/(1-3x)^3$

4. Use funções geradoras para mostrar como 10 balões idênticos podem ser distribuídos entre quatro crianças se cada criança recebe pelo menos dois balões.

5. Use funções geradoras para mostrar como 15 balões idênticos podem ser distribuídos entre 6 crianças se cada criança recebe pelo menos um e no máximo 3 balões.

6. Dê uma interpretação combinatória para $[x^4]$ em $(1+x+x^2+x^3+\cdots)^3$ e use-a para encontrar esse número.

7. Se $f(x)$ é a função geradora da sequência $(a_k\colon k\in\mathbb{N})$, determine a função geradora das sequências

(a) $(0,0,0,a_3,a_4,a_5,\ldots)$;
(b) $(a_0,0,a_1,0,a_2,0,a_3,0,\ldots)$;
(c) $(0,0,0,0,a_0,a_1,a_2,a_3,\ldots)$;
(d) $(a_0,2a_1,4a_2,8a_3,16a_4\ldots)$.

8. Use funções geradoras para mostrar que

(a)
$$\binom{m+n}{r} = \sum_{k=0}^{r}\binom{m}{r-k}\binom{n}{k}$$

(b)
$$F_{n+1} = \sum_{k=0}^{n}\varphi^k\overline{\varphi}^{n-k}$$

onde F_n é o n-ésimo número de Fibonacci e φ e $\overline{\varphi}$ são as raízes de $1-x-x^2$.

9. Use funções geradoras para determinar o n-ésimo termo da sequência definida por $a_n = 3a_{n-1}+n$ se $n\geq 1$, $a_0 = 1$.

10. Seja c_n (para todo $n\in\mathbb{N}$) o número de maneiras de escrever uma sequência de n bits sem que ocorra dois 0 consecutivos. Use funções geradoras para determinar c_n. (dica: escreva uma definição recursiva para os termos da sequência)

11. Uma escada tem $n\geqslant 1$ degraus. Você pode subir usando 1 ou 2 degraus a cada passo. De quantas maneiras distintas pode-se chegar ao topo da escada. Escreva a recorrência e resolva usando funções geradoras.

12. Escreva uma recorrência que expresse o número de seqüências de $n\geqslant 1$ digitos tomados do conjunto $\{0,1,2,3,4\}$ com pelo menos um 2 e o primeiro 2 ocorre antes do primeiro 0 (pode não ocorrer 0's).

13. Verifique as series de McLaurin associadas às funções seguintes:

(a) $\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i$

(b) $e^x = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$

(c) $\frac{1}{1-x^2} = \sum_{i=0}^{\infty} x^{2i}$

(d) $\text{sen}(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1}$

(e) $\frac{1}{(1-x)^2} = -\sum_{i=1}^{\infty} i\, x^{i-1}$

(f) $\cos(x) = \sum_{n=0}^{\infty} \frac{1}{(2n)!} x^{2n}$.

(g) $\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i$

(h) $\frac{1}{1-x^2} = \sum_{i=0}^{\infty} x^{2i}$,

(i) $\frac{1}{(1-x)^2} = -\sum_{i=1}^{\infty} i\, x^{i-1}$.

14. Dada $(a_n)_n$ sucessão de números reais, definimos a sua serie numérica associada como a sucessão de termo geral $S_n = \sum_{i=0}^{n} a_i$. Verifique que se $A(x)$ é a função geradora associada a uma sucessão de números reais $(a_n)_n$, então $\frac{A(x)}{1-x}$ é a função geradora associada à sucessão das somas parciais $(S_n)_n$.

15. Desenvolva os seguintes quocientes como soma de frações simples:

    (a) $\frac{1-2x+2x^2}{(1-x)^2(1-2x)}$,

    (b) $\frac{6x+10}{(1-2x)^2}$

    (c) $\frac{1}{(1-x^3)}$.

16. Dê a função geradora associada às seguintes recorrências, escrevendo a serie formal e identificando a função se possível:

    (a) $a_n = n a_{n-1}$, $a_0 = 1$

    (b) $b_n = 2b_{n-1} + 1$, $b_0 = 0$

    (c) $c_{n+1} = 2c_n + n$, $c_0 = 0$

    (d) $d_{n+2} = d_{n+1} + 2d_n + d_{n-1}$, $d_0 = 0, d_1 = 5, d_2 = 4$

17. Verifique que se $b_0 = 0$ então $A(B(x)) = \sum_{n \geqslant 0} c_n x^n$ onde $c_0 = a_0$ e, para $n \geqslant 1$,

$$c_n = \sum_{k=1}^{n} a_k \left(\sum_{\substack{t_1+t_2+\cdots+t_n=k \\ t_1+2t_2+\cdots+nt_n=n}} \binom{k}{t_1, t_2, \ldots, t_n} b_1^{t_1} b_2^{t_2} \cdots b_n^{t_n} \right)$$

18. Determine a quantidade de soluções inteiras não-negativas que verificam as seguintes equações:

    (a) $x + 3y = n$,

    (b) $x + y = n$, e $x \geq y$.

    (c) $x + y + z = n$, e $z \geq 2$

    (d) $x + 2y + 3z + 4u = n$.

19. Determine a quantidade de soluções inteiras não-negativas à inequação: $x + y + z < 100$.

Complemento: Série analítica de potências

Vimos que podemos manipular séries de potências formais sem considerar se elas convergem ou não. Mais que isso, tais séries podem ser tomadas com coeficientes em um anel comutativo com unidade onde a convergência não faria sentido. Por outro lado se as nossas séries, com coeficientes reais, são convergentes para valores de x diferentes de zero, então podemos usar as ferramentas de análise com elas. Em Análise Matemática, cada série de potências com coeficientes em $\mathbb{R}$ e convergente define uma função de $\mathbb{R}$ em $\mathbb{R}$. Se infinitamente muitos dos a_n não são nulos, então precisamos considerar a convergência da série de potência:

Toda série de potências têm um raio de convergência $0 \leqslant R \leqslant +\infty$ que depende dos coeficientes a_n e tal que a série converge absolutamente[5] em todo x com $|x| < R$ e diverge em $|x| > R$.

A partir da convergência as definições dada na tabela 5.1 são propriedades que devem ser demonstradas. Por exemplo, demonstra-se que se o raio de convergência $R > 0$, então a soma da série de potência é infinitamente diferenciável no intervalo $|x| < R$ e suas derivadas são dados pela diferenciação da série termo a termo.

Um fato importante é o seguinte princípio devido à unicidade da série de Taylor–Maclaurin:

Qualquer identidade entre séries analíticas envolvendo adição, multiplicação (possivelmente somas e produtos infinitos) e substituição, é uma identidade no anel de séries formais.

A versão analítica da série formal da equação (5.19) vale por se tratar do limite de uma soma de progressão geométrica; se considerarmos $|x| < 1$ e tomarmos o limite quando $n \to \infty$ em (5.19) obtemos

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots \quad (\forall x \in (-1,1)). \tag{5.20}$$

No intervalo de convergência podemos derivar os dois lados que a igualdade permanece

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 + \cdots \quad (\forall x \in (-1,1))$$

que do ponto de vista formal é a função geradora da sequência $(1,2,3,4,\ldots)$. Também podemos integrar e, por exemplo, a integral de (5.20) resulta em (5.21).

Duas séries analíticas importantes são as da exponencial e logaritmo

$$\mathrm{e}^x = 1 + \frac{x}{1} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \quad (\forall x \in \mathbb{R})$$

que do ponto de vista formal é a função geradora da sequência $\left(1,1,\frac{1}{2!},\frac{1}{3!},\ldots\right)$ e

$$\ln\left(\frac{1}{1-x}\right) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \quad (\forall x \in (-1,1)) \tag{5.21}$$

função geradora da sequência $\left(0,1,\frac{1}{2},\frac{1}{3},\ldots\right)$. Outras séries conhecidas são

$$\frac{1}{\sqrt{1-4x}} = \sum_{n\geqslant 0} \binom{2n}{n} x^n \quad (\forall x \in (-1/4, 1/4)$$

$$\operatorname{sen}(x) = \sum_{n\geqslant 0} \frac{(-1)^n}{2n+1!} x^{2n+1} \quad (\forall x \in \mathbb{R})$$

$$\cos(x) = \sum_{n\geqslant 0} \frac{(-1)^n}{2n!} x^{2n} \quad (\forall x \in \mathbb{R}).$$

Sobre convergência

Considere a seguinte soma de n termos (que é uma soma de PG)

$$\mathscr{S}_n = 1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^{n-1}} = 2 - \frac{1}{2^{n-1}}.$$

Recorde-se da definição de limite vista em Cálculo e verifique que

$$\lim_{n\to\infty} \mathscr{S}_n = 2.$$

Uma soma com infinitas parcelas, como em $1 + \frac{1}{2} + \frac{1}{4} + \cdots$ não faz sentido se levarmos em conta a definição usual de soma. Essa soma é chamada de *série* e é definida usando limite: dada uma sequência $(a_n)_{n\in\mathbb{N}}$ formamos a sequência $(S_n)_{n\in\mathbb{N}}$

$$S_n = a_0 + a_1 + \cdots + a_{n-1},$$

[5] *absolutamente* significa que $\sum_{n\geqslant 0} |a_n x^n|$ converge, o que implica que $\sum_{n\geqslant 0} a_n x^n$ converge. A reciproca não é verdadeira. Uma propriedade importante de convergência absoluta é que o limite não depende da ordem com que os termos são "somados".

e dessa forma

$$\sum_{n\geqslant 0} a_n = \lim_{n\to\infty} S_n.$$

Quando o limite acima existe então dizemos que a série $\sum_{n\geqslant 0} a_n$ é **convergente**, caso contrário, isto é, se o limite não existe, então a série e dita **divergente**. Por exemplo,

$$\begin{aligned} 1+\frac{1}{2}+\frac{1}{4}+\cdots &= \sum_{n\geqslant 0}\left(\frac{1}{2}\right)^n \text{ é convergente,} \\ 1+\frac{1}{2}+\frac{1}{3}+\cdots &= \sum_{n\geqslant 0}\frac{1}{n} \text{ é divergente.} \end{aligned}$$

As séries de funções mais importantes são as do tipo

$$\sum_{n\geqslant 0} a_n(x-c)^n$$

chamadas *série de potências em torno do ponto c*. Fazendo a transformação de variáveis $y = x - c$, o caso geral das séries de potências se reduz ao estudo das séries para $c = 0$, ou seja em torno do 0, a saber $\sum_{n\geqslant 0} a_n x^n$.

Um dos principais resultados sobre convergência de séries de potências é o seguinte.

TEOREMA 238 *A série de potências $\sum_{n\geqslant 0} a_n x^n$ **(1)** ou converge apenas para $x = 0$ **(2)** ou converge absolutamente para todo x **(3)** ou existe um número real $R > 0$ tal que $\sum_{n\geqslant 0} a_n x^n$ converge absolutamente no intervalo $(-R,+R)$ da reta e diverge fora do intervalo $[-R,+R]$, e nos pontos $+R$ e $-R$ a série pode divergir ou convergir. Ademais, se o raio de $f(x) = \sum_{n\geqslant 0} a_n x^n$ é $R > 0$ então*

1. $\frac{\mathrm{d}}{\mathrm{d}x} f(x) = \sum_{n\geqslant 1} n a_n x^{n-1}$,
2. $\int f(x)\,\mathrm{d}x = C + \sum_{n\geqslant 0} \frac{a_n}{n+1} x^{n+1}$,

com o mesmo raio de convergência.

Para determinar o raio de convergência usamos o *teste da razão* dos termos consecutivos

$$R = \lim_{n\to\infty} \left| \frac{a_n}{a_{n+1}} \right| \tag{5.22}$$

se o limite existe, senão

$$R = \frac{1}{\limsup_{n\to\infty} |a_n|^{1/n}}$$

com $\frac{1}{\infty} = 0$ e $\frac{1}{0} = \infty$.

Uma demonstração desse teorema pode ser encontrada no livro *Curso de análise, voluma 1* do Elon Lages Lima.

A série de Taylor–Maclaurin da função (analítica) f em torno de c é a série de potências

$$\sum_{n\geqslant 0} \frac{f^{(n)}(c)}{n!} x^n,$$

e pode acontecer de: (1) a série divergir, ou (2) a série convergir para $f(c+x)$, ou (3) a série convergir para algum outro número. Na maioria das funções que estudamos acontece o segundo fato, felizmente.

Complemento: Teorema binomial estendido

Newton generalizou teorema binomial para os casos $(1+x)^u$ com $u \in \mathbb{R}$. A ideia para estender os coeficientes binomiais é considerar que o número $(n)_k = n(n-1)\cdots(n-k+1)$ pode ser definido para n real.

Para qualquer $x \in \mathbb{R}$ e $k \in \mathbb{N}$

$$(x)_k = x(x-1)(x-2)\cdots(x-k+1) \quad \text{e} \quad \binom{x}{k} = \begin{cases} \frac{(x)_k}{k!} & \text{se } k > 0 \\ 1 & \text{se } k = 0 \end{cases}.$$

Por exemplo, $\binom{-2}{3} = -4$ e $\binom{1/2}{3} = 1/16$ e para todo $n \in \mathbb{N}$, $\binom{n}{k} = 0$ se $n < k$.

Uma identidade bastante útil nesse contexto é que se $x \in \mathbb{Z}^+$ então

$$\begin{aligned}\binom{-x}{k} &= \frac{-x(-x-1)(-x-2)\cdots(-x-k+1)}{k!} \\ &= \frac{(-1)^k x(x+1)(x+2)\cdots(x+k-1)}{k!} \\ &= \frac{(-1)^k (x+k-1)!}{(x-1)!\,k!} \\ &= (-1)^k \binom{n+k-1}{k}.\end{aligned}$$

TEOREMA 239 (TEOREMA BINOMIAL ESTENDIDO) *Para todo real t*

$$(1+x)^t = \sum_{n \geqslant 0} \binom{t}{n} x^n$$

sempre que $|x| < 1$.

DEMONSTRAÇÃO. O lado direito é série da Taylor–Maclaurin para $(1+x)^t$ e não é difícil provar, usando (5.22), que a série converge para $-1 < x < 1$. Os detalhes ficam como exercício. □

Esse teorema é um resultado em análise já que não há interpretação combinatória. É um resultado bastante útil, com a definição e teorema acima temos, por exemplo, para todo $k \in \mathbb{N}$

$$\frac{1}{(1+x)^k} = \sum_{n \geqslant 0} \binom{-k}{n} x^n = \sum_{n \geqslant 0} (-1)^n \binom{k+n-1}{k-1} x^n$$

e

$$\frac{1}{(1-x)^k} = \sum_{n \geqslant 0} \binom{-k}{n} (-x)^n = \sum_{n \geqslant 0} \binom{k+n-1}{k-1} x^n$$

como funções geradoras.

Índice Remissivo

$A \not\subset B$, 19
$C(n,r)$, 96
$(n)_r$, 94
$A \Rightarrow B$, 9
$A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow B$, 9
B^A, 94
$[x^n]A(x)$, 112
$\aleph_0$, 86
F, 3
V, 3
$\mathfrak{c}$, 86
$\max(A)$, 44
Árvore binária com raiz, 76
ímpar, 30
Modus Ponens, 11
Modus ponens, 11
Modus tollens, 12
modus ponens, 9

antecedente, 5
anticadeia, 67
anulamento, 28
argumento, 11
arranjo, 95
arranjo com repetição, 95
arranjo simples, 94
associativa, 28
atômica, 3

base da indução, 50
bem definidas, 55
bem fundada, 73
bicondicional, 3
bijetividade, 25
boa ordem, 67
boa-ordem, 27

cadeia, 67
cancelativa, 28
cardinalidade, 81, 84
cardinalidade do contínuo, 86
classe de equivalência, 62
cobre, 65
coeficiente, 112
coeficiente binomial, 96
coeficiente multinomial, 103
combinação, 95
comparáveis, 65
composto, 41
comutativa, 28
conclusão, 11
condição de cadeia descendente, 73
condicional, 3
conectivos lógicos, 3
conjunção, 3
conjunto das partes de A, 19
conjunto indutivo, 22
conjunto quociente, 63
consequente, 5
contagem, 85
contagem dupla, 99
contradição, 5
contraexemplo, 7
contrapositiva, 5
converge, 112
convergente, 121
cota inferior, 29
crescente, 40

decrescente, 40
definição recursiva, 55
Desigualdade de Bernoulli, 51
diagrama de Hasse, 65
Diferença, 20
Diferença simétrica, 20
disjunção, 3
disjuntos, 21
distributiva, 28
divergente, 121
divide, 33
domínio, 24

e, 3
elemento neutro, 28
elemento simétrico, 28
enumerável, 86
enumeração, 85
equação de recorrência, 55
equivalência lógica, 10

fatores, 33
fatorial, 55

fecho reflexivo, 78
fecho transitivo, 79
finito, 85
forma fechada, 56
forma reduzida, 36
função, 25
função de Ackermann, 74
função de pareamento de cantor, 90
função geradora ordinária, 112

Generalização existencial, 13
Generalização universal, 13
grafo
    de Moser, 92

hipótese do contínuo, 87

identidade de Vandermonde, 107
implica logicamente, 9
implicam logicamente, 9
incomparáveis, 65
indução noetheriana, 74
Indução pra frente–pra trás, 50
injetividade, 25
instanciação, 6
Instanciação existencial, 13
Instanciação universal, 13
Intersecção, 20
irracional, 36
isomorfas, 72
isomorfismo, 72

juro composto, 55

lema de Tukey, 79
Lema de Zorn, 79
limitado inferiormente, 29
limitado superiormente, 44
linearização, 71
logicamente equivalentes, 10

mínimo, 29, 66
máximo, 66
média aritmética, 53
média geométrica, 53
módulo, 29
mãos de bridge, 103
maior divisor comum, 35
maior elemento, 44
mapa logístico, 55
maximal, 66
menor elemento, 27, 29
mesma cardinalidade, 81
minimal, 66

número de Bell, 105
número de Stirling do segundo tipo, 104
números de Fibonacci, 51

não, 3
não-crescente, 40
não-decrescente, 40
negação, 3

ordem estrita, 65
ordem estrita associada, 65
ordem lexicografica, 70
ordem parcial, 64
ordem produto, 70
ordem total, 67
ordenação topológica, 70
ordinais finitos de Von Neumann, 72
ordinais limites, 73
ordinais sucessores, 73
ou, 3

par, 30
par ordenado, 23
paradoxo
    dos aniversários, 88, 95
partição, 21
passo da indução, 50
permutação, 95
permutação caótica, 107
PG, 84
PIF, 48
PIF passo k, 50
PIFc, 49
PIFcg, 49
PIFg, 49
PM, 85
premissas, 11
preserva a ordem, 70
primo, 41
princípio
    das gavetas
        generalizado, 87
princípio aditivo, 85
princípio da casa dos pombos, 84
princípio da descida infinita de Fermat, 41
Princípio da Indução finita, 48
Princípio da Indução finita completo, 49
Princípio da Indução finita completo generalizado, 49
Princípio da Indução finita generalizado, 49
Princípio das Gavetas, 84
Princípio das gavetas generalizado, 87
princípio das gavetas infinitário, 91
Princípio das gavetas ordenado, 88
Princípio das gavetas probabilístico, 88
Princípio de Inclusão–Exclusão, 93, 107
Princípio de indução completo para boa ordem, 68
Princípio de indução completo para relação bem fundada, 74
princípio multiplicativo, 85
princípo da boa ordenação do naturais, 27
problema

de Hadwiger–Nelson, 92
produto cartesiano, 23
progressões aritmética e geométrica, 55
projeção canônica, 63
Prova por casos, 13

quantificação existencial, 7
quantificação universal, 7

racional, 36
recíproca, 5
recíproco, 113
refina, 63
Regra da Adição, 11
Regra da conjunção, 12
Regra da contradição, 12
Regra da Simplificação, 11
Regra do silogismo disjuntivo, 12
Regra do silogismo hipotético, 12
Regras de inferência, 11
relação, 24
relação composta, 25
relação de equivalência, 61
relação de Stifel, 72
relação inversa, 25
representante, 62
Resolução, 13

se, e somente se,, 3
se,... então, 3
segmento inicial, 72
segmento inicial próprio, 72
sentença, 3
sentença aberta, 6
sequência numérica, 40
sequência transfinita, 73
sobrejetividade, 25
solução, 56
subconjunto, 19
subconjunto próprio, 19
subconjuntos próprios, 66

tautologia, 5
Teorema Binomial, 99
Teorema da boa ordem, 79
teorema da divisão euclidiana, 41
teorema de Bézout, 42
teorema de Bachet–Bézout, 75
Teorema de Cantor, 86
Teorema de Cantor–Schröder–Bernstein, 82
Teorema de Dilworth, 69
teorema de Erdős–Szekerés, 69
teorema fundamental da aritmética, 41
teorema fundamental das relações de equivalência, 62
teorema multinomial, 108
triângulo de Pascal, 100

União, 20

válido, 11
valor absoluto, 29
valor-lógico, 3
variável livre, 5
variável muda, 6