Preenchemos o meio da prova com a sentença 7 e estamos terminados! Como forma de celebrar e registrar o final de uma prova, acrescentamos, ao final da prova, o símbolo de fim-de-prova: ■

Este passo intermediário – bastante fácil – é, na verdade, a parte mais difícil da prova. A tradução da afirmação contida na proposição em forma "se-então", e o desenredamento de definições são questões de rotina; uma vez redigidas várias provas, veremos que esses passos são obtidos facilmente. A parte difícil vem ao procurar fazer os extremos se encontrarem!

A prova da Proposição 4.2 é o tipo mais fundamental de prova; ela é chamada prova *direta*. Os estágios da formulação de uma prova direta de um teorema do tipo "se-então" são apresentados no Esquema de prova 1.

Esquema de prova 1

A prova direta de um teorema "se-então".

- Escrever a(s) primeira(s) sentença(s) da prova, apresentando de novo a hipótese do resultado. Criar uma notação adequada (por exemplo, atribuir letras para representar variáveis).
- Escrever a(s) última(s) sentença(s) da prova, apresentando de novo a conclusão do resultado.
- Desenredar as definições, trabalhando para a frente, a partir do começo da prova, e para trás, a partir do fim da prova.
- Avaliar o que já sabe e o que necessita. Procurar estabelecer um elo entre as duas metades de seu argumento.

Vamos aplicar a técnica da prova direta para provar outro resultado.

Proposição 4.3

Sejam a, b e c inteiros. Se $a|b$ e $b|c$, então $a|c$.

O primeiro passo na elaboração de uma prova dessa proposição consiste em escrever a primeira e a última sentenças com base na hipótese e na conclusão. Vem:

Sejam a, b e c inteiros, com $a|b$ e $b|c$.

...

Portanto, $a|c$. ■

Em seguida, desenredamos a definição de divisibilidade.

Seja x um inteiro.
($\Rightarrow$) Suponhamos x par... Portanto, $x + 1$ é ímpar.
($\Leftarrow$) Suponhamos $x + 1$ ímpar... Portanto, x é par. ■

Note que assinalamos as duas seções da prova com os símbolos ($\Rightarrow$) e ($\Leftarrow$). Isso permite ao leitor identificar a seção da prova.

Agora, desenredamos as definições na frente de cada parte da prova. (Recorde-se da definição de *ímpar*; ver Definição 2.4.)

Seja x um inteiro.
($\Rightarrow$) Suponhamos x par. Isso significa que $2|x$. Logo, há um inteiro a de modo que $x = 2a$... Portanto, $x + 1$ é ímpar.
($\Leftarrow$) Suponhamos $x + 1$ ímpar. Então, existe um inteiro b de modo que $x + 1 = 2b + 1$... Portanto, x é par. ■

Os próximos passos são claros. Na primeira parte da prova, temos $x = 2a$, e queremos provar que $x + 1$ é ímpar. Basta somarmos 1 a cada um dos membros de $x = 2a$, para obter $x + 1 = 2a + 1$, e isso mostra que $x + 1$ é ímpar.

Na segunda parte da prova, sabemos que $x + 1 = 2b + 1$; queremos provar que x é par. Subtraímos 1 de cada um dos membros e estamos terminados.

Seja x um inteiro.
($\Rightarrow$) Suponhamos x par. Isso significa que $2|x$. Logo, existe um inteiro a de modo que $x = 2a$. Adicionando 1 a ambos os membros, obtemos $x + 1 = 2a + 1$. Pela definição de ímpar, $x + 1$ é ímpar.
($\Leftarrow$) Suponhamos $x + 1$ é ímpar. Então, existe um inteiro b de modo que $x + 1 = 2b + 1$. Subtraindo 1 de ambos os membros, obtemos $x = 2b$. Isso mostra que $2|x$ e, portanto, x é par. ■

O Esquema de prova 2 mostra o método básico para provar um teorema do tipo "se-e-somente-se".

Esquema de prova 2

Prova direta de um teorema do tipo "se-e-somente-se".

Para provar uma afirmação da forma "A se e somente se B":

- ($\Rightarrow$) Prove que "se A, então B".
- ($\Leftarrow$) Prove que "se B, então A".

Por exemplo, consideremos a afirmação "Se x é primo, então x é ímpar". Essa afirmação é falsa. Para prová-lo, basta darmos um exemplo de um inteiro que seja primo, mas não seja ímpar. O inteiro 2 goza dessas propriedades.

Consideremos outra afirmação falsa.

Afirmação 5.1

(Falsa) Sejam a e b inteiros. Se $a|b$ e $b|a$, então $a = b$.

Essa afirmação se afigura plausível. Parece que, se $a|b$, então $a \leq b$ e se $b|a$, então $b \leq a$, então $a = b$. Mas este raciocínio é incorreto.

Para refutar a Afirmação 5.1, precisamos achar inteiros a e b, tais que, de um lado, verifiquem $a|b$ e $b|a$, mas, do outro, não verifiquem $a = b$.

Eis um contraexemplo. Tomemos $a = 5$ e $b = -5$. Para verificar que se trata de um contraexemplo, basta notarmos que, de um lado, $5|-5$ e $-5|5$, mas, do outro, $5 \neq -5$.

Esquema de prova 3

Como refutar uma afirmação do tipo "se-então" falsa por meio de um contraexemplo.

Para refutar uma afirmação da forma "Se A, então B":

Achar uma situação em que A é verdadeira, mas B é falsa.

Refutar afirmações falsas é, em geral, mais fácil que provar afirmações verdadeiras. Todavia, achar contraexemplos pode ser trabalhoso. Para criar um contraexemplo, recomendo criar várias instâncias em que a hipótese da afirmação é verdadeira, e verificar cada uma a fim de ver se a conclusão é válida ou não. Tudo quanto é preciso para refutar uma afirmação é um contraexemplo.

Infelizmente, é fácil embaraçarmo-nos com um pensamento rotineiro. No caso da Afirmação 5.1, poderíamos considerar $3|3$, $4|4$ e $5|5$, sem jamais cogitarmos de tomar um número positivo e o outro negativo.

Tente livrar-se de tal situação criando exemplos estranhos. Não esqueça o número 0 (que atua de maneira estranha) e dos números negativos. Naturalmente, seguindo esse conselho, poderíamos ainda ver-nos diante de casos como $0|0$, $-1|-1$, $-2|-2$ e assim por diante.

Eis uma estratégia para achar contraexemplos. Começamos procurando provar a afirmação; quando encontrar dificuldade, procure determinar em que consiste o problema e construa um contraexemplo.

Apliquemos esta técnica à Afirmação 5.1. Comecemos, como de costume, convertendo a hipótese e a conclusão da afirmação no começo e no fim da prova.

> Sejam a e b inteiros com $a|b$ e $b|a$. ... Portanto, $a = b$. ■

Desenredemos, agora, as definições.

O ponto importante a ressaltar é que as colunas $\neg(x \wedge y)$ e $(\neg x) \vee (\neg y)$ são exatamente as mesmas. Portanto, quaisquer que sejam os valores que escolhamos para x e y, as expressões $\neg(x \wedge y)$ e $(\neg x) \vee (\neg y)$ conduzem ao mesmo valor verdade. Portanto, as expressões $\neg(x \wedge y)$ e $(\neg x) \vee (\neg y)$ são logicamente equivalentes.

As provas com auxílio de tabelas verdade são fáceis, porém maçantes. O resultado seguinte resume as propriedades algébricas básicas das operações $\wedge$, $\vee$ e $\neg$. Em vários casos, atribuímos nomes às propriedades. ■

Esquema de prova 4

Prova da equivalência lógica pela tabela-verdade

Para mostrar que duas expressões booleanas são logicamente equivalentes:

Construímos uma tabela-verdade mostrando os valores das duas expressões para todos os valores possíveis das variáveis.

Fazemos uma verificação para constatar que as duas expressões booleanas têm sempre o mesmo valor.

Provas efetuadas com base em tabelas verdade são simples mas extensas. Os resultados apresentados a seguir sintetizam as propriedades algébricas básicas das operações $\wedge$, $\vee$ e $\neg$. Em muitos casos, essas propriedades recebem nomes específicos.

Teorema 6.2

- $x \wedge y = y \wedge x$ e $x \vee y = y \vee x$ (Propriedades comutativas)
- $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ e $(x \vee y) \vee z = x \vee (y \vee z)$ (Propriedades associativas).
- $x \wedge$ Verdadeiro $= x$ e $x \vee$ Falso $= x$ (Elementos identidades)
- $\neg(\neg x) = x$
- $x \wedge x = x$ e $x \vee x = x$
- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ e $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ (Propriedades distributivas).
- $x \wedge (\neg x) =$ Falso e $x \vee (\neg x) =$ Verdadeiro.
- $\neg(x \wedge y) = (\neg x) \vee (\neg y)$ e $\neg(x \vee y) = (\neg x) \wedge (\neg y)$ (Leis de DeMorgan).

Todas essas equivalências lógicas são facilmente demonstradas por meio de tabelas-verdade. Em algumas dessas identidades, há apenas uma variável (por exemplo, $x \wedge \neg x =$ Falso); nesse caso, haveria apenas duas linhas na tabela-verdade (uma para $x =$ Verdadeiro e uma para $x =$ Falso). Nos casos em que há três variáveis, há oito linhas na tabela verdade, na medida em que (x, y, z) tomam os valores possíveis (V, V, V), (V, V, F), (V, F, V), (V, F, F), (F, V, V), (F, V, F), (F, F, V) e (F, F, F).

Mais operações

As operações $\wedge$, $\vee$ e $\neg$ foram criadas para reduzir o uso, empregados pelos matemáticos, das palavras *e*, *ou* e *não*. Vamos introduzir agora mais duas operações, $\rightarrow$ e $\leftrightarrow$, criadas para

É importante notar que o símbolo Ø não é a mesma coisa que a letra grega *phi*: ϕ ou Φ.

Notação de conjunto

Há duas maneiras principais de especificarmos um conjunto. A maneira mais direta consiste em listar, entre chaves, os elementos do conjunto, como em $\{3, 4, 9\}$. Essa notação é apropriada para pequenos conjuntos. Mais frequentemente, utiliza-se a *notação de conjunto* cuja forma é

{variável de referência: condições}

Consideremos, por exemplo,

$$\{x : x \in \mathbb{Z}, x \geq 0\}$$

Este é o conjunto de todos os objetos x que satisfazem duas condições: (1) $x \in \mathbb{Z}$ (isto é, x deve ser inteiro) e (2) $x \geq 0$ (isto é, x é não negativo). Em outras palavras, esse conjunto é $\mathbb{N}$, os números naturais.

Uma forma alternativa de escrever a notação de conjunto é:

{variável de referência $\in$ conjunto: condições}

Este é o conjunto de todos os objetos extraídos do conjunto mencionado e sujeitos às condições especificadas. Por exemplo,

$$\{x \in \mathbb{Z} : 2|x\}$$

é o conjunto de todos os inteiros divisíveis por 2 (isto é, o conjunto dos inteiros pares).

Pode-se cogitar de escrever um conjunto estabelecendo um padrão para os seus elementos e utilizando pontos (...) para indicar que o padrão continua. Por exemplo, poderíamos representar o conjunto dos inteiros de 1 a 100, inclusive como $\{1, 2, 3, ..., 100\}$. Nesse caso, a notação é clara, mas seria preferível escrevermos $\{x \in \mathbb{Z} : 1 \leq x \leq 100\}$.

Eis outro exemplo, não tão claro: $\{3, 5, 7, ...\}$. O que é que se pretende? Temos de supor se trata do conjunto dos inteiros ímpares maiores que 1 ou do conjunto de inteiros primos. Use a notação "..." com parcimônia e somente quando não houver qualquer possibilidade de confusão.

Igualdade de conjuntos

O que significa dois conjuntos serem *iguais*? Significa que os dois conjuntos têm exatamente os mesmos elementos. Para provar que dois conjuntos A e B são iguais, mostramos que todo elemento de A é também elemento de B, e vice-versa.

Esquema de prova 5 Provar que dois conjuntos são iguais. Sejam A e B os conjuntos. Para provar que $A = B$, temos o seguinte esquema:

- Suponhamos que $x \in A$... Portanto, $x \in B$.
- Suponhamos que $x \in B$... Portanto, $x \in A$.

Portanto, $A = B$. ■

A diferença entre $\in$ e $\subset$ é análoga à diferença entre x e $\{x\}$. O símbolo x se refere a um objeto (um número ou o que seja), e a notação $\{x\}$ significa o conjunto cujo único elemento é x. É sempre correto escrever $x \in \{x\}$, mas não é correto escrever $x = \{x\}$ ou $x \subseteq \{x\}$. (Bem, *em geral* não é correto escrever $x \subseteq \{x\}$; cf. Exercício 9.9).

Para provar que um conjunto é subconjunto de outro, devemos mostrar que todo elemento do primeiro conjunto é também elemento do outro conjunto.

Proposição 9.3

Seja x um objeto arbitrário e seja A um conjunto; então $x \in A$ se e somente se $\{x\} \subseteq A$.

Prova. Seja x um objeto arbitrário e A um conjunto.

($\Rightarrow$) Suponhamos que $x \in A$. Pretendemos mostrar que $\{x\} \subseteq A$. Para tanto, devemos mostrar que todo elemento de $\{x\}$ é também elemento de A. Mas o único elemento de $\{x\}$ é x, e sabemos que $x \in A$. Portanto, $\{x\} \subseteq A$.

($\Leftarrow$) Suponhamos que $\{x\} \subseteq A$. Isso significa que todo elemento do primeiro conjunto ($\{x\}$) é também membro do segundo conjunto (A). Mas o único elemento do conjunto $\{x\}$ é certamente x; assim, $x \in A$. ■

O Esquema de Prova 6 dá o método geral para mostrar que um conjunto é subconjunto de outro.

Esquema de prova 6

Provar que um conjunto é subconjunto de outro.

Mostrar que $A \subseteq B$:

Seja $x \in A$. ... Portanto, $x \in B$ e, assim, $A \subseteq B$. ■

Ilustramos o uso do Esquema de Prova 6 utilizando o seguinte conceito.

Definição 9.4

(Terno Pitagórico) Uma lista de três inteiros (a, b, c) é chamada *terno pitagórico*, contanto que $a^2 + b^2 = c^2$.

Por exemplo, (3, 4, 5) é um terno pitagórico porque $3^2 + 4^2 = 5^2$. Os ternos pitagóricos são chamados assim por serem os comprimentos dos lados de um triângulo retângulo.

Observe que $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ não representa um terno pitagórico porque os números na lista não são inteiros; o termo *terno pitagórico* aplica-se apenas a listas de inteiros.

Proposição 9.5

Seja P o conjunto de ternos pitagóricos; ou seja,

$$P = \{(a, b, c) : a, b, c \in \mathbb{Z} \text{ e } a^2 + b^2 = c^2\}$$

mas a expressão "existe" não elimina a possibilidade de haver mais de um objeto com as propriedades desejadas.

A palavra *existe* é sinônimo de *há*.

Como a palavra "existe" aparece com tanta frequência, os matemáticos criaram uma notação formal para afirmações da forma "Existe um x no conjunto A tal que...". Escrevemos um E maiúsculo invertido ($\exists$), que se lê *há*, ou *existe*. A forma geral de uso desta notação é

$$\exists x \in A, \text{ afirmações sobre } x.$$

Lê-se: "Existe um x, elemento do conjunto A, para o qual as afirmações são válidas". A sentença "Existe um número natural que é primo e par" seria escrita da seguinte forma:

$$\exists x \in \mathbb{N}, x \text{ é primo e par.}$$

A letra x é uma variável de referência – apenas preenche um lugar. É análoga ao índice de somatório na notação Σ.

Às vezes, abreviamos a afirmação "$\exists x \in A$, afirmações sobre x", para "$\exists x$, afirmações sobre x" quando o contexto deixa claro que tipo de objeto x deve ser.

O símbolo E é chamado *quantificador existencial*.

Para provar uma afirmação da forma "$\exists x \in A$, afirmações sobre x", devemos mostrar que algum elemento de A satisfaz as afirmações. A forma geral dessa prova é dada no Esquema de prova 7.

Esquema de prova 7

Prova de afirmações existenciais.

Provar que $\exists x \in A$, afirmações sobre x:

Seja x (dar um exemplo explícito) ... (Mostrar que x satisfaz as afirmações...)

Portanto, x satisfaz as afirmações requeridas. ■

Provar uma afirmação existencial é análogo a achar um contraexemplo. Basta achar um objeto com as propriedades requeridas.

Exemplo 10.1

Eis uma prova (muito rápida!) de que existe um inteiro que é par e primo.

Afirmação: $\exists x \in \mathbb{Z}$, x é par e x é primo.

Prova. Consideremos o inteiro 2. Obviamente 2 é par e 2 é primo. ■

Para todo

A outra expressão que vamos considerar nesta seção é *todo* como em "Todo inteiro é par ou ímpar". Há expressões alternativas que usamos em lugar de *todo*, inclusive *todos*, *cada* e *qualquer*. Todas as sentenças a seguir significam a mesma coisa:

- *Todo* inteiro é ou par ou ímpar.
- *Todos os* inteiros são ou pares ou ímpares.
- *Cada* inteiro é ou par ou ímpar.
- Seja x um inteiro *qualquer*. Então x é par ou ímpar.

Em todos os casos, queremos dizer que a condição se aplica a todos os inteiros, sem exceção.

Há uma notação simbólica para esses tipos de sentença. Assim como usamos o $\exists$ ($\exists$ invertido) para *há*, ou *existe*, utilizamos um A invertido ($\forall$) com a significação de *para todo*, ou *qualquer que seja*. A forma geral para esta notação é

$$\forall x \in A, \text{ afirmações sobre } x.$$

Isso significa que todos os elementos do conjunto A satisfazem as afirmações como em

$$\forall x \in \mathbb{Z}, x \text{ é ímpar ou } x \text{ é par.}$$

Quando o contexto não deixa dúvida sobre que tipo de objeto x é, a notação pode ser abreviada para "$\forall x$, afirmações sobre x".

O A invertido é chamado *quantificador universal.*

Para provar um teorema do tipo "todo", devemos mostrar que todo elemento do conjunto satisfaz as afirmações requeridas. A forma geral desse tipo de prova é dada no Esquema de prova 8.

Esquema de prova 8

Prova de afirmações universais

Provar $\forall x \in A$, afirmações sobre x:

Seja x um elemento qualquer de A. ... (Mostre que x satisfaz as afirmações lançando mão apenas do fato de $x \in A$, e não de quaisquer outras suposições sobre x.)... Portanto, x verifica as afirmações exigidas. ■

Exemplo 10.2

Provar: Todo inteiro divisível por 6 é par.

Mais formalmente: Seja $A = \{x \in \mathbb{Z}: 6 \mid x\}$. Então, a afirmação que desejamos provar é

$$\forall x \in A, x \text{ é par.}$$

Prova. Seja $x \in A$; isto é, x é um inteiro divisível por 6. Isso significa que existe um inteiro y, de modo que $x = 6y$, que se pode escrever como $x = (2 \cdot 3)y = 2(3y)$. Assim, x é divisível por 2 e, portanto, é par. ■

Note que essa prova não difere realmente da prova de um teorema comum do tipo "se-então", "Se x é divisível por 6, então x é par". O ponto que procuramos salientar é que, na prova, admitimos que x seja um elemento arbitrário de A, e então passamos a mostrar que x satisfaz a condição.

Como essas duas grandezas, $|A| + |B|$ e $|A \cup B| + |A \cap B|$ respondem à mesma pergunta, elas devem ser iguais. ■

Essa prova é um exemplo de *prova combinatória*. Tipicamente, uma prova combinatória é usada para demonstrar que uma equação (tal como a da Proposição 11.4) é válida. Para tanto, criamos uma questão e mostramos que ambos os membros da equação dão uma resposta correta para a questão. Segue-se então – ambos os membros são respostas corretas – que os dois membros da equação alegada devem ser iguais. Resumimos esta técnica no Esquema de prova 9.

Esquema de prova 9
Prova combinatória

Provar uma equação da forma ME = MD (membro esquerdo = membro direito):

Coloque uma questão da forma: "De quantas maneiras...?"

De um lado, mostre por que ME é uma resposta correta da questão.

Do outro lado, mostre por que MD é uma resposta correta.

Por conseguinte, ME = MD. ■

Nem sempre é fácil achar a pergunta correta a ser formulada. Redigir demonstrações combinatórias é análogo a jogar o jogo de TV *Jeopardy*!* O leitor recebe a resposta (na verdade, duas respostas) a um problema de contagem; seu trabalho consiste em achar uma pergunta cujas respostas são os dois membros da equação que está tentando provar.

Inclusão-exclusão básica.

Daremos mais provas combinatórias, mas, por ora, voltemos à Proposição 11.4. Uma forma útil de reformulação desse resultado é a seguinte:

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{4}$$

Trata-se de um caso especial de um método de contagem, chamado *inclusão-exclusão*, que pode ser interpretado como segue. Suponha que queiramos contar o número de objetos que tenham uma ou outra propriedade. Imagine que o conjunto A contenha os objetos que têm uma das propriedades, e que o conjunto B contenha os objetos que têm a outra propriedade. Então, o conjunto $A \cup B$ contém os objetos que têm uma propriedade, ou a outra; podemos contar esses objetos calculando $|A| + |B| - |A \cap B|$. Essa fórmula é útil quando o cálculo de $|A|$, $|B|$ e $|A \cap B|$ é mais fácil que o cálculo de $|A \cup B|$. Na Seção 18 desenvolvemos mais extensamente o conceito de inclusão-exclusão.

Exemplo 11.5

Quantos inteiros do intervalo 1 a 1.000 (inclusive) são divisíveis por 2 ou por 5?

* Programa de televisão dos Estados Unidos, cuja atração é um jogo de perguntas e respostas de temas diversos. (N. E.)

$$= \binom{n}{0}n^k - \binom{n}{1}(n-1)^k + \binom{n}{2}(n-2)^k$$
$$- \binom{n}{3}(n-3)^k + \cdots \mp \binom{n}{n}(n-n)^k$$
$$= \sum_{j=0}^{n}(-1)^j \binom{n}{j}(n-j)^k$$

o que responde à pergunta do Exercício 18.3.

O Exemplo 18.4 é conhecido como *problema da verificação dos chapéus*. A história relata que n pessoas vão a um teatro e deixam seus chapéus com um porteiro descuidado. O porteiro devolve os chapéus aos donos de maneira aleatória. O problema é: qual é a probabilidade de nenhuma das pessoas receber de volta seu próprio chapéu? A resposta dessa questão de probabilidade é a resposta do Exemplo 18.4 dividida por $n!$

Desordenações

Ilustramos o método do Esquema de prova 10 com o seguinte problema clássico.

Exemplo 18.4

(Desordenações de contagem) Há $n!$ maneiras de criar listas de comprimento n utilizando os elementos de $\{1, 2, ..., n\}$ sem repetição. Essa lista é chamada *desordenação* se o número j não ocupar a posição j da lista para qualquer $j = 1, 2, ..., n$. Quantas desordenações existem?

Por exemplo, se $n = 8$, as listas (8, 7, 6, 5, 4, 3, 2, 1) e (6, 5, 7, 8, 1, 2, 3, 4) são desordenações, mas (3, 5, 1, 4, 8, 6, 7) e (2, 1, 4, 3, 8, 6, 7, 5) não o são.

Esquema de prova 10
Utilizando inclusão-exclusão.

Contagem com inclusão-exclusão:

- Classificar os objetos como "bons" (os que deseja contar) ou "maus" (os que não deseja contar).
- Decidir se deseja contar diretamente os objetos bons ou os maus e subtrair seu número do total.
- Colocar o problema de contagem como o tamanho de uma união de conjuntos. Cada conjunto descreve uma forma como os objetos podem ser "bons" ou "maus".
- Aplicar a inclusão-exclusão (Teorema 18.1).

Exemplo 18.5

As desordenações de $\{1, 2, 3, 4\}$ são

a	b	$a \rightarrow b$	$\neg b$	$\neg a$	$(\neg b) \rightarrow (\neg a)$
V	V	V	F	F	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

A linha da base é: "para provar que "Se A, então B", é aceitável provar "Se (não B), então (não A)", conforme esboçado no Esquema de prova 11.

Esquema de prova 11
Prova pela contrapositiva
Provar que "Se A, então B": supor (não B) e tentar provar (não A).

Vamos trabalhar com um exemplo.

Proposição 19.1
Seja R uma relação de equivalência em um conjunto A e sejam $a, b \in A$. Se $a \not R\ b$, então $[a] \cap [b] = \emptyset$.

Essencialmente, isso já foi provado (ver Proposição 14.12). Nosso objetivo aqui é ilustrar a prova pela contrapositiva. Nós o faremos utilizando o Esquema de prova 11.

> Seja R uma relação de equivalência em um conjunto A e sejam $a, b \in A$. Vamos provar a contrapositiva da afirmação.
> Suponhamos $[a] \cap [b] \neq \emptyset$ .... Portanto, $a\ R\ b$. ■

O ponto-chave a observar é que supomos a oposta da conclusão (não $[a] \cap [b] = \emptyset$) e procuramos provar a oposta da hipótese (não $a \not R\ b$; isto é, $a\ R\ b$).

Note que você foi alertado para o fato de que não estamos utilizando a prova direta, anunciando que vamos provar a contrapositiva.

Para prosseguir a prova, observamos que $[a] \cap [b] \neq \emptyset$ significa que existe um elemento simultaneamente em $[a]$ e em $[b]$. Introduzamos esse fato na prova.

> Seja R uma relação de equivalência em um conjunto A e sejam $a, b \in A$. Vamos provar a contrapositiva da afirmação.
> Suponhamos $[a] \cap [b] \neq \emptyset$. Então, existe um $x \in [a] \cap [b]$, isto é, $x \in [a]$ e $x \in [b]$ ... Portanto, $a\ R\ b$. ■

Esquema de prova 12

Prova por contradição

Provar que "Se A, então B":

Supomos as condições em A.

Por contradição, supomos não B.

Argumentamos até chegar a uma contradição.

$\Rightarrow\Leftarrow$ ■

(O símbolo $\Rightarrow\Leftarrow$ é uma abreviatura do seguinte: assim, chegamos a uma contradição. Portanto, a suposição (não B) deve ser falsa. Logo, B é verdadeira.)

Vamos apresentar uma descrição formal de uma prova por contradição e, em seguida, dar um exemplo.

Pretendemos provar uma afirmação da forma "Se A, então B". Para isso, admitimos A e (não B) e mostramos que isso implica algo falso. Simbolicamente, queremos mostrar que $a \rightarrow b$. Para tanto, provamos que $(a \wedge \neg b) \rightarrow$ FALSO. Essas duas proposições são logicamente equivalentes.

Proposição 19.2

As fórmulas *booleanas* $a \rightarrow b$ e $(a \wedge \neg b) \rightarrow$ FALSO são logicamente equivalentes.

Prova. Para confirmar que as duas expressões se equivalem logicamente, construímos uma tabela-verdade.

a	b	$a \rightarrow b$	$\neg b$	$(a \wedge \neg b) \rightarrow$ FALSO
V	V	V	F	V
V	F	F	V	F
F	V	V	F	V
F	F	V	F	V

Portanto, $a \rightarrow b = (a \wedge \neg b) \rightarrow$ FALSO. ■

Apliquemos esse método para provar o seguinte:

Proposição 19.3

Nenhum inteiro é ao mesmo tempo par e ímpar.

Reexpressa na forma "se-então", a Proposição 19.3 é "se x é um inteiro, então x não pode ser simultaneamente par e ímpar".

Formulemos uma prova por contradição.

manipular esses elementos a fim de chegar a algo falso. Tentemos dividir a equação $x = 2a = 2b + 1$ por 2, obtendo $\frac{x}{2} = a = b + \frac{1}{2}$, o que nos diz que um inteiro é apenas $\frac{1}{2}$ maior que o outro (isto é, $a - b = \frac{1}{2}$). Mas $a - b$ é um inteiro e $\frac{1}{2}$ não é! Um número $(a - b)$ não pode ser ao mesmo tempo inteiro e não inteiro! É uma contradição. Hurra!! Vamos introduzi-la na prova. (Note que não utilizamos $\frac{x}{2}$ na contradição, o que nos permite simplificar bastante.)

Seja x um inteiro.

Suponhamos, por contradição, que x seja par e ímpar.

Como x é par, sabemos que $2|x$; isto é, existe um inteiro a de modo que $x = 2a$.

Como x é ímpar, sabemos que existe um inteiro b de modo que $x = 2b + 1$.

Portanto, $2a = 2b + 1$. Dividindo ambos os membros por 2, obtemos $a = b + \frac{1}{2}$, de forma que $a - b = \frac{1}{2}$. Note que $a - b$ é um inteiro (pois a e b o são), mas $\frac{1}{2}$ não é inteiro. $\Rightarrow\Leftarrow$ Logo, *x não* é ao mesmo tempo par e ímpar, e a proposição está provada. ■

Isso completa a prova. Quando começamos essa prova, não sabíamos que a contradição a que chegaríamos seria a de que $\frac{1}{2}$ é um inteiro. Isso é típico em uma prova por contradição; começamos com A e (não B) e vemos aonde a implicação conduz.

A Proposição 19.3 também pode expressar-se como segue. Sejam

$$X = \{x \in \mathbb{Z} : x \text{ é par}\} \text{ e}$$
$$Y = \{x \in \mathbb{Z} : x \text{ é ímpar}\}$$

Então $X \cap Y = \emptyset$.

A prova por contradição é, em geral, a melhor técnica para mostrar que um conjunto é vazio. Ela justifica a codificação em um esquema de prova.

Esquema de prova 13
Provar que um conjunto é vazio

Para provar que um conjunto é vazio:

Suponha que o conjunto é não vazio e argumente de forma a chegar a uma contradição.

O Esquema de prova 13 é apropriado para provar afirmações da forma: "Não há objeto que satisfaça às condições".

A contradição é também a técnica de prova escolhida quando devemos provar afirmações de *unicidade*. Tais afirmações asseguram que só pode haver um objeto que satisfaça às condições dadas.

Linguagem matemática!

Você poderia esperar que, acima de todas as pessoas, os matemáticos empregassem a palavra *dois* corretamente. Pode surpreender, pois, quando um matemático diz "dois", ele eventualmente quer dizer "um ou dois". Eis um exemplo. Consideremos a seguinte afirmação: "Todo inteiro positivo par é a soma de dois inteiros positivos ímpares". Os matemáticos consideram verdadeira essa afirmação, a despeito do fato de só haver uma maneira de escrever 2 como soma de dois inteiros positivos ímpares, a saber, 2 = 1 + 1. Ocorre que apenas os dois números são o mesmo.

A frase "Sejam x e y dois inteiros..." permite que os inteiros x e y sejam o mesmo. Esta é a convenção, embora um tanto perigosa. Seria melhor escrever simplesmente "Sejam x e y inteiros...". Ocasionalmente, interessa-nos eliminar a possibilidade $x = y$. Nesse caso, escrevemos "Sejam x e y dois inteiros diferentes..." ou "Sejam x e y dois inteiros distintos...".

Esquema de prova 14

Prova da unicidade

Para provar que há, no máximo, um objeto que satisfaz determinadas condições:

Suponhamos que haja dois objetos diferentes, x e y, que verificam as condições.

Argumente de modo a chegar a uma contradição.

Com frequência, a contradição em uma prova de unicidade é que os dois objetos alegadamente diferentes são, na verdade, o mesmo. Eis um exemplo simples.

Proposição 19.4

Sejam a e b números com $a \neq 0$. Existe no máximo um número x com $ax + b = 0$.

Prova. Suponhamos que haja dois números diferentes x e y de modo que $ax + b = 0$ e $ay + b = 0$. Isso nos dá $ax + b = ay + b$. Subtraindo b de ambos os membros, vem $ax = ay$. Como $a \neq 0$, podemos dividir ambos os membros por a, obtendo $x = y$.⇒⇐ ■

Uma questão de estilo

A prova por contradição de "Se A, então B" em geral é mais fácil do que a prova direta, porque oferece mais condições. Em vez de começarmos com a única condição A e procurarmos demonstrar a condição B, comecemos com A e (não B) conjuntamente e procuramos uma contradição. Isso nos dá mais material para trabalhar.

Às vezes, quando optamos por uma prova por contradição, podemos descobrir que tal prova realmente não era exigida, sendo possível um tipo mais simples de prova. Uma prova é uma prova, e você deve dar-se por feliz se conseguir chegar a uma prova correta. Não obstante, é sempre preferível uma forma mais simples de apresentar seu argumento. Eis como dizer se é possível simplificar uma prova do tipo "Se A, então B".

Vamos resumir os principais pontos dessa prova.

- É uma prova por contradição.
- Consideramos um contraexemplo mínimo do resultado.
- Devemos tratar como um caso especial a possibilidade mínima *extrema*.
- Descemos até um caso menor para o qual o teorema é verdadeiro, e passamos a trabalhar de volta.

Antes de passarmos a outro exemplo, terminemos a tarefa a que nos propusemos.

Corolário 20.2

Todo inteiro é ou par ou ímpar.

A ideia-chave é que ou $x \geq 0$ (quando estamos resolvidos, pela Proposição 20.1) ou $x < 0$ (caso em que $-x \in \mathbb{N}$ e podemos novamente utilizar a Proposição 20.1).

Prova. Seja x um inteiro arbitrário.

Se $x \geq 0$, então $x \in \mathbb{N}$ e, pela Proposição 20.1, x ou é par ou é ímpar.

Caso contrário, $x < 0$, e $-x > 0$, e $-x$ ou é par ou é ímpar.

- Se $-x$ é par, então $-x = 2a$ para algum inteiro a. Mas, então, $x = -2a$ para algum inteiro a. Então, $x = -2a = 2(-a)$, de modo que x é par.
- Se $-x$ é ímpar, então $-x = 2b + 1$ para algum inteiro b. Daí, temos $x = -2b - 1 = 2(-b - 1) + 1$; x é, pois, ímpar.

Em qualquer caso, x ou é par ou é ímpar. ■

O Esquema de prova 15 dá a forma geral dessa técnica.

Esquema de prova 15

Prova por contraexemplo mínimo

Primeiro, seja x um contraexemplo mínimo do resultado que estamos procurando provar. Deve ser claro que pode existir tal x.

Segundo, descarte o fato de x ser a possibilidade mínima. Esse passo (em geral fácil) é chamado passo *básico*.

Terceiro, considere uma instância x' do resultado que seja "apenas" menor que x. Utilize o fato de que o resultado é verdadeiro para x', mas falso para x para chegar a uma contradição $\Rightarrow\Leftarrow$.

Conclua que o resultado é verdadeiro. ■

Eis outra proposição que provamos utilizando o método do contraexemplo mínimo.

Exemplo 20.9

Em contraposição, consideremos o conjunto

$$Y = \{y \in \mathbb{Q} : y \geq 0, y \notin \mathbb{Z}\}$$

Na prova fictícia da Afirmação 20.5, procuramos um elemento mínimo de Y. Subsequentemente, constatamos que Y não tem elemento mínimo e que havia um erro em nossa "prova". O Princípio da Boa Ordenação se aplica a $\mathbb{N}$, mas não a $\mathbb{Q}$.

Note que chamamos o Princípio da Boa Ordenação uma *afirmação*; não o denominamos *teorema*. Por quê? A razão remonta ao começo deste livro. Poderíamos (mas não o fizemos) definir exatamente o que são os inteiros. Se enveredássemos pela difícil tarefa de dar uma definição cuidadosa dos inteiros, começaríamos definindo os números naturais. Os números naturais são definidos como um conjunto de "objetos" que satisfazem certas condições; essas condições definidoras são chamadas *axiomas*. Um desses axiomas definidores é o Princípio da Boa Ordenação. Assim, os números naturais obedecem, por definição, ao Princípio da Boa Ordenação. Há outras maneiras de definir números inteiros e naturais, e, nesses contextos, podemos provar o Princípio da Boa Ordenação. Se você estiver intrigado sobre como se faz tudo isso, recomendo-lhe um curso de fundamentos da matemática (tal curso poderia ser chamado Lógica e Teoria dos Conjuntos).

O Princípio da Boa Ordenação é um *axioma* dos números naturais.

Em qualquer caso, nossa abordagem tem sido a de supor propriedades fundamentais dos inteiros; consideramos uma dessas propriedades o Princípio da Boa Ordenação.

O Princípio da Boa Ordenação explica por que a técnica do contraexemplo mínimo funciona para provar que os números naturais não podem ser simultaneamente pares e ímpares, mas não funciona para provar que os racionais não negativos são inteiros.

O Esquema de prova 16 dá uma alternativa do Esquema de prova 15, que utiliza explicitamente o Princípio da Boa Ordenação.

Esquema de prova 16

Prova pelo Princípio da Boa Ordenação

Para provar uma afirmação sobre números naturais:

Prova. Suponhamos, por contradição, que a afirmação seja falsa. Seja $X \subseteq \mathbb{N}$ o conjunto de contraexemplos da afirmação.(Prefiro a letra X para eXceções.) Como supusemos, a afirmação falsa é $X \neq \emptyset$. Pelo Princípio da Boa Ordenação, X contém um elemento mínimo, x.

(Etapa básica.) Sabemos que $x \neq 0$, porque *mostra que o resultado vale para 0; isto em geral é fácil.*

Consideremos $x - 1$. Como $x > 0$, sabemos que $x - 1 \in \mathbb{N}$ e a afirmação é verdadeira para $x - 1$ (porque $x - 1 < x$). *A partir daqui, argumentamos para chegar a uma contradição – em geral, que x é e não é um contraexemplo da afirmação.* $\Rightarrow\Leftarrow$ ■

Esquema de prova 17

Prova por indução.

Para provar que todo número natural tem *determinada propriedade*:

Prova.

- Seja A o conjunto dos números naturais para os quais o resultado é verdadeiro.
- Prove que $0 \in A$. Isso constitui a chamada *etapa básica*. Em geral é fácil.
- Prove que, se $k \in A$, então $k + 1 \in A$. É a chamada *etapa indutiva*. Para tanto:
  - Supomos que o resultado seja verdadeiro para $n = k$. É a chamada *hipótese da indução*.
  - Use a hipótese da indução para provar que o resultado é verdadeiro para $n = k + 1$.
- Invocamos o Teorema 21.2 para concluir que $A = \mathbb{N}$.
- Portanto, o resultado é verdadeiro para todos os números naturais. ∎

Prova (da Proposição 21.3).
Provamos esse resultado por indução. Seja A o conjunto dos números naturais para os quais a Proposição 21.3 é verdadeira; isto é, os valores de n para os quais a Equação (18) se verifica.

- **Etapa básica:** Note que o teorema é verdadeiro para $n = 0$, porque ambos os membros da Equação (18) se reduzem a 0.
- **Hipótese de indução:** Suponha que o resultado seja verdadeiro para $n = k$; isto é, podemos supor

$$0^2 + 1^2 + 2^2 + \cdots + k^2 = \frac{(2k + 1)(k + 1)(k)}{6}. \tag{19}$$

- Devemos, agora, provar que a Equação (18) é válida para $n = k + 1$; isto é, devemos provar que

$$0^2+1^2+2^2+\cdots+k^2+(k+1)^2 = \frac{[2(k + 1) + 1][(k + 1) + 1][k + 1]}{6}. \tag{20}$$

- Para provar a Equação (20) com base na Equação (19), adicionamos $(k + 1)^2$ a ambos os membros da Equação (19):

$$0^2 + 1^2 + 2^2 + \cdots + k^2 + (k + 1)^2 = \frac{(2k + 1)(k + 1)(k)}{6} + (k + 1)^2. \tag{21}$$

- Para completar a prova, devemos mostrar que o membro direito da Equação (20) é igual ao membro direito da Equação (21); isto é, devemos provar que

$$\frac{(2k + 1)(k + 1)(k)}{6} + (k+1)^2 = \frac{[2(k + 1) + 1][(k + 1) + 1][k + 1]}{6}. \tag{22}$$

Deixamos a seu cargo a prova desse teorema (ver Exercício 21.14).

Por que chamamos esse teorema de indução *forte*? Suponha que estejamos utilizando a indução para provar uma proposição. Em ambos os casos de indução – padrão e forte – começamos mostrando o caso básico ($0 \in A$). Na indução-padrão, admitimos a hipótese da indução ($k \in A$; isto é, a proposição é verdadeira para $n = k$) e a aplicamos, então, para provar que $k + 1 \in A$ (isto é, a proposição é válida para $n = k + 1$). A indução forte nos dá uma hipótese mais forte de indução. Na indução forte, podemos supor $0, 1, 2, ..., k \in A$ (a proposição é verdadeira para todo n de 0 a k) e utilizar o fato para provar que $k + 1 \in A$ (a proposição é verdadeira para $n = k + 1$).

Esse método está esboçado no Esquema de prova 18.

Esquema de Prova 18

Prova por indução forte

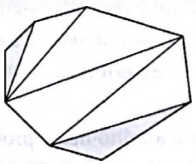
Provar que todo número natural tem *alguma propriedade*:

Prova.

- Seja A o conjunto dos números naturais para os quais o resultado é verdadeiro.
- Prove que $0 \in A$. Esta é a chamada *etapa básica*. Em geral é fácil.
- Prove que, se $0, 1, 2, ..., k \in A$, então $k + 1 \in A$. Esta é a chamada *etapa indutiva*. Para tanto,
  - Suponha o resultado verdadeiro para $n = 0, 1, 2, ..., k$. É a hipótese de *indução forte*.
  - Aplique a hipótese de indução forte para provar que o resultado é verdadeiro para $n = k + 1$.
- Invoque o Teorema 21.9 para concluir que $A = \mathbb{N}$.
- Portanto, o resultado é verdadeiro para todos os números naturais. ■

Vejamos como usar a indução forte e por que ela nos dá maior flexibilidade do que a indução-padrão. Ilustramos a prova por indução forte em um problema de geometria.

Seja P um polígono no plano. *Triangular* um polígono é traçar diagonais pelo interior do polígono de modo que (1) as diagonais não se cruzem e (2) cada região criada é um triângulo (ver figura). Note que sombreamos dois dos triângulos. Esses triângulos são chamados triângulos *exteriores*, pois dois de seus três lados situam-se no exterior do polígono original.



Provaremos o resultado seguinte usando a indução forte.

Para provar que $f: A \to B$ (isto é, para provarmos que f é uma função de A para B), usaremos o Esquema de prova 19.

Esquema de prova 19

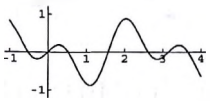
Mostrar que $f: A \to B$

Provar que f é uma função de um conjunto A para um conjunto B:

- Prove que f é uma função.
- Prove que $\text{dom } f = A$.
- Prove que $\text{im } f \subseteq B$.

Gráficos de funções

Os gráficos constituem uma forma excelente de visualizarmos funções cujas entradas e saídas são números reais. Por exemplo, a figura a seguir mostra o gráfico da função $f(x) = \text{sen } x \cos 3x$. Para traçar o gráfico de uma função, marcamos um ponto no plano das coordenadas $(x, f(x))$ para todo $x \in \text{dom } f$.



Formalmente, o *gráfico* de uma função é o conjunto $\{(x, y) : y = f(x)\}$. O interessante é que esse conjunto é a função! A função f é o conjunto de todos os pares ordenados (x, y) para os quais $y = f(x)$. Por isso, falar a respeito do "gráfico de uma função" é redundante! Isso não é ruim. Ao utilizarmos a palavra *gráfico* nesse contexto, estamos formulando uma visão geométrica da função

Os gráficos são instrumentos poderosos para entender funções definidas nos reais. Para verificar se uma ilustração representa uma função, podemos aplicar o *teste da reta vertical*. Qualquer reta vertical no plano só pode interceptar o gráfico de uma função no máximo em 1 (um) ponto. Uma reta vertical não pode cortar o gráfico duas vezes, porque então teríamos dois pontos diferentes (x, y_1) e (x, y_2), ambos no gráfico da função. Isso significaria que tanto (x, y_1) como $(x, y_2) \in f$, com $y_1 \neq y_2$. E isso está em desacordo com a definição de função.

Na matemática discreta, estamos especialmente interessados em funções para e de conjuntos finitos (ou $\mathbb{N}$ ou $\mathbb{Z}$). Em tais casos, os gráficos tradicionais de funções podem, ou não, ajudar, ou mesmo não ter sentido. Por exemplo, seja A um conjunto finito. Podemos considerar a função $f: 2^A \to \mathbb{N}$ definida por $f(x) = |x|$. (Alerta: As barras verticais nesse contexto não significam valor absoluto!) A cada subconjunto x de A, a função f faz corresponder ao seu tamanho. Não há maneira prática de representar este fato como um gráfico em eixos coordenados.

Temos uma forma alternativa para traçar gráficos de funções $f: A \to B$, em que A e B são conjuntos finitos. Sejam $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{1, 2, 3, 4, 5\}$ e consideremos a função $f: A \to B$ definida por

Linguagem matemática!

A expressão *um para um* costuma também ser escrita como 1:1. Outra designação para uma função um para um é injeção ou função *injetiva*.

A função do Exemplo 23.12 não é um para um, porque $f(1) = f(4)$, mas $1 \neq 4$. Compare detalhadamente as Definições 23.13 (um para um) e 23.1 (função). As condições são bastante semelhantes.

Proposição 23.14

Seja f uma função. A relação inversa f^{-1} é uma função se e somente se f é um para um.

Deixamos a prova como exercício (Exercício 23.10). Enquanto trabalha nela, prove também o seguinte.

Proposição 23.15

Seja f uma função e suponhamos que f^{-1} também seja uma função. Então $\text{dom}\, f = \text{im}\, f^{-1}$ e $\text{im}\, f = \text{dom}\, f^{-1}$.

Frequentemente, queremos provar que uma função é um para um. O Esquema de prova 20 dá a estratégia para provar que uma função é um para um.

Esquema de prova 20

Provar que uma função é um para um.

Mostrar que f é um para um:

Método direto: Suponhamos $f(x) = f(y)$. ... Portanto, $x = y$ e, assim, f é um para um. ■

Método pela contrapositiva: Suponhamos $x \neq y$.... Portanto, $f(x) \neq f(y)$ e, assim, f é um para um. ■

Método da contradição: Suponhamos $f(x) = f(y)$, mas $x \neq y$. ... $\Rightarrow\Leftarrow$. Portanto, f é um para um. ■

Exemplo 23.16

Seja $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = 3x + 4$. Prove que f é um para um.

Prova. Suponhamos $f(x) = f(y)$. Então $3x + 4 = 3y + 4$. Subtraindo 4 de ambos os membros, vem $3x = 3y$. Dividindo ambos os membros por 3, obtemos $x = y$. Portanto, f é um para um. ■

Em contrapartida, para provar que uma função não é um para um, devemos tipicamente apresentar um contraexemplo, isto é, um par de objetos x e y com $x \neq y$, mas $f(x) = f(y)$.

Note que $f: A \to B$ é sobre porque, para cada elemento b de B, podemos achar um ou mais elementos $a \in A$ de modo $f(a) = b$. É fácil ver também que im $f = B$.

Entretanto, $g: A \to B$ não é sobre. Note que $8 \in B$, mas não há $a \in A$ com $g(a) = 8$. Também, im $g = \{7, 9, 10\} \neq B$.

A condição de $f: A \to B$ ser sobre se expressa com auxílio dos quantificadores $\exists$ e $\forall$ como

$$\forall b \in B, \exists a \in A, f(a) = b$$

A condição de f não ser sobre se expressa como

$$\exists b \in B, \forall a \in A, f(a) \neq b$$

Essas maneiras de encarar as funções *sobre* são formalizadas no Esquema de prova 21.

Esquema de Prova 21

Provar que uma função é sobre.

Mostrar que $f: A \to B$ é sobre:

Método direto: Seja b um elemento arbitrário de B. Explique como achar/construir um elemento $a \in A$ de modo que $f(a) = b$. Portanto, f é sobre. ■

Método dos conjuntos: Mostre que os conjuntos B e im f são iguais. ■

Exemplo 23.20

Seja $f: \mathbb{Q} \to \mathbb{Q}$ dada por $f(x) = 3x + 4$. Prove que f é sobre $\mathbb{Q}$.

Prova. Seja $b \in \mathbb{Q}$ arbitrário. Procuramos um $a \in \mathbb{Q}$ de modo $f(a) = b$. Seja $a = \frac{1}{3}(b - 4)$. (Como b é um número racional, também o é a.) Note que

$$f(a) = 3\left[\tfrac{1}{3}(b-4)\right] + 4 = (b-4) + 4 = b$$

Portanto, $f: \mathbb{Q} \to \mathbb{Q}$ é sobre. ■

Tenha em mente que $\mathbb{Q}$ representa o conjunto dos números racionais.

Como conseguimos "adivinhar" que deveríamos tomar $a = \frac{1}{3}(b - 4)$? Na realidade, não supusemos. Trabalhamos em sentido contrário!

Seja $f: A \to B$. Para que f^{-1} seja uma função, é necessário e suficiente que f seja um a um. Dado isso, para que $f^{-1}: B \to A$, é necessário que f seja sobre B. Caso contrário, se f não é sobre B, podemos achar um $b \in B$ de modo $f^{-1}(b)$ não esteja definida.

Teorema 23.21

Sejam os conjuntos A e B e $f: A \to B$. A relação inversa f^{-1} é uma função de B para A se e somente se f é um para um e sobre B.

Portanto, $(g \circ f) \neq (f \circ g)$

Mais geralmente,

$$\begin{aligned}(g \circ f)(x) &= g[f(x)] = g[x^2 + 1] \\ &= 2[x^2 + 1] - 3 = 2x^2 - 1 \quad \text{e}\end{aligned}$$

$$\begin{aligned}(f \circ g)(x) &= f[g(x)] = f[2x - 3] \\ &= [2x - 3]^2 + 1 \\ &= 4x^2 - 12x + 10\end{aligned}$$

Portanto, $g \circ f \neq f \circ g$

Assim, a composição de funções não satisfaz a propriedade comutativa. Verifica-se, entretanto, a propriedade associativa.

Proposição 25.6

Sejam os conjuntos A, B, C e D e sejam $f: A \to B$, $g: B \to C$ e $h: C \to D$. Então,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Essa proposição afirma que duas funções $h \circ (g \circ f)$ e $(h \circ g) \circ f$ são a mesma função. Antes de começarmos a prova, façamos uma pausa. Como provamos que duas funções são a mesma função? Podemos voltar aos fundamentos e recordar que funções são relações e, por sua vez, relações são conjuntos de pares ordenados. Podemos, então, seguir o Esquema de prova 5 para mostrar que os conjuntos são iguais.

Entretanto, é mais simples mostrarmos que as duas funções têm o mesmo domínio e que, para cada elemento em seu domínio comum, geram o mesmo valor. Isso implica que os dois conjuntos são o mesmo (ver Exercício 25.2). Esses fatos estão resumidos no Esquema de prova 22.

Esquema de prova 22

Provar que duas funções são iguais.

Sejam as funções f e g. Para provar que $f = g$, devemos fazer o seguinte:

- Provar que dom f = dom g.
- Provar que, para todo x em seu domínio comum, $f(x) = g(x)$.

Passamos agora à prova da Proposição 25.6.

Prova. Sejam $f: A \to B$, $g: B \to C$ e $h: C \to D$. Pretendemos provar que $h \circ (g \circ f) = (h \circ g) \circ f$.

Em primeiro lugar, verificamos que os domínios de $h \circ (g \circ f)$ e de $(h \circ g) \circ f$ coincidem. Já havíamos notado que dom $(g \circ f)$ = dom f. Aplicando esse fato à situação em curso, temos

$\otimes$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

Os inversos dos elementos neste $\mathbb{Z}_{14}^*$ podem ser achados nessa tabela. Temos:

$$1^{-1} = 1 \quad 3^{-1} = 5 \quad 5^{-1} = 3$$
$$9^{-1} = 11 \quad 11^{-1} = 9 \quad 13^{-1} = 13$$

Proposição 39.15

Seja n um inteiro positivo. Então, $(\mathbb{Z}_n^*, \otimes)$ é um grupo.

Para provarmos que $(G, *)$ é um grupo, precisamos verificar a Definição 39.10. Vamos resumir esse problema no Esquema de prova 23.

Esquema de Prova 23

Provar que (G, $*$) é um grupo

Para provar que $(G, *)$ é um grupo:

- Prove que G é fechado sob $*$: sejam $g, h \in G$,..., portanto, $g * h \in G$.
- Prove que $*$ é associativa: sejam $g, h, k \in G$, ..., portanto, $g * (h * k) = (g * h) * k$.
- Prove que G contém um elemento identidade para $*$: seja e um elemento específico de G. Seja $g \in G$ arbitrário,... Portanto, $g * e = e * g = g$.
- Prove que todo elemento de G tem um $*$-inverso em G: seja $g \in G$. Construa um elemento h de modo que $g * h = h * g = e$.

Portanto, $(G, *)$ é um grupo. ■

Prova (da Proposição 39.15).

Primeiro, provamos que $\mathbb{Z}_n^*$ é fechado sob $\otimes$. Sejam $a, b \in \mathbb{Z}_n^*$. Devemos provar que $a \otimes b \in \mathbb{Z}_n^*$. Recorde-se de que $a \otimes b = (ab) \bmod n$.

Sabemos que $a, b \in \mathbb{Z}_n^*$. Isso significa que a e b são relativamente primos com n. Portanto, pelo Corolário 35.9, é possível acharmos inteiros x, y, z, w de modo que

$$ax + ny = 1 \quad \text{e} \quad bw + nz = 1$$

Multiplicando essas equações uma pela outra, vem

$$\begin{aligned} 1 = (ax + ny)(bw + nz) &= (ax)(bw) + (ax)(nz) + (ny)(bw) + (ny)(nz) \\ &= (ab)(wx) + (n)[axz + ybw + ynz] \\ &= (ab)(X) + (n)(Y) \end{aligned}$$

$\{0\}$	$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
$\{0, 5\}$	$\{0, 2, 4, 6, 8\}$

Em todos os quatro casos a operação é $\oplus$.

A solução do Exemplo 41.2 está correta? Há dois pontos a considerar:

- Para cada um dos quatro subconjuntos H que relacionamos, $(H, \oplus)$ é um grupo?
- Há outros subconjuntos $H \subseteq \mathbb{Z}_{10}$ que tenhamos deixado de incluir?

Consideremos essas duas questões, uma de cada vez.

Se $(G, *)$ é um grupo e $H \subseteq G$, como podemos determinar se $(H, *)$ for um subgrupo?

A Definição 41.1 nos diz o que fazer. Primeiro, devemos nos certificar de que $H \subseteq G$. Segundo, devemos ter a certeza de que $(H, *)$ é um grupo. Para tanto, a maneira mais direta consiste em verificar que $(H, *)$ satisfaz as quatro condições listadas na Definição 39.10: fechamento, associatividade, identidade e inversos.

Para verificar o fechamento, devemos provar que, se $g, h \in H$, então $g * h \in H$. Por exemplo, os inteiros pares formam um subgrupo de $(\mathbb{Z}, +)$, mas os inteiros ímpares não, pois não verificam a propriedade do fechamento; se g e h são inteiros ímpares, $g + h$ não é ímpar.

Em seguida, não precisamos verificar a associatividade. Releia a sentença! Escrevemos: *não* precisamos verificar a associatividade. Sabemos que $(G, *)$ é um grupo e que, portanto, $*$ é associativa em G; isto é, $\forall g, h, k \in G, g * (h * k) = (g * h) * k$. Como $H \subseteq G$, devemos ter que $*$ já é associativa em H. Obtemos de graça a associatividade!

Em seguida, verificamos se o elemento identidade está em H. Essa etapa é fácil, em geral.

Por fim, sabemos que todo elemento de H tem um inverso (porque todo elemento de $G \supseteq H$ tem um inverso). O problema consiste em, se $g \in H$, mostrar que $g^{-1} \in H$.

Essas etapas para provar que um subconjunto de um grupo é um subgrupo estão relacionadas no Esquema de prova 24.

Esquema de prova 24

Provar que um subconjunto de um grupo é um subgrupo.

Seja $(G, *)$ um grupo e seja $H \subseteq G$. Para provar que $(H, *)$ é um subgrupo de $(G, *)$:

- Prove que H é fechado sob $*$ (isto é, $\forall g, h \in H, g * h \in H$).

  "Sejam $g, h \in H$... Portanto, $g * h \in H$."
- Prove que e (o elemento identidade para $*$) está em H.
- Prove que o inverso de todo elemento de H está em H (isto é, $\forall h \in H, h^{-1} \in H$).
- "Seja $h \in H$... Portanto, $h^{-1} \in H$."

Reconsideremos agora a questão: os quatro subconjuntos do Exemplo 41.2 são realmente subgrupos de $(\mathbb{Z}_{10}, \oplus)$? Vamos verificá-los todos.

Uma recíproca dessa afirmação também é verdadeira; deixamos a prova a seu cargo, como exercício (Exercício 49.7).

Prova. Devemos provar que $T - v$ é uma árvore. Obviamente, $T - v$ é acíclico. Se $T - v$ contivesse um ciclo, esse ciclo também existiria em T. Devemos, pois, mostrar que $T - v$ é conexo.

Seja $a, b \in V(T - v)$. Devemos mostrar que existe um caminho (a, b) em $T - v$. Sabemos que, embora T seja conexo, existe um caminho (a, b) P em T. Afirmamos que P não inclui o vértice v. Em caso contrário, teríamos

$$P = a \sim \ldots \sim v \sim \ldots \sim b$$

e, como v não é o primeiro nem o último vértice nesse caminho, tem dois vizinhos distintos no caminho, o que contradiz o fato de que $d(v) = 1$. Portanto, P é um caminho (a, b) em $T - v$ e, assim, $T - v$ é conexo e é uma árvore. ■

A Proposição 49.8 constitui a base de uma técnica de prova para árvores. Muitas provas sobre árvores são feitas por indução sobre o número de vértices. O Esquema de prova 25 dá a forma básica de tal prova.

Vamos demonstrar esta técnica de prova para o resultado a seguir.

Teorema 49.9

Seja T uma árvore com $n \geq 1$ vértices. Então, T tem $n - 1$ arestas.

Esquema de prova 25

Prova de teoremas sobre árvores por supressão de folhas

Provar: Alguns teoremas sobre árvores.

Prova. Provamos o resultado por indução sobre o número de vértices em T.

Caso básico: Afirmar que o teorema é verdadeiro para todas as árvores com $n = 1$ vértices. Isso deve ser fácil!

Hipótese de indução: Supor que o teorema seja verdadeiro para todas as árvores em $n = k$ vértices.

Seja T uma árvore em $n = k + 1$ vértices. Sejam v uma folha de T e $T' = T - v$. Note que T' é uma árvore com k vértices, de forma que, por indução, T' satisfaz o teorema.

Utilizamos, agora, o fato de que o teorema é verdadeiro para T' para, de alguma forma, provar que a conclusão do teorema é válida para T. Isso pode ser enganoso.

Prova-se o resultado por indução. ■

Recorremos ao Gabarito de prova 25 para provar esse resultado.

Prova. Provamos o Teorema 49.9 por indução sobre o número de vértices em T.