Elementos de Matemática

Leandro F. Aurichi [1]

2 de dezembro de 2016

[1]Instituto de Ciências Matemáticas e de Computação - Universidade de São Paulo, São Carlos, SP

Sumário

Capítulo 1

Rudimentos de lógica

1.1 Introdução

Primeiramente, vejamos a diferença entre provar e convencer. Quando damos um argumento do porque algo vale, em geral, estamos tentando convencer alguém de que o que dizemos é verdade. Mas há espaço para discussão. No momento em que provamos determinada coisa, tal espaço inexiste. Em geral, numa prova (demonstração), assumimos algo como verdade e depois deduzimos outras afirmações. A grande diferença entre convencer e provar é que enquanto no "convencer" muitos dos passos são passíveis de discussão, numa demonstração apenas o que assumimos como verdade é passível disso. Vejamos um exemplo (conhecido como **silogismo**):

Um silogismo basicamente é a obtenção de uma conclusão a partir de duas premissas.

Exemplo 1.1.1.

- Todo homem é mortal;
- Sócrates é um homem;
- Logo, Sócrates é mortal.

Examinemos um pouco mais de perto tal construção. As duas primeiras afirmações (que chamaremos de premissas ou hipóteses) é o que assumimos como verdade. A última é chamada de conclusão. Podemos até discutir se as duas primeiras afirmações são verdadeiras ou não. Mas uma vez que supomos as duas como verdadeiras, não há outra opção para a conclusão a não ser que ela seja verdadeira também. Note também que nada precisamos assumir (ou saber) sobre os termos "homem", "mortal" ou mesmo "Sócrates". Isto é, seguindo essa estrutura, podemos criar outras tentativas de provas:

A ideia aqui é que o silogismo estar certo ou não, não depende de fatores externos a ele - por exemplo, não faz diferenção se as premissas são verdadeiras ou não.

Exemplo 1.1.2.

- Nenhum cachorro voa;
- Snoopy é um cachorro;
- Logo, Snoopy não voa.

Exemplo 1.1.3.

- Todo pássaro é amarelo;
- Todo papagaio é um pássaro;
- Todo papagaio é amarelo.

A conclusão do último silogismo é claramente falsa. Mas isso não é um problema do desenvolvimento do silogismo, mas sim do fato que a primeira hipótese também é falsa. O que se tenta criar com os silogismos é uma maneira em que o único jeito de se obter uma afirmação falsa seja assumindo como verdade uma outra afirmação falsa. Ou seja, nesse exemplo obtemos como conclusão uma afirmação falsa ("Todo papagaio é amarelo") porque uma das nossas hipóteses era falsa ("Todo pássaro é amarelo"). De qualquer forma, do ponto de vista de estrutura, tal silogismo está correto: duas hipóteses e uma conclusão que decorre delas. O caso é diferente nos próximos exemplos:

Exemplo 1.1.4.

- Alguns cachorros são pretos;
- Snoopy é um cachorro;
- Logo, Snoopy é preto.

Exemplo 1.1.5.

- Algumas flores são vermelhas;
- Sócrates é um homem;
- Logo, Snoopy é um cachorro.

O problema com o primeiro silogismo é que tentamos derivar a partir de que alguns cachorros são pretos que algum determinado é preto. Isso não é verdade. Se só sabemos que alguns são pretos, ao tomarmos um exemplo em particular, não podemos concluir que ele necessariamente é preto. Podem ser verdadeiras simultaneamente as frases "Alguns cachorros são pretos", "Snoopy é um cachorro" e "Snoopy não é preto". É diferente no caso do Exemplo **1.1.1**, onde derivamos que a partir de "todos", um exemplo em particular tinha determinada propriedade.

O problema no segundo silogismo é que as hipóteses e a conclusão nada dizem uma sobre as outras. Ou seja, tais frases podem ser verdadeiras ou falsas em conjunto.

Um dos problemas com silogismos é que eles são feitos em linguagem corriqueira (no nosso caso, em Português). Isso muitas vezes pode ocasionar problemas como no próximo exemplo:

Exemplo 1.1.6.

- Quanto mais queijo suiço, mais buracos há nele;
- Quanto mais buracos houver num pedaço de queijo, menos queijo há em tal pedaço;
- Logo, quanto mais queijo, menos queijo.

Exemplo 1.1.7.

- Todo cavalo raro é caro;
- Um cavalo barato é raro;
- Logo, um cavalo barato é caro.

Tais exemplos são exemplos de **sofismas**, que é algo em que aparentemente as regras lógica foram seguidas mas a conclusão é claramente falsa. O grande problema aqui é o uso da linguagem corriqueira. Se tentarmos dar um caráter mais formal (veremos mais adiante como fazer isso) aos conceitos de "mais", "menos", "caro", "barato" e "raro" que aparecem em tais exemplos, veremos que teremos problemas. Uma maneira de contornarmos tal problema é abandonar a linguagem corriqueira e usarmos uma linguagem própria, onde não sobre espaço para interpretações. Veremos como fazer isso nas próximas seções.

Para finalizar esta seção, terminamos mostrando como a linguagem coloquial não é adequada para desenvolver demonstrações. Considere a seguinte frase:

"Esta afirmação é falsa"

Note que não há como dizer que esta afirmação é verdadeira ou falsa, uma vez que se a considerarmos verdadeira, ela se diz falsa. E se a considerarmos falsa, teremos que ela é verdadeira. Tal problema ocorre porque tal frase faz uma **autorreferência**. Isso será algo a ser evitado quando formalizarmos nossa ideia de demonstração.

O problema com autorreferência é que ela nem sempre é explícita. Por exemplo, considere N o conjunto de todos os números naturais em podem ser descritos com até 100 palavras em Português. Por, exemplo, 1 pertence a esse conjunto (a palavra "um" atesta isso). E também 10^{1000} já que "10 elevado a mil" também atesta. Mas note que a quantidade de palavras é finita e que, portanto, as possiveis combinações destas finitas palavras em grupos de 100 também é finito. Ou seja, o conjunto N claramente é finito e, portanto, diferente de $\mathbb{N}$ - o conjunto de todos os naturais. Dessa forma, podemos tomar n como "o menor elemento que não está em N". O que, traduzindo, pode ser escrito como "o menor elemento que não pode ser descrito com menos de 100 palavras". Note que, desta forma, acabamos de descrever n com menos de 100 palavras e portanto ele está em N.

Alongamentos

Alongamento 1.1.8. Para tentar resolver o problema do queijo, tente ver que um dos "mais" indica um sentido absoluto, enquanto o outro indica um sentido relativo (numa conotação de densidade). Tente deixar as frases mais específicas de forma a deixar clara a falha do silogismo.

Exercícios

Exercício 1.1.9. Numa ilha existem duas portas, cada uma vigiada por um guardião. Uma porta vai para o céu e a outra vai para o inferno. Sabe-se também que um dos guardiões sempre fala a verdade e que o outro sempre fala a mentira (mas não se sabe quem guarda qual porta). Supondo que você queira ir para o céu e que só tem direito a fazer uma pergunta aos guardiões (uma para ambos, não para cada), que pergunta fazer para descobrir qual a porta certa?

1.2 Proposições e tabelas verdade

Vamos começar a ver agora como representar afirmações usando uma simbologia mais apropriada. Começamos simplesmente trocando as afirmações por letras. Isso, entre outras vantagens, vai nos ajudar a ver quais coisas seguem da estrutura com que estamos mexendo, já que o que cada afirmação quer dizer fica de lado.

É preciso deixar claro que o que veremos aqui é um enfoque bastante simplificado. Para quem tiver curiosidade sobre o assunto, recomendamos [3] sobre esse assunto.

Vamos começar com o que vem a ser uma **proposição simples**. Intuitivamente, ela é uma afirmação qualquer que possui sentido por si só. O melhor é explicar por exemplos:

Exemplo 1.2.1. "Existe um cachorro branco" é uma proposição simples, assim como "$7 > 4$", "o Sol é uma estrela" ou mesmo "$5 > 10$". Note que não pedimos que uma proposição seja verdadeira.

Por outro lado, "camisa" não é uma proposição simples, já que ela não afirma nada sobre coisa alguma.

As proposições simples representaremos por letras, normalmente $p, q, r...$ De posse das proposições simples, vejamos o que é uma **proposição composta**. Esta nada mais é do que uma ou mais proposições (simples ou já compostas) utilizando-se pelo menos um **conectivo**. Os conectivos comumente usados são (mas outros podem ser utilizados também):

- $\sim$ (negação);
- $\wedge$ (e);
- $\vee$ (ou);
- $\rightarrow$ (implicação);
- $\leftrightarrow$ (bi-implicação).

Por exemplo, se p e q são proposições, então $p \vee q$ também é. Assim como $p \rightarrow q$ ou $\sim q$. No caso em que já temos proposições compostas, utiliza-se parênteses para evitar ambiguidades. Por exemplo, $(p \vee q) \wedge (\sim s)$. Mas qual a interpretação que devemos dar a esses conectivos? A negação serve para quando queremos o contrário de uma afirmação. Isto é, $\sim p$ é verdadeira se, e somente se, p é falsa. O conectivo $\wedge$ serve para indicar que ambas as

proposições devem ser verdadeiras. Isto é, $p \wedge q$ é verdadeira se, e somente se, p e q são verdadeiras simultaneamente.

Um jeito fácil de definir um conectivo é por meio de uma **tabela verdade**. Vejamos os dois exemplos anteriores:

p	$\sim p$
V	F
F	V

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Nas primeiras colunas, estão indicados todos os possíveis valores de p e q, enquanto na última, indicamos os correspondentes valores com o conectivo. Note que, de fato, $p \wedge q$ só é verdadeira quando ambas p e q o são também. Vejamos o conectivo $\vee$. Queremos que $p \vee q$ só seja falso quando ambos p e q forem falsos, isto é, basta um deles ser verdadeiro para que $p \vee q$ seja verdadeiro (veja nos exercícios sobre outra intepretação de "ou", que chamaremos de "ou exclusivo"). Assim, a tabela fica

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

A tabela da bi-implicação também é simples, basta que os valores de p e q sejam idênticos para que a bi-implicação seja verdadeira:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Já a implicação muitas vezes causa confusão. Quando que a implicação $p \rightarrow q$ é verdadeira? Neste caso, é mais fácil pensar quando ela é falsa. Ela só é falsa no caso em que p é verdadeiro e q é falso. De modo que todos os outros casos são verdadeiros. Assim, a tabela fica:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

Note que as duas últimas linhas da tabela podem causar estranhamento. Mas um argumento em favor delas é "se p é falsa, então não importa o que aconteça com q, ainda temos que $p \to q$".

Tabelas verdade não precisam conter apenas um conectivo, nem precisam ter apenas ter 3 colunas. Muitas vezes diversas colunas nos ajudam a encontrar quando uma certa proposição composta é verdadeira ou não. Por exemplo:

Exemplo 1.2.2.

p	q	$\sim q$	$p \wedge (\sim q)$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	V	F

Observe o seguinte exemplo:

Exemplo 1.2.3.

p	q	$p \to q$	$(\sim q) \to (\sim p)$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Note que as duas últimas colunas são idênticas. Nesse caso, dizemos que $(p \to q)$ e $((\sim q) \to (\sim p))$ são **equivalentes**. Isto é, elas tem o mesmo comportamento, não importa quais os valores de p e q. Num certo sentido, escrever a primeira proposição é o mesmo que escrever a segunda.

Vejamos mais um exemplo de equivalência:

Exemplo 1.2.4.

p	q	$p \to q$	$(\sim p) \vee q$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Terminamos esta seção com um outro tipo de proposição:

Exemplo 1.2.5.

p	$\sim p$	$p \vee (\sim p)$
V	F	V
F	V	V

Note a última coluna. Não importa se p é verdade ou não, $p \vee (\sim p)$ é sempre verdade. Proposições que são sempre verdadeiras, independente de seus significados, são ditas **tautologias**.

Alongamentos

Alongamento 1.2.6. Faça a tabela verdade do **ou exclusivo**, isto é, $p \dot{\vee} q$ é verdadeiro caso p ou q sejam verdadeiros mas não ambos ao mesmo tempo.

Alongamento 1.2.7. Construa uma tabela verdade para cada uma das proposições abaixo:

(a) $p \vee (p \wedge q)$;

(b) $p \to (\sim q)$;

(c) $\sim (p \to q)$;

(d) $p \vee (q \vee r)$;

(e) $p \to (q \to r)$.

Exercícios

Exercício 1.2.8. Sejam a, b e c números reais. Vamos considerar as seguintes afirmações p, q, r, s, t e u:

- p: $a > b$
- q: $a < b$
- r: $a < c$
- s: $a > c$
- t: $b < c$
- u: $b > c$.

Use conectivos para compor essas proposições de forma a obter uma que signifique:

As proposições obtidas não vão seguir diretamente das afirmações aqui - para obter a interpretação correta, você pode usar coisas como "se x, y são reais, então $x \leq y$ ou $y \leq x$".

(a) $a = b$;

(b) $a \neq b$;

(c) $a \geq b$;

(d) $a < b < c$;

(e) c está entre a e b e é diferente de ambos.

Exercício 1.2.9. Escreva uma proposição equivalente a $p \wedge q$ só usando os seguintes símbolos: $p, q, \sim, \vee$ e parênteses.

Exercício 1.2.10. Mostre que proposição $(p \to q) \leftrightarrow ((\sim p) \vee q)$ é uma tautologia.

Exercício 1.2.11. Um conectivo é dito binário se ele recebe duas proposições (por exemplo, $\wedge$ e $\vee$ são binários, enquanto $\sim$ é unário - pois só recebe uma proposição). Quantos conectivos binários não equivalentes entre si podem ser definidos?

1.3 Quantificadores

Com o que fizemos até agora, não trabalhamos com muita comodidade sobre frases do tipo "todos os cachorros são brancos" ou "existe pelo menos um pássaro amarelo". Nossa única escolha seria tratar tais frases como proposições simples. O problema aparece quando tentamos usar os conectivos. Vamos a um exemplo para mostrar um dos possíveis problemas. Suponha que numa fazenda só existam vacas pretas e vacas brancas. Suponha que temos duas proposições:

- p: "todas as vacas são pretas";
- q: "todas as vacas são brancas".

Como construir uma proposição que indique o que há na fazenda a partir destas duas? Na linguagem coloquial, apareceu um "e". Mas se tentamos usar $p \wedge q$, obtemos uma proposição que diz que todas as vacas são pretas e brancas (malhadas?). Não é o que queremos. Se tentamos usar o $\vee$, temos ainda outro significado. $p \vee q$ quer dizer que todas as vacas são pretas ou

que todas as vacas são brancas. Ou seja, isso só é verdade se todas as vacas forem pretas, ou se todas as vacas forem brancas (ou se todas forem brancas e pretas ao mesmo tempo). Novamente, não é isso que gostaríamos. Vamos mostrar aqui um método que faz com que os "quantificadores" (todos, algum, nenhum etc.) tenham um comportamento parecido com os conectivos, isto é, que possamos trabalhar com eles mesmo sem nos preocuparmos com seus significados.

Os quantificadores com os quais trabalharemos são dois $\exists$ (existe) e $\forall$ (para todo). Para usar quantificadores, precisamos da noção de variável. Variável fará o papel do objeto em nossas proposições, podendo representar números, conjuntos, vacas etc. Usaremos letras para variáveis, por exemplo x, y, z, mas muitas vezes usaremos letras indexadas, como v_1, v_2 etc. Comecemos com um exemplo. Considere a frase "x é branco". Por enquanto, não temos ideia do que x possa ser, então não temos como dizer se tal frase é verdadeira ou não. Vejamos como fica depois do uso de um quantificador "$(\forall x$ x é branco)". Se combinarmos que nossas variáveis podem representar as vacas de nosso exemplo, esta frase é lida como "todas as vacas são brancas". O que, no nosso exemplo, é falso. Vamos usar uma notação um pouco mais simbólica. A frase "x é branco", indica uma propriedade sobre x (ainda que não saibamos o que x possa ser). E x é a única variável nessa frase. Assim, vamos indicar "x é branco" por $B(x)$. Desta forma, a frase acima fica $(\forall x\ B(x))$. Podemos indicar também a frase "x é preto" por $P(x)$. Desta forma, podemos tratar $B(x)$ e $P(x)$ como proposições e trabalhar como fizemos na seção anterior, isto é, utilizar os conectivos. Qual a ideia do sentido de $\forall x$? Ele significa que para qualquer x que tomarmos, a proposição que vem a seguir deve ser verdadeira. Assim, se x representa uma vaca, para que a frase original seja verdadeira devemos exigir que valha $B(x) \vee P(x)$ (note que não é $B(x) \wedge P(x)$ - nesse caso teríamos que cada x, isto é, que cada vaca, fosse branca e preta ao mesmo tempo). Assim, nossa frase em notação simbólica fica $(\forall x(B(x) \vee P(x)))$. Aproveitando o exemplo, para dizer que há pelo menos uma vaca branca, podemos escrever $(\exists x\ B(x))$.

Resumindo, temos:

- $(\forall x\ A(x))$ quer dizer que, para cada valor para x, a afirmação $A(x)$ é verdadeira;
- $(\exists x\ A(x))$ quer dizer que há pelo menos um valor para x de forma que $A(x)$ seja verdadeira.

Note que o $A(x)$ pode ser algo "composto" como $(B(x) \vee P(x))$.

Exemplo 1.3.1. Considere as seguintes propriedades sobre números reais:

- $P(x)$ dada por "$x \geq 0$";
- $N(x)$ dada por "$x \leq 0$".

Se queremos dizer que há um número real positivo (não estrito), podemos simplesmente escrever $(\exists x\ P(x))$. Se queremos dizer que todo número real é positivo ou negativo, podemos dizer $(\forall x\ (P(x) \vee N(x)))$. Se quisermos dizer que existe um que é positivo e negativo ao mesmo tempo (o 0 tem essa propriedade), podemos dizer $(\exists x(P(x) \wedge N(x)))$. Podemos também dizer que todo número que não for negativo é positivo: $(\forall x((\sim N(x)) \rightarrow P(x)))$.

É claro que podemos usar conectivos em fórmulas que já possuam quantificadores. Fazemos isso mantendo os mesmos valores de verdadeiro ou falso que apresentamos na seção anterior. Por exemplo: $(\forall x P(x)) \vee (\forall y B(y))$ só é verdade se for verdade que todos os valores de x satisfazem $P(x)$ ou que todos os valores de y satisfazem $B(y)$ ou ambas as coisas.

Podemos também quantificar sobre fórmulas já quantificadas. Para isso, precisaremos de propriedades sobre mais de uma variável. Façamos um exemplo. Considere a propriedade sobre x, y dada por $M(x, y)$ significa $x > y$. Se x, y vão simbolizar números reais, precisamos dizer quais exatamente: se algum, se todos etc. Começamos com a seguinte fórmula $(\exists x M(x, y))$. Com isso que queremos dizer que algum x é maior que y. Mas qual o valor de y? Resolvemos isso com o uso de outro quantificador. Vejamos algumas possibilidades:

(a) $(\exists y(\exists x M(x, y)))$;

(b) $(\forall y(\forall x M(x, y)))$;

(c) $(\exists y(\forall x M(x, y)))$;

(d) $(\forall y(\exists x M(x, y)))$;

(e) $(\forall x(\exists y M(x, y)))$;

Vejamos o significado de cada uma das fórmulas acima. (a) simplesmente diz que há um y e um x de forma que $x > y$. E, de fato, tal frase é verdadeira (basta tomarmos $x = 1$ e $y = 0$). Já (b) diz que para qualquer y e qualquer x que tomarmos, teremos que $x > y$. Essa frase é falsa, pois para ser verdadeira deveria valer para qualquer valor de x e y que tomássemos (e ela é falsa se tomarmos $x = 0$ e $y = 1$). O item (c) significa que existe algum

y que é menor que qualquer x (o que é falso), enquanto que o item (d) diz que para qualquer y que tomarmos, existe algum x que é maior que y (que é verdade). Note que a única diferença entre o item (e) e o item (c) é a ordem em que os quantificadores foram colocados. Mas isso apresenta diferença de significado. O item (e) diz que para todo x, existe um y que é menor que ele (o que é verdade, ao contrário do que diz o item (c)).

A negação de quantificadores costuma causar um pouco de confusão. Considere a fórmula

$$(\forall x P(x))$$

Estamos afirmando que todo x satisfaz a propriedade P. Então o que significa

$$\sim (\forall x P(x))?$$

Simplesmente ela quer dizer que não é verdade que todo x satisfaz a propriedade P. Isto é, que é verdade que

$$(\exists x(\sim P(x)))$$

O que é muito diferente de

$$(\forall x(\sim P(x)))$$

que simplesmente diz que todos os valores de x não satisfazem P. Por outro lado, dizer que

$$\sim (\exists x P(x))$$

é o mesmo que afirmar que não é verdade que algum x satisfaz a propriedade P. Isto é, para qualquer valor de x, $P(x)$ não é satisfeito. Isto é, tal afirmação é equivalente a

$$(\forall x(\sim (P(x))))$$

Ou seja, para negar um quantificador basta "trocar o mesmo e negar o que vem depois". Vamos aplicar isso nos próximos exemplos:

Exemplo 1.3.2. Comecemos com a negação a da seguinte fórmula[1]

$$(\forall x(\exists y(x < y)))$$

Vamos utilizar o método descrito acima, sem nos preocupar com o sinificado. Ou seja, começamos escrevendo a negação da fórmula:

$$\sim (\forall x(\exists y(x < y)))$$

[1]Vamos escrever as propriedades necessárias já dentro das fórmulas, para facilitar a leitura. Se tiver dificuldades, escreva-as separadamente como vínhamos fazendo.

Daí negamos o primeiro quantificador (o segundo fica "aguardando"):

$$(\exists x(\sim (\exists y(x < y))))$$

Agora negamos o segundo:

$$(\exists x(\forall y \ \sim (x < y)))$$

Ou seja, nossa primeira fórmula significava que "para todo x existe um y que é maior que ele". Negando isso, obtemos pelo método acima descrito uma fórmula que significa "existe um x que para qualquer y que tomamos, não é verdade que $x < y$". Note que, de fato, a última afirmação descreve exatamente o contraexemplo necessário para dizer que a afirmação original era falsa.

Exercícios

Exercício 1.3.3. Considere as seguintes propriedades sobre cachorros:

- $B(x)$, "x é branco";
- $P(x)$, "x é preto";
- $R(x)$, "x é rápido";

Só utilizando as propriedades acima, quantificadores e conectivos, escreva fórmulas que afirmem:

(a) Há pelo menos um cachorro branco;

(b) Todo cachorro preto é rápido.

(c) Nenhum cachorro branco é rápido.

(d) Negue a fórmula obtida no item (a). O que ela quer dizer?

Exercício 1.3.4. Escreva a fórmula que diz que a função $f : \mathbb{R} \longrightarrow \mathbb{R}$ é contínua no ponto x_0 só usando símbolos.

1.4 Axiomas e Demonstrações

Informalmente, uma demonstração é uma sequência de afirmações, sendo que cada uma é consequência das anteriores ou é algo sabidamente verdadeiro. Vamos examinar isso mais de perto. Como dizer que algo é consequência de outras coisas? Para não deixar dúvidas, deixaremos claro o

que entendemos por isso. Diremos que B é consequência de afirmações anteriores se dentre as anteriores tivermos uma afirmação do tipo A e uma do tipo $A \to B$. Tal regra é comumente resumida da seguinte forma:

Essa regra é conhecida como *modus ponens*. Veja o Exercício 1.4.11

$$\frac{A \qquad A \to B}{B}$$

A interpretação disso é "se sabemos que A vale e que toda vez que A vale, B vale, então B vale".

Formalmente, precisamos de mais regras que envolvem substituição de variáveis. Por exemplos, precisamos poder deduzir $\forall x \ P(x)$ a partir de $\forall y \ P(y)$ - mas não seremos tão formais neste texto.

Exemplo 1.4.1. Vamos mostrar que $A \to B$ e $B \to C$ implicam que $A \to C$. O que queremos mostrar é que toda vez que ocorre A, ocorre C. Isso, quando vale tanto $A \to B$ como $B \to C$. Isto é, vamos assumir que valem A, $A \to B$ e $B \to C$ e ver se conseguimos mostrar que vale C. Do fato que A e $A \to B$ valem, temos que B vale. Do fato que B e $B \to C$ valem, temos que vale C. Ou seja, obtemos o que desejávamos.

Mas e a parte do "sabidamente verdadeiro"? O que algumas pessoas acham que é verdadeiro, outras podem achar que não é. Assim, teremos que ser bastante precisos com o que podemos supor verdadeiro ou não. Primeiramente, é claro que podemos supor verdadeiras tudo o que for logicamente verdadeiro, como as tautologias - lembre que elas são verdadeiras independentemente de qualquer coisa. Mas e o resto? O resto é o que vamos chamar de axiomas.

Um **axioma** é uma afirmação que vamos supor verdadeira. O uso disso em geral é o seguinte: queremos definir uma determinada coisa, dizemos quais os axiomas que isso satisfaz e daí deduzimos tudo o que podemos a partir de tais axiomas. Ou seja, tudo aquilo que satisfizer tais axiomas, vai satisfazer suas consequências também. Vamos dar a seguinte definição como exemplo:

Definição 1.4.2. Dizemos que uma relação $\preceq$ é uma **relação de ordem** sobre um conjunto A se são satisfeitas as seguintes condições[2]:

(a) $\forall a \in A \ (a \preceq a)$ (reflexiva);

(b) $\forall a \in A \ \forall b \in A \ (a \preceq b \wedge b \preceq a) \to a = b$ (antissimétrica);

[2]Vamos começar a usar quantificacores "restritos", isto é, em vez de dizer $\forall x$, diremos $\forall x \in X$. A leitura é simplesmente "para todo x que for elemento de X temos...". Uma maneira de formalizar isso seria toda vez escrever "$\forall x((x \in X) \to ...$", mas isso deixaria a leitura mais complicada. Deixaremos de lado também alguns parênteses quando isso não gerar dúvidas

(c) $\forall a \in A\ \forall b \in A\ \forall c \in A((a \preceq b \wedge b \preceq c) \to a \preceq c)$ (transitiva).

Os itens (a), (b) e (c) são os axiomas de ordem. Para dizermos que uma determinada relação é uma ordem, ela tem que satisfazer tais axiomas. Por outro lado, tudo que provarmos para uma relação de ordem, vai valer para qualquer relação que satisfaça tais axiomas.

Exemplo 1.4.3. Um exemplo de uma ordem sobre um conjunto é a relação $\leq$ sobre os números reais. Verificamos isso simplesmente notando que para qualquer $x \in \mathbb{R}$, temos $x \leq x$; que para todo $x \in \mathbb{R}$ e todo $y \in \mathbb{R}$, se $x \leq y$ e $y \leq x$, então $x = y$; e, por fim, que para qualquer $x \in \mathbb{R}$, qualquer $y \in \mathbb{R}$ e qualquer $z \in \mathbb{R}$, temos que $x \leq y$ e $y \leq z$, então $x \leq z$.

Podemos provar o seguinte resultado sobre uma ordem:

Proposição 1.4.4. *Seja $\preceq$ uma ordem sobre X. Sejam $x, y \in X$. Se, para todo $z \in X$ tal que $z \preceq x$ temos que $z \preceq y$, então $x \preceq y$.*

Demonstração. Vamos aproveitar que essa demonstração é simples para fazê-la com todos os detalhes. Note que o que queremos provar é a seguinte proposição, fixados $x, y \in X$:

$$\forall z(z \preceq x \to z \preceq y) \to x \preceq y$$

Temos que provar uma implicação (a segunda, não a primeira). Assim, vamos assumir o lado esquerdo da implicação, que é, dado $z \in X$:

$$z \preceq x \to z \preceq y \tag{1.1}$$

e mostrar o lado direito, que é:

$$x \preceq y \tag{1.2}$$

Note que, como $\preceq$ é ordem, temos que vale

$$x \preceq x$$

Assim, substituindo z em (1.1) por x (podemos fazer isso já que (1.1) valia para qualquer $z \in X$, temos que

$$\frac{\begin{array}{l} x \preceq x \\ x \preceq x \to x \preceq y \end{array}}{x \preceq y}$$

Ou seja, obtemos (1.2) como queríamos. □

Um outro exemplo de ordem, um tanto diferente, é o seguinte:

Exemplo 1.4.5. Considere a relação $|$ sobre os números naturais maiores que 0 dada por $m|n$ se "m divide n". Note que tal relação também é uma relação de ordem. De fato:

(a) $m|m$ para todo $m \in \{k \in \mathbb{N} : k > 0\}$, já que m divide m se $m \neq 0$;

(b) Se m divide n e n divide m, temos que, necessariamente, $m = n$;

(c) Se m divide n e n divide k, então m divide k.

Na verdade, voltaremos a este exemplo mais tarde e poderemos provar a última afirmação.

Como mostramos a Proposição 1.4.4 para qualquer ordem, obtemos o mesmo resultado em particular para $|$. Qual a interpretação do resultado neste caso?

Vamos agora a uma nova definição:

Definição 1.4.6. Dizemos que $\prec$ é uma **ordem estrita** sobre A se são satisfeitas as seguintes condições:

(a) $\forall a \in A \ \sim (a \prec a)$ (irreflexiva);

(b) $\forall a \in A \ \forall b \in A \ \forall c \in A (a \prec b \wedge b \prec c) \rightarrow a \prec c$ (transitiva).

Vamos aproveitar a próxima demonstração para mostrar uma técnica diferente. Vamos fazer essa **demonstração por contradição**. Essa técnica consiste do seguinte: suponha que queremos mostrar P. Então supomos como falso o que queremos mostrar, isto é $\sim P$. Tiramos algumas consequências disso até chegar numa contradição - isto é, algo que seja falso (por exemplo, a negação de algum axioma ou tautologia). Isso funciona por que sabemos que seguindo os passos de uma demonstração, se tudo que assumimos é verdadeiro, então suas consequências também devem ser. Assim, se chegamos a algo falso, é porque algo que supomos era falso. No caso, que $\sim P$ é falso. Ou seja, obtemos que P é verdadeiro.

Proposição 1.4.7. *Se $\prec$ é uma ordem estrita sobre A, então vale a seguinte propriedade (chamada de assimétrica):*

$$\forall a \in A \ \forall b \in A \ a \prec b \rightarrow \sim (b \prec a)$$

Demonstração. Suponha por contradição que vale

$$\sim (\forall a \in A \; \forall b \in Aa \prec b \rightarrow \sim (b \prec a))$$

Usando nosso método de negar fórmulas, obtemos que vale

$$\exists a \in A \; \exists b \in A \sim (a \prec b \rightarrow \sim (b \prec a))$$

Negando a implicação, obtemos:

$$\exists a \in A \; \exists b \in A(a \prec b \wedge b \prec a)$$

Aplicando o axioma de transitividade da ordem estrita, obtemos que

$$a \prec a$$

o que contraria o primeiro axioma. □

Vejamos como uma ordem se relaciona com uma ordem estrita[3]

Proposição 1.4.8. *Se $\preceq$ é uma ordem sobre A, então $\prec$ dada por, dados $a, b \in A$, $a \prec b$ se, e somente se, $a \preceq b$ e $a \neq b$, é uma ordem estrita sobre A.*

Demonstração. Precisamos mostrar que $\prec$ assim definida satisfaz os dois axiomas de ordem estrita.

(a) Seja $a \in A$. Como não é verdade que $a \neq a$, não vale $a \preceq a \wedge a \neq a$. Logo, temos que $\sim (a \prec a)$ como queríamos.

(b) Sejam $a, b, c \in A$. Suponha que $a \prec b$ e $b \prec c$. Precisamos mostrar que $a \prec c$. Note que, como $a \prec b$ e $b \prec c$, temos que

$$(a \preceq b \wedge a \neq b) \wedge (b \preceq c \wedge b \neq c)$$

pela definição de $\prec$. Assim, pela propriedade de transitividade de $\preceq$, temos que $a \preceq c$. Para concluir o que queremos, basta mostrarmos que $a \neq c$. Vamos fazer isso por contradição. Suponha $a = c$. Como $a \prec b$, temos que $c \prec b$. Por outro lado, temos que $b \prec c$. Pela definição de $\prec$, temos então que $c \preceq b$ e $b \preceq c$. Assim, pela propriedade de antissimetria de $\preceq$, temos que $b = c$. Contradição com o fato que $b \prec c$.

□

[3] Veja também o Exercício 1.4.16.

Considere a seguinte definição:

Definição 1.4.9. Seja $\preceq$ uma ordem sobre A. Dizemos que $a \in A$ é um **mínimo** de A se vale $a \preceq b$ para todo $b \in A$.

Poderíamos nos perguntar se a existência de um mínimo é consequência dos axiomas de ordem. Isto é, se podemos provar a partir de tais axiomas a seguinte proposição:

$$\exists a \in A \ \forall b \in A \ a \preceq b$$

A resposta para isso é que não. Não podemos provar tal proposição a partir de tais axiomas. Mas então alguém poderia dizer que se não podemos provar tal afirmação, deveríamos poder provar sua negação. Mas isso também não é verdade. Não podemos provar tal afirmação nem sua negação. E como provar isso? (que não podemos provar). Isso é fácil. Suponha que pudéssemos provar tal afirmação. Então todas as relações que satisfaçam os axiomas de ordem devem satisfazer tal afirmação também. Por outro lado, se pudéssemos provar sua negação, então todas as relações que satisfaçam os axiomas de ordem deve satisfazer tal negação também. Ou seja, se mostrarmos uma relação de ordem que satisfaça a existência de mínimo e uma outra que não satisfaça (isto é, que satisfaça sua negação) teremos que nem a existência nem sua negação podem ser consequências dos axiomas de ordem. Este é o caso em que dizemos que uma afirmação é **independente** de certa coleção de axiomas.

Exemplo 1.4.10. Note que 1 é um mínimo na ordem $|$ sobre $\{n \in \mathbb{N} : n > 0\}$ já que $1|b$ para todo $b \in \mathbb{N} \setminus \{0\}$. Ou seja, $|$ é uma ordem que admite mínimo. Por outro lado, $\leq$ é uma ordem sobre $\mathbb{R}$ que não admite mínimo. Basta notar que, para qualquer $x \in \mathbb{R}$, $\sim (x \leq (x-1))$.

Exercícios

Exercício 1.4.11. Monte uma tabela verdade que justifique o *modus ponens*. Isto é, com entradas p e q, verifique que a única linha em que p e $p \to q$ tem valores verdadeiros é a linha em que q também é verdade.

Exercício 1.4.12. Considere $\preceq$ uma ordem sobre A. Seja $B \subset A$. Defina em B a seguinte relação, para qualquer $x, y \in B$, $x \preceq^* y$ se, e somente se, $x \preceq y$. Mostre que $\preceq^*$ é uma ordem sobre B. Esta é chamada de **restrição** de $\preceq$ a B (em geral, denotamos as duas ordens com o mesmo símbolo).

Exercício 1.4.13. Mostre que $\preceq$ dada por, para $(a, b), (c, d) \in \mathbb{R}^2$, $(a, b) \preceq (c, d)$ se, se somente se

$$(a < c) \vee (a = c \wedge b \leq d)$$

é uma ordem sobre $\mathbb{R}^2$. Esta ordem é chamada de **ordem lexicográfica**.

Exercício 1.4.14. Mostre que $\subseteq$ é uma relação de ordem sobre o conjunto de todos os subconjuntos de um conjunto X fixado.

Exercício 1.4.15. Mostre que assumindo que valem as propriedades de assimetria e de transitividade para ordens estritas, temos que vale a de irreflexividade (ou seja, por causa da Proposição 1.4.7, poderíamos trocar a propriedade de irreflexividade pela de assimetria na definição de ordem estrita).

Exercício 1.4.16. Mostre que se $\prec$ é uma ordem estrita sobre A, então $\preceq$ dada por, dados $a, b \in A$, $a \preceq b$ se, e somente se, $(a \prec b \vee a = b)$ é uma ordem sobre A.

Exercício 1.4.17. Mostre que a seguinte afirmação é independente dos axiomas de ordem estrita:

$$\forall a \in A \; \exists b \; a \prec b$$

Exercício 1.4.18. Mostre que a seguinte afirmação é independente dos axiomas de ordem estrita:

$$\forall a \in A \; \forall b \in A \; (a \prec b \rightarrow (\exists c \in A \; a \prec c \wedge c \prec b))$$

1.5 Exercícios do Capítulo

1.5.1. Aplique nosso método de negação de fórmulas para escrever a fórmula que diz "A não tem mínimo".

1.5.2. Negue a fórmula que diz que uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ não é contínua num ponto x_0. Dê um exemplo de uma função não contínua no ponto 1 e mostre que, de fato, ela não é contínua.

1.5.3. Suponha que $\prec$ é uma ordem sobre A e que tal ordem tem um mínimo. Mostre que tal mínimo é único. Isto é, suponha a é um mínimo e suponha que b também seja. Mostre que $a = b$.

Capítulo 2

Números naturais

2.1 Introdução

Na primeira seção deste capítulo, vamos dar uma definição axiomática para os números naturais. Nas seções seguintes, mostraremos como definir em tal conjunto as operações básicas, como a soma e a multiplicação.

Depois, nos capítulos seguintes, mostraremos como usar os naturais para definir outros conjuntos importantes em matemática, como os inteiros e os racionais. Ou seja, de certa forma, vamos mostrar como fundamentar parte da matemática assumindo apenas algumas afirmações sobre números naturais.

2.2 Axiomas de Peano

Comecemos com os **axiomas de Peano**. Tais axiomas são uma forma de definir axiomaticamente o conjunto $\mathbb{N}$ dos números naturais. Para descrever tais propriedades, usaremos, além dos símbolos usuais já descritos, os seguintes símbolos: 0 (zero) e s (sucessor).

Basicamente estes axiomas dizem: 0 é um número natural; se algo é um número, seu sucessor também é; 0 não é sucessor de ninguém; se dois números tem o mesmo sucessor, eles são iguais e, finalmente, que vale a indução.

(a) $0 \in \mathbb{N}$;

(b) $\forall n \in \mathbb{N}\ s(n) \in \mathbb{N}$;

(c) $\forall n \in \mathbb{N}\ s(n) \neq 0$;

(d) $\forall n \in \mathbb{N}\ \forall m \in \mathbb{N}\ s(n) = s(m) \rightarrow n = m$;

(e) Seja $P(x)$ uma propriedade sobre elementos de $\mathbb{N}$. Se valem

(i) $P(0)$;

(ii) $\forall n \in \mathbb{N}\ P(n) \to P(s(n))$;

Então vale $P(n)$ para todo $n \in \mathbb{N}$.

O axioma (e) é conhecido como **princípio de indução**. O conjunto $\{0, 1, 2, ...\}$ satisfaz as propriedades acima se interpretamos o símbolo $s(n)$ como $n + 1$. Para notar que vale o princípio de indução em tal conjunto, suponha que não vale. Então existe n o menor tal que não vale $P(n)$. Note que tal n não pode ser o 0 já que temos que vale $P(0)$. Sabemos então que $n = m+1$ para algum $m \in \{0, 1, 2, ...\}$. Como $m < n$, temos que vale $P(m)$. Logo, vale $P(s(m))$. Mas $P(s(m)) = P(m + 1) = P(n)$, contradição.

Basicamente o que estamos fazendo aqui é provar que se todo conjunto não vazio admite mínimo, então vale indução.

Agora vamos começar a ver algumas consequências de tais axiomas. Ou seja, propriedades que os números naturais também tem e que decorrem do fato deles satisfazerem os axiomas de Peano.

O primeiro resultado basicamente diz que, ao tomarmos sucessores, nunca voltamos ao próprio elemento:

Proposição 2.2.1. *Temos que $s(n) \neq n$ para todo $n \in \mathbb{N}$.*

Demonstração. Vamos provar isso por indução. Ou seja, para concluirmos o que queremos, basta mostrarmos, utilizando o princípio de indução, que a fórmula $P(x)$ vale para todo $x \in \mathbb{N}$, onde $P(x)$ é "$s(x) \neq x$". Para mostrar isso por indução, precisamos mostrar que vale $P(0)$ e que se vale $P(n)$ vale $P(s(n))$. Note que $0 \neq s(0)$ já que $0 \in \mathbb{N}$ (por (a)) e, portanto, $s(0) \neq 0$ por (c).

Agora suponha que vale $P(n)$ para algum n. Ou seja, vale $n \neq s(n)$. Vamos mostrar que vale $P(s(n))$, isto é, $s(n) \neq s(s(n))$. Suponha que não, isto é, que vale $s(n) = s(s(n))$. Por (d), temos que $n = s(n)$, contrariando nossa hipótese. □

O próximo resultado diz que, com exceção do 0, todo natural é sucessor de outro natural:

Proposição 2.2.2. *Se $n \in \mathbb{N}$ e $n \neq 0$, então existe $m \in \mathbb{N}$ tal que $n = s(m)$.*

Demonstração. Novamente, vamos mostrar por indução. Ou seja, vamos mostrar que vale a fórmula $P(x)$ para todo $x \in \mathbb{N}$ onde $P(x)$ é a fórmula

$$x \neq 0 \to \exists m\ x = s(m)$$

Note que $0 \neq 0 \to \exists m\ 0 = s(m)$ simplesmente porque não vale $0 \neq 0$ (não importa que também não valha o lado direito da implicação).

Agora suponha que vale $P(n)$ para algum n. Isto é, para tal n vale $n \in \mathbb{N}$ $n \neq 0 \rightarrow \exists m\ n = s(m)$. Precisamos mostrar então que vale $P(s(n))$. Isto é, precisamos mostrar que, se vale $s(n) \neq 0$, então vale que existe m tal que $s(n) = s(m)$. Suponha então que $s(n) \neq 0$. Considere $m = n$. Note que, então $s(n) = s(m)$ como queríamos. □

Num primeiro momento, pode parecer que o princípio de indução só serve para mostrar afirmações sobre os números naturais. Mas muitas afirmações que são mostradas por indução não falam sobre números naturais (ou, pelo menos não sobre eles diretamente). Vejamos um exemplo (note que esse exemplo só está aqui para mostrar como indução aparece em outros contextos. Nessa demonstração usaremos diversas coisas que ainda não foram (ou nem serão) mostradas neste trabalho):

Exemplo 2.2.3. Vamos mostrar que, para qualquer $n \in \mathbb{N}$ e qualquer $x > 0$, temos $(x^n)' = nx^{n-1}$ ($(x^n)'$ denota a derivada de x^n). Para mostrarmos isso por indução, precisamos transformar isso numa afirmação sobre números naturais. Assim, nossa afirmação $P(n)$ simplesmente é

$$\forall x > 0\ (x^n)' = nx^{n-1}$$

Vamos verificar se vale $P(0)$. Para isso ser verdade, precisamos que

$$(x^0)' = 0$$

Mas isso de fato ocorre já que $x^0 = 1$ (ou seja, é constante). Agora vamos mostrar que $P(n) \rightarrow P(s(n))$. Antes disso, vamos fazer o caso $n = 1$ separadamente (vamos usar isso mais para frente). Note que

$$(x^1)' = x' = 1 = 1x^0$$

Lembrando que $s(n) = n + 1$, vamos usar também que $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$. Assim, suponha que

$$(x^n)' = nx^{n-1}$$

e vamos mostrar que

$$(x^{n+1})' = (n+1)x^n$$

Temos que

$$\begin{aligned}
(x^{n+1})' &= (x^n x)' \\
&= (x^n)'x + x^{n+1}(x)' \\
&= nx^{n-1}x + x^n 1 \\
&= nx^n + x^n \\
&= (n+1)x^n
\end{aligned}$$

Exercícios

Exercício 2.2.4. Considere o seguinte argumento para mostrar que todos os cavalos são de uma mesma cor: Vamos mostrar que todos os cavalos tem apenas uma cor por indução sobre a quantidade de cavalos. Ou seja, $P(n)$ é a afirmação: Dada uma coleção de n cavalos, todos eles tem a mesma cor. É claro que temos que $P(0)$ vale (se não valesse, teria que ter um conjunto com 0 cavalos, sendo dois com cores diferentes). Agora vamos supor que vale $P(n)$ e mostrar $P(n+1)$. Sejam $n+1$ cavalos. Vamos mostrar que eles são todos de uma cor só. Pegue um dos cavalos e separe. Vamos chama-lo de a. Note que sobraram n cavalos. Pela nossa hipótese, os n cavalos são todos da mesma cor. Devolva o cavalo original e separe um outro qualquer (vamos chama-lo de b). Novamente ficamos com apenas n cavalos e, por hipótese, todos são da mesma cor. Assim, o cavalo a tem a mesma cor que os demais (diferentes de b). Mas, pela primeira passagem, o cavalo b tem a mesma cor que os demais. Ou seja, a e b tem a mesma cor, que é a cor dos demais. Logo, todos tem a mesma cor.

Qual o erro cometido acima?

Exercício 2.2.5. Note que, se tirarmos o axioma $s(n) \neq 0$ para todo $n \in \mathbb{N}$, teríamos que o conjunto $N = \{0\}$ também iria satisfazer todos os axiomas listados (colocando N no lugar de $\mathbb{N}$).

2.3 A soma nos naturais

Vejamos agora como definir a operação de soma (+) sobre os naturais:

Definição 2.3.1. Chamamos de **soma** nos naturais (ou **adição**) uma função $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que sejam satisfeitas:

(a) $\forall a \in \mathbb{N}\ f(a, 0) = a$;

(b) $\forall a \in \mathbb{N}\ \forall b \in \mathbb{N}\ f(a, s(b)) = s(f(a, b))$.

Vamos ver que, na verdade, existe uma única função f que satisfaz os axiomas acima. Antes, vamos provar algumas propriedades que qualquer função que satisfaz tais axiomas vai satisfazer:

Lema 2.3.2. *Seja $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ uma soma sobre $\mathbb{N}$. Então, dado $a \in \mathbb{N}$, temos que $f(0, a) = a$.*

Demonstração. Vamos mostrar a afirmação $P(x)$ dada por

$$f(0, x) = x$$

por indução.

$P(0)$**:** Temos que $f(0, 0) = 0$ pelo axioma (a) de adição.

$P(n) \to P(s(n))$**:** Suponha que $f(0, n) = n$ e vamos provar que $f(0, s(n)) = s(n)$. Temos, por (b), que $f(0, s(n)) = s(f(0, n)) = s(n)$.

□

Lema 2.3.3. *Seja $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ uma soma sobre $\mathbb{N}$. Então, dados $a, b \in \mathbb{N}$, temos que $f(a, s(b)) = f(s(a), b)$*

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$f(a, s(x)) = f(s(a), x)$$

Note que se $P(x)$ for verdadeira para todo $x \in \mathbb{N}$, temos o resultado desejado (já que o a é qualquer). Vamos mostrar $P(x)$ por indução.

$P(0)$**:** Temos $f(a, s(0)) = s(f(a, 0)) = s(a)$. Por outro lado, $f(s(a), 0) = s(a)$. Logo, temos $P(0)$.

$P(n) \to P(s(n))$**:** Suponha que vale $f(a, s(n)) = f(s(a), n)$ e vamos mostrar $f(a, s(s(n))) = f(s(a), s(n))$. Temos

$$\begin{aligned} f(a, s(s(n))) &= s(f(a, s(n))) \\ &= s(f(s(a), n)) \\ &= f(s(a), s(n)) \end{aligned}$$

□

E note que conseguimos provar tudo isso sem nem mesmo saber se existe de fato alguma função que satisfaça os axiomas de soma.

Finalmente, podemos provar que qualquer função que satisfaça os axiomas de soma precisa ser comutativa:

Proposição 2.3.4. *Seja $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ uma soma sobre $\mathbb{N}$. Então, dados $a, b \in \mathbb{N}$, temos que $f(a, b) = f(b, a)$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere a seguinte afirmação sobre $x \in \mathbb{N}$:

$$f(x, a) = f(a, x)$$

Vamos chamar tal afirmação de $P(x)$. Note que se mostrarmos $P(x)$ para todos os $x \in \mathbb{N}$, teremos o resultado desejado (já que o a é qualquer). Assim, vamos mostrar $P(x)$ por indução sobre $n \in \mathbb{N}$.

$P(0)$**:** Temos que $f(x, 0) = x$, pelo axioma (a) da definição de soma. Por outro lado, temos que $f(0, x) = x$ também (pelo Lema **2.3.2**).

$P(n) \to P(s(n))$**:** Suponha que vale $f(n, a) = f(a, n)$ e vamos mostrar que $f(s(n), a) = f(a, s(n))$. Temos:

$$\begin{aligned} f(s(n), a) &\overset{\mathbf{2.3.3}}{=} f(n, s(a)) \\ &= s(f(n, a)) \\ &= s(f(a, n)) \\ &= f(a, s(n)) \end{aligned}$$

□

Note que só dissemos duas condições sobre f, mas essas duas condições são suficientes para descrevê-la completamente, como atesta o seguinte resultado:

Proposição 2.3.5. *Suponha que $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ e $g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ sejam duas adições sobre $\mathbb{N}$. Então, para quaisquer $a, b \in \mathbb{N}$ temos que $f(a, b) = g(a, b)$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$f(a, x) = g(a, x)$$

Vamos mostrar tal afirmação por indução (note que isso é suficiente para o que queremos).

$P(0)$**:** Pelo axioma (a) da soma, temos que $f(a, 0) = a = g(a, 0)$.

$P(n) \to P(s(n))$**:** Vamos supor que vale $f(a, n) = g(a, n)$ e mostrar que vale $f(a, s(n)) = g(a, s(n))$. Temos $f(a, s(n)) = s(f(a, n)) = s(g(a, n)) = g(a, s(n))$.

□

Ou seja, agora temos que, no máximo, uma função pode satisfazer os axiomas de soma. Resta provar que existe alguma.

Para isso, vamos provar um resultado conhecido como teorema da recursão. Este teorema costuma ser apresentado numa forma bem mais geral, mas, para o que vamos precisar aqui, a versão a seguir é suficiente (e boa parte da ideia da demonstração mais geral será apresentada também de forma simplificada).

Teorema 2.3.6 (da Recursão em $\mathbb{N}$). *Seja $\varphi : \mathbb{N} \to \mathbb{N}$ uma função. Seja $a \in \mathbb{N}$. Então existe uma única função $f : \mathbb{N} \to \mathbb{N}$ tal que*

Veja o Exercício 2.3.15

(a) $f(0) = a$*;*

(b) $f(s(n)) = \varphi(f(n))$*.*

Demonstração. A unicidade segue por indução (como fizemos no caso da soma). Vamos mostrar que existe alguma f satisfazendo as condições.

Considere $\mathcal{F}$ o conjunto de todas as funções g tais que:

- $0 \in \mathrm{dom}(g)$;
- se $s(n) \in \mathrm{dom}(g)$, então $n \in \mathrm{dom}(g)$.
- $g(0) = a$
- $g(s(n)) = \varphi(g(n))$ para todo $s(n) \in \mathrm{dom}(g)$.

Primeiramente, note que $\mathcal{F} \neq \emptyset$, já que a função com domínio igual a $\{0\}$ e tal que $g(0) = a$, é um elemento de $\mathcal{F}$.

Da mesma forma, temos que a função h com domínio $\{0, s(0)\}$ tal que $h(0) = a$ e $h(s(0)) = \varphi(a)$ também é um elemento de $\mathcal{F}$.

Em geral, dizemos que duas funções F, G são **funções compatíveis** se, para todo $x \in \text{dom}(F) \cap \text{dom}(G)$, temos que $F(x) = G(x)$. Note que se duas funções são compatíveis entre si, elas tem uma extensão em comum. Basta definir.

$$H(x) = \begin{cases} F(x) & \text{se } x \in \text{dom}(F) \\ G(x) & \text{se } x \in \text{dom}(G) \end{cases}$$

Note que H estende ambas as funções por elas serem compatíveis (em outro caso, teríamos problemas na intersecção dos domínios).

Note que, se $g, h \in \mathcal{F}$, então g e h são compatíveis. Para isso, basta, fixadas $g, h \in \mathcal{F}$, mostrar por indução a afirmação

$$\forall n \in \mathbb{N}\ n \in \text{dom}(g) \cap \text{dom}(h) \to g(n) = h(n)$$

Finalmente, como todas as funções em $\mathcal{F}$ são compatíveis, para definir f, basta tomar $f(n) = g(n)$ para qualquer $g \in \mathcal{F}$ que tenha n em seu domínio (já que qualquer outra função em $\mathcal{F}$ vai ter o mesmo valor). Assim, só precisamos mostrar que, dado qualquer $n \in \mathbb{N}$, existe $g \in \mathcal{F}$ tal que $n \in \text{dom}(g)$. Novamente, tal resultado pode ser provado por indução.

Finalmente, note que f definida desta forma satisfaz o enunciado. □

Com isso, podemos mostrar a existência de uma função soma:

Proposição 2.3.7. *Existe uma função soma.*

Demonstração. Seja $a \in \mathbb{N}$. Pelo teorema da recursão, temos que existe $f_a : \mathbb{N} \to \mathbb{N}$ dada por

Note que estamos usando como φ a própria função s.

- $f_a(0) = a$;
- $f_a(s(b)) = s(f_a(b))$.

Agora defina $f(a, b) = f_a(b)$. Note que tal função é uma soma. □

Dados os últimos resultados, temos que existe uma única função satisfazendo os axiomas de adição. Para manter a coerência com a notação usual, a partir deste momento adotaremos a notação $a + b$ no lugar da $f(a, b)$.

Vejamos mais algumas propriedades sobre a soma:

Proposição 2.3.8. *Valem as seguintes propriedades:*

*(a) Dados $a, b \in \mathbb{N}$, temos $a + b = b + a$; (**comutativa**)*

*(b) Dados $a, b, c \in \mathbb{N}$, temos que $(a + b) + c = a + (b + c)$; (**associativa**)*

Demonstração. (a) É simplesmente o que foi provado na Proposição **2.3.4**.

(b) Sejam $a, b \in \mathbb{N}$. Considere a seguinte afirmação $P(x)$ para $x \in \mathbb{N}$:

$$(a + b) + x = a + (b + x)$$

Vamos mostrar $P(x)$ por indução (note que isso é suficiente).

$P(0)$**:** $(a + b) + 0 = a + b$, pelo axioma (a) da soma. Por outro lado, $a + (b + 0) = a + b$, pelo mesmo axioma.

$P(n) \to P(s(n))$**:** Vamos supor que vale $(a+b)+n = a+(b+n)$ e vamos mostrar que $(a + b) + s(n) = a + (b + s(n))$. Temos

$$\begin{aligned} (a + b) + s(n) &= s((a + b) + n) \\ &= s(a + (b + n)) \\ &= a + s(b + n) \\ &= a + (b + s(n)) \end{aligned}$$

□

Proposição 2.3.9 (**Lei do Cancelamento**)**.** *Sejam $a, b, c \in \mathbb{N}$. Se $a+b = a + c$, então $b = c$.*

Demonstração. Sejam $b, c \in \mathbb{N}$. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$(x + b = x + c) \to b = c$$

Vamos mostra-la por indução (note que isso é suficiente).

$P(0)$**:** Suponha que $0 + b = 0 + c$. Note que $0 + b = b$ e que $0 + c = c$. Logo, temos que $b = c$ como queríamos.

$P(n) \to P(s(n)$**:** Suponha que vale $(n + b = n + c) \to b = c$. Suponha que vale $s(n) + b = s(n) + c$. Logo, temos $b + s(n) = c + s(n)$. Pela axioma (b) da adição, temos $s(b+n) = s(c+n)$. Pelo axioma (d) dos naturais, temos que $b + n = c + n$. Logo, $n + b = n + c$ e, portanto, $b = c$.

□

Vamos terminar essa seção apresentando mais alguma notações para deixar $\mathbb{N}$ mais parecido com o usual.

Definição 2.3.10. Vamos chamar de 1 o elemento $s(0)$ de $\mathbb{N}$. Também usaremos a notação usual para $s(1) = 2$, $s(2) = 3$...

Proposição 2.3.11. *Seja $a \in \mathbb{N}$. Então $s(a) = a + 1$.*

Demonstração. Considere $P(x)$ a seguinte afirmação para $x \in \mathbb{N}$:

$$s(x) = x + 1$$

Vamos mostra-la por indução.

$P(0)$**:** Temos $s(0) = 1$ por definição. Por outro, $0 + 1 = 1 + 0 = 1$.

$P(n) \to P(s(n))$**:** Suponha que vale $s(n) = n + 1$ e vamos mostrar que vale $s(s(n)) = s(n) + 1$. Temos

$$\begin{aligned} s(s(n)) &= s(n+1) \\ &= s(1+n) \\ &= 1 + s(n) \\ &= s(n) + 1 \end{aligned}$$

□

Dado o último resultado, daqui em diante muitas vezes utilizaremos a notação $n + 1$ no lugar da $s(n)$.

Exercícios

Exercício 2.3.12. Mostre que, dados $a, b, c \in \mathbb{N}$, se $b + a = c + a$, então $b = c$.

Exercício 2.3.13. Seja $a \in \mathbb{N}$ tal que $n + a = n$ para todo $n \in \mathbb{N}$. Mostre que $a = 0$ (um elemento satisfazendo tal propriedade é dito um **elemento neutro** com relação à operação $+$. Assim, o que estamos mostrando com esse exercício é que o 0 é o único elemento neutro com relação à $+$).

Exercício 2.3.14. Sejam $a, b \in \mathbb{N}$ tais que $a + b = 0$.

(a) Mostre que $b = 0$.

(b) Conclua que $a = 0$ e $b = 0$.

Exercício 2.3.15. Adapte a demonstração para o Teorema da Recursão para o caso em que $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ e substituimos a segunda condição por

$$f(s(n)) = \varphi(f(n), n)$$

2.4 O produto nos naturais

Vamos agora, de forma semelhante ao que fizemos com a soma, definir o produto de naturais.

Definição 2.4.1. Chamamos de **produto** (ou de **multiplicação**) uma função $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ que satisfaz:

(a) $\forall a \in \mathbb{N}\ f(a, 0) = 0$;

(b) $\forall a \in \mathbb{N}\ \forall b \in \mathbb{N}\ f(a, s(b)) = a + f(a, b)$.

Da mesma forma que com a soma, o produto também é único:

Proposição 2.4.2. *Sejam $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ e $g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ dois produtos sobre $\mathbb{N}$. Então, dados $a, b \in \mathbb{N}$, temos que $f(a, b) = g(a, b)$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $f(a, x) = g(a, x)$. Vamos mostrar $P(x)$ para todo $x \in \mathbb{N}$ por indução.

$P(0)$**:** Temos, pelo axioma (a) que $f(a, 0) = 0 = g(a, 0)$.

$P(n) \to P(s(n))$**:** Suponha que vale $f(a, n) = g(a, n)$ e vamos mostrar que vale $f(a, s(n)) = g(a, s(n))$. Temos

$$\begin{aligned} f(a, s(n)) &= a + f(a, n) \\ &= a + g(a, n) \\ &= g(a, s(n)) \end{aligned}$$

□

Vamos agora mostrar a existência de uma função produto:

Proposição 2.4.3. *Existe uma função produto.*

Demonstração. Fixado $a \in \mathbb{N}$, considere $f_a : \mathbb{N} \to \mathbb{N}$ dada pelo teorema da recursão satisfazendo:

Note que aqui precisamos da versão do Teorema da Recursão apresentada no Exercício 2.3.15.

- $f_a(0) = 0$;
- $f_a(s(n)) = f_a(n) + n$.

Com isso, definimos $f(a, b) = f_a(b)$. Note que f assim definida é um produto. □

Dados os últimos resultados, denotaremos o único produto sobre os naturais por $\cdot$. Isto é, em vez de usarmos $f(a, b)$ usaremos $a \cdot b$. Muitas vezes omitiremos o $\cdot$ e usaremos simplesmente ab.

Lema 2.4.4. *Seja $a \in \mathbb{N}$. Então $0 \cdot a = 0$.*

Demonstração. Considere $P(x)$ sendo $0 \cdot x = 0$. Vamos mostrar por indução.

$P(0)$**:** $0 \cdot 0 = 0$, pelo axioma (a).

$P(n) \to P(s(n))$**:** Suponha $0 \cdot n = 0$. Temos

$$\begin{aligned} 0 \cdot s(n) &= 0 + (0 \cdot n) \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

□

Lema 2.4.5. *Sejam $a, b \in \mathbb{N}$. Então vale $s(b) \cdot a = a + (b \cdot a)$.*

Demonstração. Seja $b \in \mathbb{N}$. Considere $P(x)$ sendo $s(b) \cdot x = x + (b \cdot x)$. Vamos mostrar por indução. Temos:

$P(0)$**:** $s(b) \cdot 0 = 0$. Por outro lado, $0 + (c \cdot 0) = 0 + 0 = 0$.

$P(n) \to P(s(n))$**:** Suponha que vale $s(b) \cdot n = n + (b \cdot n)$. Temos

$$\begin{aligned} s(b) \cdot s(n) &= s(b) + (s(b) \cdot n) \\ &= s(b) + (n + (b \cdot n)) \\ &= (s(b) + n) + (b \cdot n) \\ &= (b + s(n)) + (b \cdot n) \\ &= s(n) + (b + (b \cdot n)) \\ &= s(n) + (b \cdot s(n)) \end{aligned}$$

□

Proposição 2.4.6. *Valem as seguintes propriedades:*

*(a) Dados $a, b \in \mathbb{N}$, $a \cdot b = b \cdot a$; (***comutativa***)*

*(b) Dados $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; (***distributiva***).*

*(c) Dados $a, b, c \in \mathbb{N}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; (***associativa***)*

Demonstração. (a) Seja $a \in \mathbb{N}$. Considere $P(x)$ sendo $a \cdot x = x \cdot a$. Vamos mostrar por indução.

$P(0)$**:** Temos que $a \cdot 0 = 0 = 0 \cdot a$ (pelo Lema **2.4.4**).

$P(n) \to P(s(n))$**:** Suponha $a \cdot n = n \cdot a$. Temos

$$\begin{array}{rcl} a \cdot s(n) & = & a + (a \cdot n) \\ & = & a + (n \cdot a) \\ & \overset{\mathbf{2.4.5}}{=} & s(n) \cdot a \end{array}$$

(b) Considere $P(x)$ sendo $a \cdot (b + x) = (a \cdot b) + (a \cdot x)$. Vamos mostrar por indução.

$P(0)$**:** $a \cdot (b + 0) = a \cdot b$. Por outro lado, $a \cdot b + a \cdot 0 = a \cdot b + 0 = a \cdot b$.

$P(n) \to P(s(n))$**:** Suponha que vale $a \cdot (b + n) = (a \cdot b) + (a \cdot n)$. Vamos mostrar $a \cdot (b + s(n)) = (a \cdot b) + (a \cdot (s(n))$. Temos:

$$\begin{array}{rcl} a \cdot (b + s(n)) & = & a \cdot (s(b + n)) \\ & = & a + (a \cdot (b + n)) \\ & = & a + ((a \cdot b) + (a \cdot n)) \\ & = & (a \cdot b) + (a + (a \cdot n)) \\ & = & (a \cdot b) + (a \cdot s(n)) \end{array}$$

(c) Sejam $a, b \in \mathbb{N}$. Considere $P(x)$ sendo $(a \cdot b) \cdot x = a \cdot (b \cdot x)$. Vamos mostrar por indução.

$P(0)$**:** Temos que $(a \cdot b) \cdot 0 = 0$. Por outro lado, $a \cdot (b \cdot 0) = a \cdot 0 = 0$.

$P(n) \to P(s(n))$**:** Suponha que vale $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Temos

$$\begin{array}{rcl} (a \cdot b) \cdot s(n) & = & (a \cdot b) + ((a \cdot b) \cdot n) \\ & = & (a \cdot b) + (a \cdot (b \cdot n)) \\ & \overset{(dist.)}{=} & a \cdot (b + (b \cdot n)) \\ & = & a \cdot (b \cdot s(n)) \end{array}$$

□

Proposição 2.4.7. *Sejam $a, b \in \mathbb{N}$. Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.*

Demonstração. Suponha $a \cdot b = 0$. Temos que mostrar $a = 0 \vee b = 0$. Suponha que $b \neq 0$. Vamos mostrar que então $a = 0$ (note que isso é suficiente). Como $b \neq 0$, existe $m \in \mathbb{N}$ tal que $s(m) = b$. Assim, temos que $a \cdot s(m) = 0$. Por outro lado, temos que $a \cdot s(m) = a + (a \cdot m)$. Assim, temos que $a + (a \cdot m) = 0$. Logo, $a = 0$ e $a \cdot m = 0$ (pelo Exercício **2.3.14**). Em particular, temos que $a = 0$ como queríamos. □

Proposição 2.4.8. *Seja $a \in \mathbb{N}$. Então $1 \cdot a = a$.*

Demonstração. Considere $P(x)$ sendo $1 \cdot x = x$. Vamos mostrar por indução.

$P(0)$**:** Como $1 \cdot 0 = 0$, temos o resultado.

$P(n) \to P(s(n))$**:** Suponha que vale $1 \cdot n = n$. Temos:

$$\begin{aligned} 1 \cdot s(n) &= 1 + (1 \cdot n) \\ &= 1 + n \\ &= s(n) \end{aligned}$$

□

Para evitar o uso excessivo de parênteses, vamos utilizar as convenções usuais. Por exemplo, em vez de escrevermos $(a+b)+c$, escreveremos $a+b+c$ (já que pela associativa, não importa como interpretamos a última notação). Também usaremos o "critério de prioridade" do produto sobre a soma. Por exemplo, $ab + c$ deverá ser interpretado como $(a \cdot b) + c$.

Exercícios

Exercício 2.4.9. Mostre por indução que vale a seguinte identidade para todo $x \in \mathbb{N}$:

$$2 \cdot (0 + 1 + \cdots + x) = (x + 1)x$$

Exercício 2.4.10. Considere k retas num plano, sendo que nenhuma delas é paralela a outra e que, para cada ponto do plano, passe no máximo duas destas retas. Considere R sendo a quantidade de regiões em que o plano foi dividido por tais retas. Mostre que vale a seguinte identidade:

$$2R = kk + k + 2$$

Exercício 2.4.11. Considere $f : \mathbb{N} \longrightarrow \mathbb{N}$ satisfazendo as seguintes propriedades:

(A) $f(0) = 1$;

(B) Para todo $a \in \mathbb{N}$, $f(s(a)) = f(a) \cdot s(a)$;

(a) Calcule $f(1)$, $f(2)$, $f(3)$ e $f(4)$.

(b) Mostre que só existe uma única f satisfazendo os axiomas acima. Dado este resultado, vamos denotar $f(a)$ por $a!$ (**fatorial** de a).

Exercício 2.4.12. Mostre por indução que a quantidade de formas de se colocar p objetos distintos numa fila (como todos os p objetos) é $p!$.

Exercício 2.4.13. Justifique a existência da função fatorial usando o teorema da recursão.

2.5 A ordem nos naturais

Nesta seção vamos definir a ordem sobre os naturais.

Definição 2.5.1. Dados $a, b \in \mathbb{N}$, vamos denotar por $a \leq b$ se existe $m \in \mathbb{N}$ tal que $a + m = b$. Esta é a **ordem** usual sobre $\mathbb{N}$.

Proposição 2.5.2. *A relação $\leq$ definida acima é de fato uma ordem sobre $\mathbb{N}$.*

Demonstração. Precisamos mostrar que valem os axiomas de ordem.

reflexiva: Seja $a \in \mathbb{N}$. Como $a + 0 = a$, temos que $a \leq a$.

antissimétrica: Sejam $a, b \in \mathbb{N}$ tais que $a \leq b$ e $b \leq a$. Vamos mostrar que $a = b$. Temos então que existe $m \in \mathbb{N}$ tal que $a + m = b$ e que existe $k \in \mathbb{N}$ tal que $b + k = a$. Logo, de $a + m = b$ temos que $(b + k) + m = b$. Assim $b + (k + m) = b + 0$. Logo, $k + m = 0$. Pelo Exercício 2.3.14, temos que $k = m = 0$. Assim, de $a + m = b$ temos que $a = b$ como queríamos.

transitiva: Sejam $a, b, c \in \mathbb{N}$ tais que $a \leq b$ e $b \leq c$. Vamos mostrar que $a \leq c$. Sejam $m, k \in \mathbb{N}$ tais que $a + m = b$ e $b + k = c$. Note que tomando $t = m + k$, temos

$$\begin{aligned} a + t &= a + (m + k) \\ &= (a + m) + k \\ &= b + k \\ &= c \end{aligned}$$

Logo, $a \leq c$.

□

Os axiomas de ordem não implicam que, dados dois elementos quaisquer, eles precisam ser comparáveis. Mas, no caso desta ordem específica que apresentamos, isso vale:

Definição 2.5.3. Dizemos que uma ordem $\preceq$ sobre X é uma **ordem total** sobre X se, dados $a, b \in X$, temos que $a \preceq b$ ou $b \preceq a$.

Lema 2.5.4. *Valem as seguintes afirmações:*

(a) Seja $a \in \mathbb{N}$. Então $a < a + 1$;

(b) Sejam $a, b \in \mathbb{N}$. Então $a < b \to a + 1 \leq b$.

Demonstração. (a) Note que $a \leq a + 1$, pois $a + 1 = a + 1$. Agora suponha que $a = a + 1$. Mas então $a = s(a)$, contradição.

(b) Temos que existe $m \in \mathbb{N}$ tal que $a + m = b$, com $m \neq 0$ (pois, se $m = 0$, teríamos $a = b$). Assim, $m = s(n)$. Logo, $a + s(n) = b$ e, portanto $(a + 1) + n = b$. Isto é, $a + 1 \leq b$.

□

Proposição 2.5.5. *A ordem $\leq$ definida acima é uma ordem total sobre $\mathbb{N}$.*

Demonstração. Seja $a \in \mathbb{N}$. Considere $C_a = \{m \in \mathbb{N} : m \leq a \vee a \leq m\}$ (leia como "o conjunto de todos os elementos comparáveis com a"). Vamos mostrar que $C_a = \mathbb{N}$. Como a é qualquer, note que isso implica o resultado (já que dado qualquer a, ele é comparável com todos os outros elementos de $\mathbb{N}$). Vamos mostrar isso por indução. Isto é, considere $P(x)$ a afirmação $C_x = \mathbb{N}$.

$P(0)$**:** Note que dado qualquer $m \in \mathbb{N}$, temos que $0 \leq m$ (pois $0 + m = m$. Assim, $C_0 = \mathbb{N}$.

$P(n) \to P(n + 1)$**:** Suponha que vale $C_n = \mathbb{N}$, vamos mostrar que $C_{n+1} = \mathbb{N}$. Seja $m \in \mathbb{N}$. Temos que mostrar que $m \in \mathbb{N}$. Temos que $m \in C_n$ (pela hipótese de indução). Assim, temos dois casos:

- Caso $m \leq n$: Como $m \leq n$ e $n < n + 1$, temos que $m \leq n + 1$ e, portanto, $m \in C_{n+1}$ como queríamos.
- Caso $n \leq m$: Vamos dividir esse caso em dois. Se $n < m$, então $n + 1 \leq m$ e, portanto, $m \in C_{n+1}$. Se $n = m$, então $m \leq n + 1$ e, portanto, $m \in C_{n+1}$.

□

Finalmente, com a ajuda da ordem, podemos provar a lei de cancelamento para o produto:

Proposição 2.5.6. *Sejam $a, b, c \in \mathbb{N}$ com $c \neq 0$. Se $ac = bc$, então $a = b$.*

Demonstração. Suponha que $a \leq b$ (note que o outro caso seria $b \leq a$, que seria análogo). Então existem $m \in \mathbb{N}$ tal que $a + m = b$. Assim, de $ac = bc$, temos que $ac = (a+m)c$. Ou seja, $ac = ac+mc$ e, portanto, $mc = 0$. Como $c \neq 0$, temos que $m = 0$ e, portanto, $a = b$ como queríamos. □

Exercícios

2.5.1. Mostre que, dados $a, b \in \mathbb{N}$, temos que vale uma, e somente uma, das seguintes afirmações:

(i) $a < b$

(ii) $b < a$

(iii) $a = b$

2.5.2. Sejam $a, b, c \in \mathbb{N}$. Mostre que se $a \leq b$, então $a + c \leq b + c$.

2.5.3. Sejam $a, b, c \in \mathbb{N}$. Mostre que se $a \leq b$, então $ac \leq bc$.

2.5.4. Seja $a \in \mathbb{N}$. Mostre que não existe $b \in \mathbb{N}$ tal que $a < b$ e $b < a + 1$.

2.5.5. Seja $P(x)$ uma afirmação sobre $x \in \mathbb{N}$. Seja $a \in \mathbb{N}$. Se

(a) vale $P(a)$;

(b) vale $P(n) \to P(n + 1)$ para todo $n \geq a$.

Mostre que então vale $P(x)$ para todo $x \in \mathbb{N}$ tal que $a \leq x$.

2.6 Exercícios do Capítulo

2.6.1. Seja $a \in \mathbb{N}$ tal que $a \cdot n = n$ para todo $n \in \mathbb{N}$. Mostre que $a = 1$ (um elemento satisfazendo tal propriedade é dito um **elemento neutro** com relação à operação $\cdot$. Assim, o que estamos mostrando com esse exercício é que o 1 é o único elemento neutro com relação à $\cdot$).

2.6.2. Considere uma pista circular onde se encontram k postos de combutível ($k \geq 1$). Sabe-se que somando a quantidade total de combustível dos postos, tem-se o suficiente para que um carro possa dar uma volta completa. Mostre que existe um local da pista em que um carro, mesmo sem combustível, possa começar e dar uma volta completa.

2.6.3. Dizemos que $f : (\mathbb{N} \setminus \{0\}) \times \mathbb{N} \longrightarrow \mathbb{N}$ é uma **exponenciação** se f satisfaz:

(A) Dado $a \in \mathbb{N}$, $a \neq 0$ temos $f(a, 0) = 1$;

(B) Dados $a, b \in \mathbb{N}$, com $a \neq 0$, temos $f(a, s(b)) = f(a, b)a$.

(a) Calcule, pela definição, $f(2, 1)$, $f(2, 2)$ e $f(2, 3)$.

(b) Mostre que a exponenciação é única. Assim, usaremos a notação a^b, em vez de $f(a, b)$. Reescreva os axiomas A e B com essa nova notação.

(c) Mostre que, dados $a, b, c \in \mathbb{N}$, com $a \neq 0$, temos $(a^b) \cdot (a^c) = a^{b+c}$.

(d) Mostre que, dados $a, b, c \in \mathbb{N}$, com $a \neq 0$, temos $(a^b)^c = a^{(bc)}$.

Capítulo 3

Números Inteiros

3.1 Introdução

Agora vamos usar o que temos sobre os naturais para conseguir definir o conjunto dos inteiros. Isto é, uma vez que se tenha os números naturais, apresentaremos um método que se obtém os inteiros.

Podemos pensar os números inteiros como representantes de "diferenças" entre números naturais. Por exemplo, o 5 representa a diferença entre 7 e 2 (quanto falta para o 2 "chegar" no 7). Já o -3 representa a diferença entre 8 e 11. Ou seja, para definirmos os inteiros, podemos usar pares de naturais. Desta forma, poderíamos representar o 5 como $(7, 2)$ e o -3 por $(8, 11)$. Veremos no que se segue que fazer essa representação nos facilita muitos casos. Mas ela tem um incoveniente: por exemplo, os pares $(4, 1)$ e $(7, 4)$ representam ambos o número 3. Veremos na próxima seção uma maneira de lidar com essa repetição. Tal método nos será útil em muitas outras situações.

3.2 Relações de equivalência

Antes de definirmos os inteiros, precisaremos do conceito de relação de equivalência.

Definição 3.2.1. Seja X um conjunto. Dizemos que uma relação $\sim$ é uma **relação de equivalência** se são satisfeitas:

(a) Para todo $x \in X$, temos que $x \sim x$; (**reflexiva**)

(b) Para todos $x, y \in X$, temos que $x \sim y \to y \sim x$. (**simétrica**)

(c) Para todos $x, y, z \in X$, temos que $(x \sim y \wedge y \sim z) \to x \sim z$. (**transitiva**)

Primeiramente, note que a igualdade é uma relação de equivalência:

Exemplo 3.2.2. A igualdade é uma relação de equivalência sobre um conjunto X, já que, para todo $x \in X$ temos que $x = x$. Também temos que se $x = y$ então $y = x$ para quaisquer $x, y \in X$. E, por último, temos que se $x = y$ e $y = z$, então $x = z$ para todo $x, y, z \in X$.

Uma ideia aqui é pensar Y como um conjunto de cores. Assim, $f(x)$ é a cor de x e a classe de x são os elementos com a mesma cor de x.

Proposição 3.2.3. *Seja $f : X \longrightarrow Y$ uma função. Então a relação $\sim$ dada por $a \sim b$ se, e somente se, $f(a) = f(b)$ para todo $a, b \in X$ é uma relação de equivalência sobre X.*

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $a \in X$. Note que $f(a) = f(a)$, logo $a \sim a$.

(b) Sejam $a, b \in X$. Note que, se $a \sim b$, então $f(a) = f(b)$ e, portanto $b \sim a$ (pois $f(b) = f(a)$).

(c) Sejam $a, b, c \in X$. Suponha $a \sim b$ e $b \sim c$. Então $f(a) = f(b)$ e $f(b) = f(c)$. Assim $f(a) = f(c)$ e, portanto, $a \sim c$ como queríamos.

□

Uma relação de equivalência serve para agrupar elementos "similares":

Definição 3.2.4. Seja X um conjunto e $\sim$ uma relação de equivalência sobre X. Dado $x \in X$, denotamos por $[x]$ (ou $\overline{x}$) o conjunto $\{y \in X : y \sim x\}$ (**classe de equivalência** de x). Denotamos por $X/\sim$ o conjunto de todas as classes de equivalência, isto é, $X/\sim = \{[x] : x \in X\}$.

O seguinte lema nos vai ser útil em diversos resultados:

Lema 3.2.5. *Seja $\sim$ uma relação de equivalência sobre X. Sejam $a, b \in X$. Se existe $x \in [a] \cap [b]$, então $[a] = [b]$.*

Demonstração. Temos que mostrar que $[a] \subset [b]$ e que $[b] \subset [a]$. Seja $y \in [a]$. Então $y \sim a$. Como $x \sim a$ (pois $x \in [a]$), temos que $y \sim x$. Como $x \sim b$, temos que $y \sim b$. Logo, $y \in [b]$. Assim mostramos que $[a] \subset [b]$. Analogamente, mostramos que $[b] \subset [a]$ (exercício). □

Esse agrupamento muitas vezes é útil:

Proposição 3.2.6. *Seja $f : X \longrightarrow Y$ uma função. Considere $\sim$ a relação de equivalência sobre X dada por, para $a, b \in X$, $a \sim b$ se, e somente se, $f(a) = f(b)$. Então a função $\tilde{f} : X/\sim \longrightarrow Y$ dada por $\tilde{f}([a]) = f(a)$ é injetora.*

Demonstração. Primeiramente, vamos mostrar que $\tilde{f}$ está bem definida. Isto porque usamos um "representante" da classe $[a]$ para para definir quanto é $\tilde{f}([a])$. Poderia ser que alguém tomasse $b \in [a]$ e tivesse um resultado diferente. Vamos mostrar que não. Seja $b \in [a]$. Então $b \sim a$. Logo, $f(b) = f(a)$. Assim, dado qualquer representante b da classe $[a]$, $\tilde{f}([a]) = f(a) = f(b)$.

Vamos agora mostrar que tal função é, de fato, injetora. Sejam $[a], [b] \in X/\sim$. Suponha que $\tilde{f}([a]) = \tilde{f}([b])$. Vamos mostrar que $[a] = [b]$. Note que temos $f(a) = f(b)$. Logo, $a \sim b$ e, portanto, $b \in [a]$. Pelo Lema **3.2.5**, temos que $[a] = [b]$. □

Definição 3.2.7. Seja X um conjunto. Chamamos uma família $\mathcal{F}$ de subconjuntos de X de uma **partição** de X se são satisfeitas:

(a) $\bigcup_{F \in \mathcal{F}} F = X$;

(b) Se $A, B \in \mathcal{F}$ são distintos, então $A \cap B = \emptyset$.

Proposição 3.2.8. *Seja $\mathcal{F}$ uma partição sobre um conjunto X. Então $\sim$ definido por $a \sim b$ (para $a, b \in X$) se, e somente se, existe $F \in \mathcal{F}$ tal que $a, b \in F$ é uma relação de equivalência sobre X. Esta é chamada de* **relação de equivalência induzida** *por $\mathcal{F}$.*

Veja o exercício 3.2.13 para o processo contrário.

Demonstração. Vamos mostrar os axiomas de relação de equivalência para $\sim$:

(a) Seja $x \in X$. Como $\bigcup_{F \in \mathcal{F}} F = X$, existe $F \in \mathcal{F}$ tal que $x \in F$. Logo, $x \sim x$ (pois $x \in F$).

(b) Sejam $x, y \in X$ tais que $x \sim y$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$. Logo, $y \sim x$.

(c) Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$. Então existe $F \in \mathcal{F}$ tal que $x, y \in F$ e existe $G \in \mathcal{F}$ tal que $y, z \in G$. Note que $y \in F \cap G$. Pelo axioma (b) de partição, se F e G fossem distintos, teríamos $F \cap G = \emptyset$. Logo, $F = G$. Assim, $x, y, z \in F$ e, portanto, $x \sim z$.

□

Alongamentos

Alongamento 3.2.9. Considere a igualdade como uma relação de equivalência sobre um conjunto X. Dado $x \in X$, quem é o conjunto $[x]$?

Alongamento 3.2.10. Mostre que se na Proposição 3.2.6 supormos também que f é sobrejetora, então $\tilde{f}$ é bijetora.

Alongamento 3.2.11. Seja $f : X \to Y$ uma função. Seja $\sim$ uma relação de equivalência sobre Y. Mostre $\simeq$ dada por $a \simeq b$ se $f(a) \simeq f(b)$ é uma relação de equivalência sobre X. Prove a Proposição 3.2.3 usando esse alongamento.

Exercícios

Exercício 3.2.12. Considere as mesmas hipóteses da Proposição **3.2.8**.

(a) Mostre que, para todo $x \in X$, existe um único $F_x \in \mathcal{F}$ tal que $x \in F_x$;

(b) Na notação do item anterior, mostre que $F_x = [x]$, considerando a relação de equivalência induzida por $\mathcal{F}$.

Exercício 3.2.13. A ideia deste exercício é complementar a Proposição 3.2.8. Seja $\sim$ uma relação de equivalência sobre X.

(a) Seja $x \in X$. Mostre que existe $y \in X$ tal que $x \in [y]$.

(b) Sejam $x, y \in X$. Mostre que se $[x], [y]$ forem distintos (como conjuntos), então $[x] \cap [y] = \emptyset$.

(c) Mostre $\{[x] : x \in X\}$ é uma partição sobre X. Esta é chamada de **partição induzida** pela relação de equivalência $\sim$.

Exercício 3.2.14. Considere $f : X \to Y$ sobrejetora e $g : Y \to Z$ injetora. Considere $\sim$ relação de equivalência sobre X dada por $a \sim b$ se $g(f(a)) = g(f(b))$ Mostre que existe uma função bijetora entre $X/\sim$ e Y

Note que isso é de fato uma relação de equivalência pela Proposição 3.2.3.

3.3 Definição e operações básicas

Proposição 3.3.1. *Considere a relação $\sim$ sobre $\mathbb{N}^2$ dada por*

$$(a, b) \sim (c, d) \text{ se, e somente se } a + d = c + b$$

onde $(a, b), (c, d) \in \mathbb{N}^2$. Então $\sim$ é uma relação de equivalência[1] *sobre $\mathbb{N}^2$.*

[1] A inspiração desta relação de equivalência vem do seguinte. Queremos que $a-b = c-d$. Ou seja, queremos que $a + d = c + b$.

Demonstração. Vamos mostrar os axiomas de relação de equivalência:

(a) Seja $(a, b) \in \mathbb{N}^2$. Temos que $a + b = a + b$, logo $(a, b) \sim (a, b)$.

(b) Sejam $(a, b), (c, d) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$. Temos que $c + b = a + d$, logo $(c, d) \sim (a, b)$.

(c) Sejam $(a, b), (c, d), (e, f) \in \mathbb{N}^2$ tais que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos $a + d = c + b$. Logo $a + d + f = c + b + f$. Também temos que $c + f = e + d$. Logo, temos $c + f + b = e + d + b$. Desta forma obtemos $a + d + f = e + d + b$ e, portanto, $a + f = e + b$. Isto é, $(a, b) \sim (e, f)$.

□

Definição 3.3.2. Chamamos de $\mathbb{Z}$ o conjunto $\mathbb{N}^2/\sim$ onde $\sim$ é a relação de equivalência definida no item anterior. Cada elemento de $\mathbb{Z}$ é chamado de **número inteiro**.

Definição 3.3.3. Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$. Definimos[2] $[(a, b)] + [(c, d)] = [(a + c, b + d)]$ (**soma nos inteiros**).

Proposição 3.3.4. *A operação de soma está bem definida.*

Demonstração. Precisamos mostrar que tal definição independe dos representantes de classe tomados. Ou seja, precisamos mostrar que se $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$ então $(a + c, b + d) \sim (x + w, y + z)$. Temos que $a + y = b + x$ e que $c + z = d + w$. Assim

$$\begin{aligned}(a + c) + (y + z) &= (a + y) + (c + z) \\ &= (b + x) + (d + w) \\ &= (b + d) + (x + w)\end{aligned}$$

□

Proposição 3.3.5. *Temos que a soma satisfaz as seguintes propriedades:*

(a) Comutativa;

(b) Associativa;

[2] A inspiração para essa definição vem do seguinte: queremos definir $(a - b) + (c - d)$ e isso é igual a $(a + c) - (b + d)$.

Demonstração. Vamos mostrar que ela é comutativa e vamos deixar a associativa como Exercício (**3.3.14**). Sejam $[(a,b)],[(c,d)] \in \mathbb{Z}$. Vamos mostrar que $[(a,b)]+[(c,d)] = [(c,d)]+[(a,b)]$. Temos

$$\begin{aligned} [(a,b)]+[(c,d)] &= [(a+c,b+d)] \\ &= [(c+a,d+b)] \\ &= [(c,d)]+[(a,b)] \end{aligned}$$

□

Proposição 3.3.6. *Para qualquer* $[(a,b)] \in \mathbb{Z}$*, temos que* $[(a,b)]+[(0,0)] = [(a,b)]$

Demonstração. Basta notar que $(a+0,b+0) \sim (a,b)$, já que $a+0+b = b+0+a$. □

Proposição 3.3.7 (**Lei do Cancelamento**)**.** *Sejam* $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$*. Se* $[(a,b)]+[(x,y)] = [(c,d)]+[(x,y)]$*, então* $[(a,b)] = [(c,d)]$.

Demonstração. Temos que $[(a+x,b+y)] = [(c+x,d+y]]$. Assim, $a+x+d+y = b+y+c+x$. Assim, cancelando $x+y$, temos $a+d = b+c$, isto é, $(a,b) \sim (c,d)$. □

Definição 3.3.8. Sejam $[(a,b)]$, $[(c,d)] \in \mathbb{Z}$. Definimos[3] $[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$. Este é o **produto nos inteiros**. Assim como fizemos com $\mathbb{N}$, omitiremos o sinal $\cdot$ normalmente.

Proposição 3.3.9. *A operação de produto está bem definida.*

Demonstração. Ver o Exercício **3.3.17**. □

Proposição 3.3.10. *Valem as seguintes propriedades para o produto.*

(a) Associativa;

(b) Comutativa;

Demonstração. Ver Exercício 3.3.18 □

Proposição 3.3.11. *Vale a propriedade distributiva entre a soma e o produto em* $\mathbb{Z}$*. Isto é, dados* $[(a,b)],[(c,d)],[(x,y)] \in \mathbb{Z}$*, temos que*

$$[(x,y)]([(a,b)+(c,d)]) = ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])$$

[3] A inspiração para essa definição é: queremos definir $(a-b)\cdot(c-d)$ e isso é igual a $(ac+db)-(ad-bc)$.

Demonstração. Temos

$$\begin{aligned}
[(x,y)]([(a,b)+(c,d)]) &= [(x,y)][(a+c,b+d)] \\
&= [(x(a+c)+y(b+d), x(b+d)+y(a+c))] \\
&= [(xa+xc+yb+yd, xb+xd+ya+yc)] \\
&= [(xa+yb, xb+ya)] + [(xc+yd, xd+yc)] \\
&= ([(x,y)][(a,b)]) + ([(x,y)][(c,d)])
\end{aligned}$$

□

Proposição 3.3.12. *Seja* $[(a,b)] \in \mathbb{Z}$. *Então* $[(1,0)][(a,b)] = [(a,b)]$.

Demonstração. Temos $[(a,b)][(1,0)] = [(a1+b0, a0+b1)] = [(a,b)]$. □

Exercícios

Exercício 3.3.13. Sejam $a, b \in \mathbb{N}$.

(a) Dê um exemplo de forma que $[(a,b)] = [(x,y)]$, mas $a \neq x$ e $b \neq y$.

(b) Mostre que se $[(x,b)] = [(a,b)]$, então $x = a$.

(c) Enuncie e prove o análo ao exercício anterior, fixando a primeria coordenada.

Exercício 3.3.14. Mostre que vale a propriedade associativa para a soma em $\mathbb{Z}$.

Exercício 3.3.15. Mostre que o elemento neutro da soma é único, isto é, dado $[(a,b)] \in \mathbb{Z}$ tal que para todo $[(x,y)] \in \mathbb{Z}$ temos que $[(x,y)] + [(a,b)] = [(x,y)]$, então $[(a,b)] = [(0,0)]$.

Exercício 3.3.16. Mostre que $[(a,b)] \in \mathbb{Z}$ é tal que $[(a,b)] = [(0,0)]$ se, e somente se, $a = b$.

Exercício 3.3.17. Mostre que o produto dos inteiros está bem definido.

Exercício 3.3.18. Mostre as propriedades associativa e comutativa para o produto em $\mathbb{Z}$.

Exercício 3.3.19. Mostre que o elemento neutro do produto é único.

Exercício 3.3.20. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$.

(a) Mostre que $[(a,b)][(0,1)] = [(b,a)]$;

(b) Mostre que $[(a,b)] + [(b,a)] = [(0,0)]$;

(c) Mostre que se $[(a,b)] + [(c,d)] = [(0,0)]$, então $[(a,b)] = [(d,c)]$.

3.4 Forma canônica e ordem

Proposição 3.4.1. *Seja* $[(a,b)] \in \mathbb{Z}$. *Então existe* $x \in \mathbb{N}$ *tal que* $[(a,b)] = [(x,0)]$ *ou* $[(a,b)] = [(0,x)]$.

Demonstração. Vamos separar em 3 casos:

$a = b$**:** Neste caso, tomamos $x = 0$ e $[(a,b)] = [(0,0)]$ (ver Exercício **3.3.16**).

$a < b$**:** Seja $m \in \mathbb{N}$ tal que $a + m = b$. Vamos mostrar que $(a,b) \sim (0,m)$. De fato, temos que $a + m = b + 0$.

$b < a$**:** Seja $m \in \mathbb{N}$ tal que $b + m = 0$. Vamos mostrar que $(a,b) \sim (m,0)$. De fato, temos que $a + 0 = b + m$.

□

Definição 3.4.2. Dizemos que um elemento de $\mathbb{Z}$ está escrito na **forma canônica** se ele está escrito na forma $[(x,0)]$ ou $[(0,x)]$. Pelo resultado anterior, temos que todo elemento pode ser escrito na forma canônica. Note que tal representação é única (ver Exercício **3.4.13**).

Escrever os elementos na forma canônica muitas vezes facilita demonstrações:

Proposição 3.4.3. *Sejam* $[(a,b)], [(c,d)] \in \mathbb{Z}$ *tais que* $[(a,b)][(c,d)] = [(0,0)]$. *Então* $[(a,b)] = [(0,0)]$ *ou* $[(c,d)] = [(0,0)]$.

Demonstração. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Temos 4 casos. Vamos mostrar 2, deixando os outros dois como exercício:

- Pela definição do produto, temos $[(x,0)][(y,0)] = [(xy,0)]$. De $[(xy,0)] = [(0,0)]$, temos que $xy = 0$ (pelo Exercício 3.3.13). Logo, $x = 0$ ou $y = 0$ e, portanto, $[(a,b)] = [(0,0)]$ ou $[(c,d)] = [(0,0)]$.
- Pela definição do produto, temos que $[(x,0)][(0,y)] = [(0,xy)]$. Como no caso anterior, temos que $xy = 0$ e, portanto, $x = 0$ ou $y = 0$. Assim $[(a,b)] = [(0,0)]$ ou $[(c,d)] = [(0,0)]$.

□

Definição 3.4.4. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Seja $x \in \mathbb{N}$ tal que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e seja $y \in \mathbb{N}$ tal que $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Dizemos que $[(a,b)] \leq [(c,d)]$ se, e somente se, ocorre um dos seguintes casos:

- $[(a,b)] = [(x,0)]$, $[(c,d)] = [(y,0)]$ e $x \leq y$;
- $[(a,b)] = [(0,x)]$, $[(c,d)] = [(y,0)]$;
- $[(a,b)] = [(0,x)]$, $[(c,d)] = [(0,y)]$ e $y \leq x$.

Esta é a **ordem usual sobre os inteiros**

Proposição 3.4.5. *A ordem sobre os inteiros é total.*

Demonstração. Sejam $[(a,b)], [(c,d)] \in \mathbb{Z}$. Temos que mostrar que $[(a,b)] \leq [(c,d)]$ ou $[(c,d)] \leq [(a,b)]$. Sejam $x, y \in \mathbb{N}$ tais que $[(a,b)] = [(x,0)]$ ou $[(a,b)] = [(0,x)]$ e $[(c,d)] = [(y,0)]$ ou $[(c,d)] = [(0,y)]$. Vamos analisar os casos:

- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(y,0)]$. Se $x \leq y$, temos que $[(x,0)] \leq [(y,0)]$. Caso contrário, temos que $y \leq x$ e, portanto, $[(y,0)] \leq [(x,0)]$.
- Se $[(a,b)] = [(x,0)]$ e $[(c,d)] = [(0,y)]$, então $[(0,y)] \leq [(x,0)]$.

Os outros casos são análogos. □

Definição 3.4.6. Denotamos por x o elemento $[(x,0)]$. Denotamos por $-x$ o elemento $[(0,x)]$. Assim, denotamos por $x+(-y)$ o elemento $[(x,0)]+[(0,y)]$. Muitas vezes, omitimos o $+$, ficando apenas $x - y$. Chamamos de **positivo** um elemento da forma $[(x,0)]$ e de **negativo** um da forma $[(0,y)]$.

Proposição 3.4.7. *(a) O produto de dois positivos é positivo;*

(b) O produto de dois negativos é positivo;

(c) O produto de um positivo com um negativo é negativo;

Demonstração. Sejam $a, b \in \mathbb{N}$.

(a) Temos que $[(a,0)][(b,0)] = [(ab,0)]$;

(b) Temos que $[(0,a)][(0,b)] = [(ab,0)]$;

(c) Temos que $[(a,0)][(0,b)] = [(0,ab)]$.

□

Definição 3.4.8. Dado $[(a,b)] \in \mathbb{Z}$, denotamos por $-[(a,b)]$ o elemento $[(b,a)]$.

Proposição 3.4.9. *Sejam $a, b \in \mathbb{Z}$. Temos:*

(a) $-(-a) = a$;

(b) $a(-b) = -(ab)$;

Demonstração. (a) Seja $[(x, y)] = a$. Então $-(-[(x, y)]) = -[(y, x)] = [(x, y)]$.

(b) Sejam $[(x, y)] = a$ e $[(w, z)] = b$. Temos

$$\begin{aligned} a(-b) &= [(x, y)](-([w, z])) \\ &= [(x, y)][(z, w)] \\ &= [(xz + yw, xw + yz)] \\ &= -[(xw + yz, xz + yw)] \\ &= -([(x, y)][(w, z)]) \end{aligned}$$

□

Proposição 3.4.10. *Dado um elemento $z \in \mathbb{Z}$, temos que z é positivo se, e somente se, $-z$ é negativo.*

Demonstração. Suponha z positivo. Então existe $a \in \mathbb{N}$ tal que $z = [(a, 0)]$. Assim, $-z = -[(a, 0)] = [(0, a)]$ e, portanto, é negativo. Por outro lado, se $-z$ é negativo, existe $a \in \mathbb{N}$ tal que $-z = [(0, a)]$. Logo, $z = -(-z) = -[(0, a)] = [(a, 0)]$ é positivo. □

Alongamentos

Alongamento 3.4.11. Mostre que $(-1)(-1) = 1$.

Alongamento 3.4.12. Seja $a \in \mathbb{Z}$. Mostre que $-a = (-1)a$.

Exercícios

Exercício 3.4.13. Mostre que cada elemento de $\mathbb{Z}$ tem apenas uma única representação na forma canônica.

Exercício 3.4.14. Mostre a **Lei do Cancelamento** do produto em $\mathbb{Z}$: Dados $[(a, b)], [(c, d)], [(x, y)] \in \mathbb{Z}$ tais que $[(a, b)][(x, y)] = [(c, d)][(x, y)]$ e $[(x, y)] \neq [(0, 0)]$, então $[(a, b)] = [(c, d)]$.

Exercício 3.4.15. Sejam $a, b \in \mathbb{Z}$ mostre que $a \leq b$ se, e somente se, existe $m \in \mathbb{Z}$ positivo tal que $a + m = b$.

Exercício 3.4.16. Mostre que $z \in \mathbb{Z}$ é positivo se, e somente se, $z \geq 0$ $(0 = [(0, 0)])$.

Exercício 3.4.17. Sejam $a, b, c \in \mathbb{Z}$.

(a) Mostre que se $a \leq b$, então $a + c \leq b + c$;

(b) Mostre que se $a \leq b$ e $c \geq 0$, então $ac \leq bc$;

(c) Mostre que se $a \leq b$ e $c \leq 0$, então $bc \leq ac$.

3.5 Divisibilidade e valor absoluto

Vamos identificar $\mathbb{N} = \{z \in \mathbb{Z} : z \geq 0\}$ da maneira usual.

Definição 3.5.1. Dados $a, b \in \mathbb{Z}$, dizemos que a **divide** b (e denotamos por $a|b$) se existe $m \in \mathbb{Z}$ tal que $am = b$.

Proposição 3.5.2. *Sejam $a, b, c \in \mathbb{Z}$. Temos:*

(a) $1|a$;

(b) $a|0$;

(c) $a|a$;

(d) Se $a|b$ e $b|c$, então $a|c$.

Demonstração. (a) Basta notar que $1a = a$.

(b) Basta notar que $a0 = 0$.

(c) Basta notar que $a1 = a$.

(d) Seja $m \in \mathbb{Z}$ tal que $am = b$. Seja $n \in \mathbb{Z}$ tal que $bn = c$. Vamos provar que $a(mn) = c$. De fato, $a(mn) = (am)n = bn = c$.

□

Proposição 3.5.3. *Sejam $a, b \in \mathbb{Z}$. Então $ab = (-a)(-b)$.*

Demonstração. Temos $(-a)(-b) = (-1a)(-1b) = (-1)(-1)(a)(b) = ab$. □

Nos naturais, temos uma única possibilidade para que um produto dê 1:

Lema 3.5.4. *Se $a, b \in \mathbb{N}$ são tais que $ab = 1$, então $a = b = 1$.*

Demonstração. Note que $b \neq 0$ (pois $a0 = 0 \neq 1$). Assim, existe $m \in \mathbb{N}$ tal que $b = m + 1$. Substituindo, temos $ab = a(m + 1) = am + a$. Isto é, $a + am = 1$. Assim, temos que $a \leq 1$. Como $a \in \mathbb{N}$, temos $a = 0$ ou $a = 1$. Como $a \neq 0$ (pois $0b = 0 \neq 1$), temos que $a = 1$. Como $1b = 1 \cdot 1$, temos, pela lei do cancelamento, que $b = 1$. □

Já nos inteiros, temos duas possibilidades para um produto dar 1:

Lema 3.5.5. *Se $a, b \in \mathbb{Z}$ são tais que $ab = 1$, então $a = b = 1$ ou $a = b = -1$.*

Demonstração. Temos 3 casos: a, b são positivos, a, b são negativos e o terceiro caso é o que um é positivo e o outro é negativo (neste último caso, podemos supor sem problemas que a é positivo e b é negativo). Note também que, claramente, a, $b \neq 0$.

- $a, b > 0$. Neste caso, pelo lema anterior, temos que $a, b = 1$.
- $a, b < 0$. Note que
$$\begin{aligned} 1 &= ab \\ &= (-a)(-b) \end{aligned}$$
Como $(-a), (-b)$ são positivos, temos que $-a, -b = 1$ e, portanto, $a, b = -1$.
- $a > 0$ e $b < 0$. Note que, neste caso, $ab < 0$ e, portanto, não pode ser 1 (ou seja, esse caso era impossível de ocorrer).

□

Proposição 3.5.6. *Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $a = b$ ou $a = -b$.*

Demonstração. Primeiramente, note que se $b = 0$, como $b|a$, temos que $a = 0$ e, portanto, o resultado vale. Logo, podemos supor agora que $b \neq 0$. De $a|b$, temos que existe $m \in \mathbb{Z}$ tal que $am = b$. De $b|a$, temos que existe n tal que $bn = a$. Assim, de $am = b$, temos que $(bn)m = b$. Como $b \neq 0$, pela lei do cancelamento, temos que $nm = 1$. Pelo lema anterior, $n = m = 1$ ou $n = m = -1$ e temos o resultado. □

Teorema 3.5.7 (Princípio do menor elemento)**.** *Seja $S \subset \mathbb{N}$. Se $S \neq \emptyset$, então existe $m \in S$ mínimo de S (isto é, $m \leq s$ para todo $s \in S$).*

Demonstração. Considere o conjunto

$$M = \{x \in \mathbb{N} : \text{para todo } s \in S,\ x \leq s\}.$$

Note que $0 \in M$. Como $S \neq \emptyset$, temos que existe $s \in S$. Note que $s+1 \notin M$. Logo, $M \neq \mathbb{N}$. Considere a propriedade $P(x)$ como $x \in M$. Note que temos $P(0)$. Logo, como tal propriedade não pode valer para todo $x \in \mathbb{N}$, temos que existe $n \in \mathbb{N}$ tal que $P(n) \not\to P(n+1)$ (pois a indução não pode valer).

Isto é, existe $n \in \mathbb{N}$ tal que $P(n)$ e $\sim P(n+1)$. Vamos mostrar que tal n é o mínimo de S. Como vale $P(n)$, temos que $n \leq s$ para todo $s \in S$. Resta mostrar que $n \in S$. Suponha que não. Então vale que, para qualquer $s \in S$, $n < s$. Logo, $n + 1 \leq s$ (pelo Lema **2.5.4**) para qualquer $s \in S$. Assim, $n + 1 \in M$ e, portanto, $P(n + 1)$, contradição. □

Teorema 3.5.8 (Algoritmo da divisão de Euclides)**.** *Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então existem inteiros q e r tais que $a = bq + r$ com $0 \leq r < b$.*

Demonstração. Considere o conjunto

$$S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Note que $S \neq \emptyset$, pois tomando $x = 0$, temos que $a - bx = a \geq 0$. Seja r o menor elemento de S. Assim, para algum $q \in \mathbb{Z}$, temos que $r = a - bq$. Logo, $r + bq = a$. Note que, como $r \in S$, $r \geq 0$.

Se mostrarmos que $r < b$ terminamos. Suponha que não. Temos

$$\begin{array}{rcl} 0 & \leq & r - b \\ & = & (a - bq) - b \\ & = & a - b(q + 1) \end{array}$$

Note então que $a - b(q + 1) \in S$. E note que $a - b(q + 1) = a - bq - b < a - bq = r$, j que $b > 0$. Mas isso contradiz a minimalidade de r. □

Definição 3.5.9. Dado $z \in \mathbb{Z}$, definimos o valor absoluto de z (denotado por $|z|$) da seguinte maneira:

$$|z| = \begin{cases} z & \text{se } z \geq 0 \\ -z & \text{se } z < 0 \end{cases}$$

Proposição 3.5.10. *Sejam $a, b \in \mathbb{Z}$. Temos que valem as seguintes afirmações:*

(a) $|a| \geq 0$*;*

(b) $|a| = 0 \rightarrow a = 0$*;*

(c) $a \leq |a|$*;*

Demonstração. (a) Se $a \geq 0$, temos que $|a| = a \geq 0$. Se $a < 0$, temos que $|a| = -a > 0$.

(b) Suponha que $a \neq 0$. Se $a > 0$, temos que $|a| = a > 0$ e, portanto $|a| \neq 0$. Se $a < 0$, temos que $|a| = -a > 0$ e novamente temos que $|a| \neq 0$.

(c) se $a \geq 0$, temos que $|a| = a$ e, portanto, $a \leq |a|$. Se $a < 0$, temos que $a < |a|$ pelo item (a).

□

Exercícios

3.5.1. Mostre que $|$ é uma ordem sobre $\mathbb{N}$. Ela é uma ordem sobre $\mathbb{Z}$?

3.5.2. Mostre que dado $a \in \mathbb{Z}$, temos que $-|a| \leq a$.

3.5.3. Sejam $a, b \in \mathbb{Z}$.

(a) Mostre que $a + b \leq |a| + |b|$;

(b) Mostre que $-(|a| + |b|) \leq a + b$;

(c) Mostre que $|a + b| \leq |a| + |b|$.

3.5.4. Sejam $a, b \in \mathbb{Z}$. Mostre que $|ab| = |a||b|$.

3.5.5. Sejam $a, b \in \mathbb{Z}$.

(a) Se $a < 0$ e $b > 0$, mostre que existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < b$.

(b) Se $b < 0$, mostre que existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < |b|$.

(c) Conclua o caso geral do **Algoritmo da divisão de Euclides**: Dados $a, b \in \mathbb{Z}$ tais que $b \neq 0$, existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < |b|$.

3.5.6. Considere uma fila de pessoas em que a primeira pessoa é uma mulher e a última é um homem. Mostre que há pelo menos um homem que está imediatamente atrás de uma mulher.

3.6 Números primos

Um conceito bastante útil é o de número primo:

Veja o Alongamento 3.6.15.

Definição 3.6.1. Dado um $p \in \mathbb{N}$, dizemos que p é **primo** se $p > 1$ e se $a \in \mathbb{N}$ é tal que $a|p$, então $a = p$ ou $a = 1$.

O próximo resultado vai facilitar algumas demonstrações por indução ou por argumentos de minimalidade:

Proposição 3.6.2. *Sejam $a, b \in \mathbb{N}$ tais que $a, b > 1$. Se $a|b$, então $a \leq b$.*

Demonstração. Como $a|b$, existe $n \in \mathbb{N}$ tal que $an = b$. Note que $n \neq 0$ pois $b \neq 0$. Assim, existe $m \in \mathbb{N}$ tal que $n = m + 1$. Temos

$$\begin{aligned} b &= an \\ &= a(m+1) \\ &= am + a \end{aligned}$$

Logo, $a \leq b$. □

Já temos material suficiente para provar que todo número maior que 1 é divisível por algum primo:

Proposição 3.6.3. *Dado $a \in \mathbb{N}$, com $a > 1$, existe p primo tal que $p|a$.*

Demonstração. Seja $D = \{n \in \mathbb{N} : n > 1 \text{ e } n|a\}$. Note que $D \neq \emptyset$ já que $a \in D$. Seja p o mínimo de D. Vamos mostrar que p é primo. Suponha que não. Então existe d tal que $d > 1$, $d \neq p$ e $d|p$. Pela Proposição 3.6.2, temos que $d < p$. Note que, como $d|p$ e $p|a$, temos que $d|a$. Logo, $d \in D$ contrariando a minimalidade de p. □

Com o resultado anterior, podemos decompor cada $a > 1$ em fatores primos:

Proposição 3.6.4. *Dado $a \in \mathbb{N}$, com $a > 1$. Então existem $p_1, ..., p_n$ primos tais que $a = p_1 \cdot \cdots \cdot p_n$.*

Demonstração. Considere $A = \{a \in \mathbb{N} : a > 1 \text{ e existem } p_1, ..., p_n \text{ primos tais que } a = p_1 \cdot \cdots \cdot p_n\}$. Temos que mostrar que $A = \{a \in \mathbb{N} : a > 1\}$. Suponha que não. Então $\{a \in \mathbb{N} : a > 1\} \setminus A$ é não vazio. Seja m o mínimo de tal conjunto. Note que $m > 1$. Pela Proposição 3.6.3, existe p primo tal que $p|m$. Pela Proposição 3.6.2, temos dois casos $p = m$ ou $p < m$. Se $p = m$, temos uma contradição com a definição de m (pois $m \notin A$).

Se $p < m$, note que existe k tal que $pk = m$ e tal que $k > 1$ (se $k = 0$, teríamos $m = 0$ e se $k = 1$, teríamos $m = p$). Assim, pela minimalidade m, temos que existem $p_1, ..., p_n$ tais que $k = p_1 \cdot \cdots \cdot p_n$. Logo, $m = (p_1 \cdot \cdots \cdot p_n)p$, contrariando a definição de m. □

Definição 3.6.5. Sejam $a, b \in \mathbb{Z}$. Dizemos que d é um **máximo divisor comum** de a e b se

(a) $d \geq 0$;

Essa definição não se parece muito com o que o nome indica - mas veremos depois que ela chega no mesmo lugar - mas ela é mais prática neste contexto.

(b) $d|a$ e $d|b$;

(c) Se e satisfaz (a) e (b), então $e|d$.

Proposição 3.6.6. *Se d e e são máximos divisores comuns de a e b, então $d = e$.*

Demonstração. Basta notar que $d|e$ e $e|d$. Logo, como ambos são positivos, temos que $d = e$. □

Proposição 3.6.7. *Sejam $a, b \in \mathbb{Z}$ com $a, b \neq 0$. Então o mínimo do conjunto $\{ax + by : ax + by > 0 \text{ e } x, y \in \mathbb{Z}\}$ é o máximo divisor comum de a e b.*

Demonstração. Vamos chamar o conjunto do enunciado de A. Note que $A \neq \emptyset$ (exercício). Assim, seja d o mínimo de A. Note que $d > 0$. Sejam $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Vamos mostrar que $d|a$. Suponha que não. Aplique o algoritmo da divisão de Euclides e tome $a = dq + r$ com $0 < r < d$. Note que

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)q \\ &= a(1 - xq) - b(yq) \end{aligned}$$

Logo $r \in A$, contrariando a minimalidade de d. Podemos provar de maneira análoga que $d|b$. Assim, só nos resta mostrar que dado $e \geq 0$ tal que $e|a$ e $e|b$ temos que $e|d$. Como $e|a$, existe m tal que $em = a$. Como $e|b$, existe n tal que $en = b$. Assim, temos

$$\begin{aligned} d &= ax + by \\ &= emx + eny \\ &= e(mx + ny) \end{aligned}$$

Logo, $d|e$ como queríamos. □

Observação 3.6.8. Note que se $a = 0$, pode ser que o máximo divisor comum entre a e b não exista. Por exemplo, não existe máximo divisor comum entre 0 e 3, pois o único divisor de 0 é o próprio 0 e 0 não é divisor de 3.

Definição 3.6.9. Dados $a, b \in \mathbb{Z}_{\neq 0}$, chamamos de $mdc(a, b)$ o máximo divisor comum de a e b.

Finalmente, podemos também definir o máximo divisor comum entre a e b de forma mais "próxima" de seu nome:

Proposição 3.6.10. *Sejam $a, b \in \mathbb{Z}_{\neq 0}$. Então M é o máximo divisor comum entre a e b se, e somente se, $M|a$, $M|b$ e, dado qualquer n tal que $n|a$ e $n|b$, temos que $n \leq M$.*

Demonstração. Suponha que M é o máximo divisor comum entre a, b. Pela definição, já temos que $M|a$ e $M|b$. Assim, dado n tal que $n|a$ e $n|b$, resta mostrar que $n \leq M$. Temos dois casos:

- Se $n < 0$, então $n < M$, já que $M \geq 0$.
- Se $n \geq 0$, então pela definição de máximo divisor comum entre a e b, temos que $n|M$. Logo, como $M, n \in \mathbb{N}$, pela Proposição 3.6.2, temos que $n \leq M$ como queríamos.

Agora suponha M como no enunciado. Primeiramente, note que $M \geq 0$. Pois, caso contrário, teríamos que $-M$ também seria um divisor de a e b e $M < -M$, contrariando a definição de M. Assim, M satisfaz as condições (a) e (b) da definição de máximo divisor comum. Seja $d = mdc(a, b)$. Pela definição de d, temos que $M|d$. Ou seja, $M \leq d$. Por outro lado, temos que $d \leq M$ pela definição de M. Logo, $M = d$. □

Proposição 3.6.11. *Se p é primo e $p \nmid a$ para $a \in \mathbb{Z}$, então $mdc(p, a) = 1$.*

Demonstração. Seja $d \geq 0$ tal que $d|a$ e $d|p$. Note que, como p é primo, temos que $d = p$ ou $d = 1$. Como $p \nmid a$, temos que $d = 1$. □

Proposição 3.6.12. *Sejam p primo e $a, b \in \mathbb{Z}$ tais que $p|ab$. Então $p|a$ ou $p|b$.*

Demonstração. Suponha que $p \nmid a$. Então $mdc(a, p) = 1$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + py = 1$. Assim, temos que $b = abx + pby$. Seja k tal que $pk = ab$. Temos que $b = pkx + pby = p(kx + by)$. Logo, $p|b$. □

Corolário 3.6.13. *Se p é um primo e $p|a_1 \cdots a_n$, então existe j tal que $p|a_j$.*

Demonstração. Vamos provar por indução sobre n. Note que o caso $n = 2$ é o que foi feito anteriormente. Agora suponha que vale o caso n e vamos provar o caso $n + 1$. Suponha $p|a_1 \cdots a_{n+1}$. Se $p|a_{n+1}$, terminamos. Caso contrário, $p|a_1 \cdots a_n$ (pela proposição anterior). Assim, por hipótese de indução, temos que $p|a_j$ para algum $j = 1, ..., n$. □

Teorema 3.6.14. *A decomposição feita na Proposição 3.6.4 é única a menos da ordem dos fatores.*

Só escrevemos os primos em ordem crescente

Demonstração. Seja $a \in \mathbb{Z}$ com $a > 1$. Sejam $p_1, ..., p_n, q_1, ..., q_m$ primos tais que $a = p_1 \cdot \cdots \cdot p_n = q_1 \cdot \cdots \cdot q_m$ e que $p_1 \leq \cdots \leq p_n$ e $q_1 \leq \cdots \leq q_m$. Vamos fazer o caso em que $p_1 \leq q_1$. Note que $p_1|a$ e, portanto, $p_1|q_1 \cdot \cdots \cdot q_m$. Assim, existe j tal que $p_1|q_j$. Como q_j é primo, temos que $p_1 = q_j$. Pela minimalidade de q_1, temos que $p_1 = q_1$. Assim, temos, aplicando o cancelamento que

$$p_2 \cdot \cdots \cdot p_n = q_2 \cdot \cdots \cdot q_m$$

De maneira análoga, podemos cancelar outro termo nesta igualdade. Procedemos até que sobre apenas um termo de cada lado. O que mostra que $m = n$ e que cada $p_i = q_i$. □

Alongamentos

Alongamento 3.6.15. Seja $p > 1$. Mostre que p é primo se, e somente se, p é minimal com relação a ordem $|$ (divide) restrita a $\{a \in \mathbb{N} : a > 1\}$.

Exercícios

3.6.1. Sejam $a, b \in \mathbb{Z}$. Mostre que se $a|b$, então $mdc(a, b) = |a|$.

3.6.2. Sejam $a, b \in \mathbb{Z}$. Dizemos que $x \in \mathbb{Z}$ é um múltiplo de a se existe $y \in \mathbb{Z}$ tal que $ay = x$. Defina o **mínimo múltiplo comum** (denotado por $mmc(a, b)$) como sendo o mínimo do conjunto $M = \{m \in \mathbb{N} : (\exists p \in \mathbb{Z}\ ap = m) \wedge (\exists q \in \mathbb{Z}\ bq = m)\}$. Mostre que M necessariamente é não vazio (assim garantimos a existência do mínimo).

3.6.3. Sejam $a, b \in \mathbb{N}$, tais que $a, b > 0$.

(a) Mostre que existe k tal que $b = mdc(a, b)k$;

(b) Mostre que ak é múltiplo de b;

(c) Note que $mmc(a, b) \leq ak$;

(d) Mostre que $mmc(a, b)mdc(a, b) \leq ab$.

3.7 Congruência

Definição 3.7.1. Seja $m \in \mathbb{N}$, com $m \neq 0$. Considere a seguinte relação sobre $\mathbb{Z}$: $a \equiv_m b$ se, e somente se, $m|a - b$ (para $a, b \in \mathbb{Z}$). A notação mais usual para isso é $a \equiv b \bmod m$.

Proposição 3.7.2. *A relação $\equiv_m$ definida acima é uma relação de equivalência sobre $\mathbb{Z}$.*

Demonstração. Sejam $a, b, c \in \mathbb{Z}$. Temos:

(a) $a \equiv_m a$: Temos que $m|a - a$ pois $a - a = 0$;

(b) Se $a \equiv_m b$, então $b \equiv_m a$: De fato, se $m|a - b$, então existe $n \in \mathbb{Z}$ tal que $mn = a - b$. Logo, $-nm = b - a$ e, portanto, $m|b - a$;

(c) Se $a \equiv_m b$ e $b \equiv_m c$, então $a \equiv_m c$: Seja $p \in \mathbb{Z}$ tal que $pm = a - b$ e seja $q \in \mathbb{Z}$ tal que $qm = b - c$. Temos que $pm + qm = a - b + b - c$, isto é, $(p + q)m = a - c$. Logo, $m|a - c$ com queríamos.

□

Proposição 3.7.3. *Sejam $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ com $m \neq 0$. Temos:*

(a) Se $a \equiv_m b$, então $-a \equiv_m -b$;

(b) Se $a \equiv_m b$, então $a + c \equiv_m b + c$;

(c) Se $a \equiv_m b$, então $ac \equiv_m bc$;

(d) Se $a \equiv_m b$ e $c \equiv_m d$, então $a + c \equiv_m b + d$;

(e) Se $a \equiv_m b$ e $c \equiv_m d$, então $ac \equiv_m bc$;

(f) Se $r \in \mathbb{N}$ e $a \equiv_m b$, então $a^r \equiv_m b^r$.

Demonstração. (a) Temos que $m|a - b$. Note que $m|b - a$.

(b) Temos que $m|a - b$. Note que $(a + c) - (b + c) = a - b$. Logo, $m|(a + c) - (b + c)$;

(c) Temos que $m|a - b$. Note que $m|c(a - b)$.

(d) Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c - d$. Logo, $(a + c) - (b + d) = (a - b) + (c - d) = mx + my = m(x + y)$. Logo, $m|(a + c) - (b + d)$.

(e) Temos que $m|a-b$ e $m|c-d$. Assim, existem $x, y \in \mathbb{Z}$ tais que $mx = a-b$ e $my = c - d$. Logo, $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = cmx + bmy = m(cx + by)$. Assim, $m|ac - bd$.

(f) Vamos mostrar por indução sobre r. Note que vale para $r = 0$, pois $1 \equiv_m 1$. Suponha que vale para $r = n$ e vamos mostrar para $r = n + 1$. Temos que $a \equiv_m b$, logo, pela hipótese de indução, temos que $a^n \equiv_m b^n$. Assim, pelo item (e), temos que $a^n a \equiv_m b^n b$. Isto é, $a^{n+1} \equiv_m b^{n+1}$.

□

Proposição 3.7.4. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$ com $m \neq 0$. Sejam r_1, r_2 dados pelo algoritmo da divisão de Euclides de a e b por m, isto é, $a = mq_1 + r_1$ e $b = mq_2 + r_2$ com $0 \leq r_1, r_2 < m$. Então $a \equiv_m b$ se, e somente se, $r_1 = r_2$.*

Demonstração. Suponha que $a \equiv_m b$. Queremos mostrar que $r_1 = r_2$. Seja $n \in \mathbb{Z}$ tal que $mn = a - b$. Vamos fazer o caso $r_1 \geq r_2$ (o outro é análogo). Temos

$$\begin{aligned} r_1 - r_2 &= (a - mq_1) - (b - mq_2) \\ &= (a - b) + (mq_2 - mq_1) \\ &= mn - m(q_2 - q_1) \\ &= m(n - q_2 + q_1) \end{aligned}$$

Logo, $m | r_1 - r_2$. Note que $r_1 < m$, logo, $r_1 - r_2 < m$. Assim, a única possibilidade para que $m | r_1 - r_2$ é se $r_1 - r_2 = 0$, isto é, $r_1 = r_2$ como queríamos.

Agora suponha que $r_1 = r_2$. Temos que $a - b = mq_1 - r_1 - (mq_2 - r_2) = m(q_1 - q_2)$. Isto é, $m | a - b$. □

Exemplo 3.7.5. Como fazer para descobrir em que dia da semana cai uma data que vai ocorrer daqui a 40 dias? E 500? Vamos dar um número de 0 a 6, para cada dia da semana, começando no domingo. Vamos supor que o dia 0 cai num domingo. Logo o dia 1, cai numa segunda. E o dia 8? Bom, temos que $8 = 7 + 1$. Note que esse 6 representa uma "volta" completa na semana. Então é "domingo" mais um dia. Isto é, segunda. Se fosse o dia 20, teríamos $20 = 2 \cdot 7 + 6$. Note que os múltiplos de 7 marcam as "voltas" completas na semana, assim, temos que tal dia é "domingo" mais 6 dias. Isto é, sábado. Desta maneira, para calcular em que dia semana será uma data daqui a 90 dias, basta tomarmos o resto da divisão do número do dia da semana atual mais quanto dias queremos. No nosso exemplo, vamos supor que hoja é sexta. Logo, o dia associado é 5. Assim, daqui a 90 dias, será o resto de 95 dividido por 7. Com $95 = 13 \cdot 7 + 4$, teremos que o dia da semana será o correspondente a 4, isto é, quinta.

Exemplo 3.7.6. Qual é o o último dígito de 27^{500}? Primeiramente, note que o último digito de um número é o resto da divisão de tal número por 10. Ou seja, queremos achar a entre 0 e 9 de forma que $a \equiv_{10} 27^{500}$. A primeira

coisa que podemos notar é que $27 \equiv_{10} 7$. Logo, $a \equiv_{10} 7^{500}$. Note também que $7^2 = 49$ Logo $7^2 \equiv_{10} 49 \equiv_{10} 9 \equiv_{10} -1$. Assim, $7^{500} = (7^2)^{250} \equiv_{10} (-1)^{250} \equiv_{10} 1$. Logo, o último dígito de 27^{500} é 1.

Exemplo 3.7.7. Maneira alternativa de resolver o problema anterior: Partimos do ponto em que temos que $27^{500} \equiv 7^{500}$. Vejamos como se comportam as potências de 7 módulo 10. Temos $7^0 \equiv 1$, $7^1 \equiv_{10} 7$, $7^2 \equiv_{10} 9$, $7^3 \equiv_{10} 3$, $7^4 \equiv_{10} 1$, ou seja, elas formam um ciclo de comprimento 4. Assim, temos que $7^{500} \equiv_{10} 7^0 \equiv_{10} 1$, pois 500 tem resto 0 na divisão por 4.

Exercícios

Exercício 3.7.8. Mostre que um número $n \in \mathbb{N}$ é múltiplo de 4 se, e somente se, o número formado pelos seus dois últimos dígitos é múltiplo de 4.

Exercício 3.7.9. Seja $n \in \mathbb{N}$ ímpar. Mostre que $2^n + 1$ é divisível por 3.

Exercício 3.7.10. Prove que todo ano (incluindo bissextos) tem pelo menos uma sexta-feira 13.

3.8 Exercícios do Capítulo

3.8.1. Numa reunião de uma seita secreta, cada participante deve, ao chegar no local, cumprimentar cada um dos participantes que chegaram antes (vamos supor que não cheguem dois participantes ao mesmo tempo). Seja n o número de participantes e C_n a quantidade total de cumprimentos na reunião. Mostre que $2C_n = n(n-1)$.

3.8.2. Sejam $a, b \in \mathbb{N}$ com $b > 0$. Sejam $q_1, q_2, r_1, r_2 \in \mathbb{N}$ tais que $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \leq r_1, r_2 < b$. Mostre que $q_1 = q_2$ e $r_1 = r_2$ (isto é, mostre que a resposta do algoritmo de Euclide é única).

3.8.3. Dizemos que um número $n \in \mathbb{N}$ é **par** se $2|n$. Dizemos que n é **ímpar** caso contrário.

(a) Mostre que todo número par pode ser escrito na forma $2k$, onde $k \in \mathbb{N}$;

(b) Mostre que todo número ímpar pode ser escrito na forma $2k + 1$, onde $k \in \mathbb{N}$;

(c) Mostre que todo número da forma $2k$ é par (para $k \in \mathbb{N}$);

(d) Mostre que todo número da forma $2k+1$ é ímpar (para $k \in \mathbb{N}$);

(e) Seja $n \in \mathbb{N}$. Mostre que n^2 é par se, e somente se, n é par.

3.8.4. Sejam $p_1, ..., p_n$ primos. Mostre que p_i não divide $p_1 \cdot \cdots \cdot p_n + 1$ para qualquer $i = 1, ..., n$.

3.8.5. Mostre que existem infinitos primos.

3.9 Racionais

Intuitivamente, estamos querendo que (a, b) represente $\frac{a}{b}$. Então, para $\frac{a}{b} = \frac{x}{y}$, temos a consdição apresentada.

Definição 3.9.1. Considere o conjunto $A = \{(a, b) \in \mathbb{Z} : b \neq 0\}$ e considere $\sim$ a seguinte relação sobre A: dados $(a, b), (x, y) \in A$, definimos $(a, b) \sim (x, y)$ se, e somente se, $ay = bx$.

Proposição 3.9.2. *A relação $\sim$ definida acima é uma relação de equivalência sobre A.*

Demonstração. Note que $(a, b) \sim (a, b)$. Também temos que $(a, b) \sim (x, y)$ implica que $(x, y) \sim (a, b)$. Agora vejamos a transitiva. Sejam $(a, b), (x, y), (\alpha, \beta) \in A$ tais que $(a, b) \sim (x, y)$ e $(x, y) \sim (\alpha, \beta)$. Temos que mostrar que $(a, b) \sim (\alpha, \beta)$. Isto é, $a\beta = b\alpha$. Temos

$$ay = bx$$

$$x\beta = y\alpha.$$

Assim, multiplicando por β a primeira equação, temos $ay\beta = bx\beta$. Logo, $ay\beta = by\alpha$. Como $y \neq 0$, temos $a\beta = b\alpha$ como queríamos. □

Definição 3.9.3. Denotamos por $\mathbb{Q}$ o conjunto $A/\sim$. Chamamos tal conjunto de conjunto dos **números racionais**.

Aqui é só pensar que estamos fazendo a soma usual, mas sem simplificar.

Definição 3.9.4. Definimos a operação de **soma** sobre os racionais da seguinte maneira: dados $[(a, b)], [(x, y)] \in \mathbb{Q}$, definimos $[(a, b)] + [(x, y)] = [(ay + xb, by)]$.

Proposição 3.9.5. *A operação de soma está bem definida.*

Demonstração. Primeiramente, note que, de fato, $(ay + xb, by) \in A$, já que $by \neq 0$ (pois tanto b como y são diferentes de 0). Agora vamos mostrar que ela independe dos representantes. Sejam $(a, b), (c, d), (x, y), (w, z) \in A$ tais que $(a, b) \sim (x, y)$ e $(c, d) \sim (w, z)$. Vamos mostrar que $(ad + cb, db) \sim$

$(xz + wy, yz)$ isto é, $(ad + cb)yz = (xz + wy)db$. Temos $ay = bx$ e $cz = dw$. Logo

$$\begin{aligned}(ad + cb)yz &= adyz + cbyz \\ &= aydz + czby \\ &= bxdz + dwby \\ &= (xz + wy)db\end{aligned}$$

□

Definição 3.9.6. Definimos a operação de **produto** sobre os racionais da seguinte maneira: dados $[(a, b)], [(x, y)] \in \mathbb{Q}$, definimos $[(a, b)] \cdot [(x, y)] = [(ax, by)]$.

Novamente, isso é apenas a operação usual, sem simplificações.

Proposição 3.9.7. *A operação de produto está bem definida.*

Demonstração. Veja o Exercício 3.10.2. □

Definição 3.9.8. Dizemos que um elemento $[(a, b)] \in \mathbb{Q}$ está na **forma canônica** se $b > 0$.

Proposição 3.9.9. *Todo número $q \in \mathbb{Q}$ admite uma representação na forma canônica.*

Demonstração. Seja $[(a, b)] = q$. Se $b > 0$, nada temos a fazer. Se $b < 0$, observe que $[(-a, -b)] = [(a, b)]$ (pois $-ab = -ba$) e $[(-a, -b)]$ está na forma canônica. □

Definição 3.9.10. Sejam $q, r \in \mathbb{Q}$. Dizemos que $q \leq r$ se $ay \leq xb$ se $q = [(a, b)]$, $r = [(x, y)]$ e $[(a, b)]$ e $[(x, y)]$ estão na forma canônica.

Proposição 3.9.11. *A relação $\leq$ definida acima está bem definida.*

Demonstração. Precisamos mostrar que se valem

$$[(a_1, b_1)] = [(a_2, b_2)]$$

$$[(x_1, y_1)] = [(x_2, y_2)]$$

$$[(a_1, b_1)] \leq [(x_1, y_1)]$$

então vale $[(a_2, b_2)] \leq [(x_2, y_2)]$. Note que as duas primeiras equações se traduzem para $a_1b_2 = b_1a_2$ e $x_1y_2 = y_1x_2$. Assim, de $a_1y_1 \leq b_1x_1$, multiplicando ambos os lados por b_2y_2 (que é maior que 0), temos

$$a_1y_1b_2y_2 \leq b_1x_1b_2y_2.$$

Substituindo a_1b_2 por b_1a_2 do lado esquerdo e x_1y_2 por x_2y_1 do lado direito, obtemos:

$$b_1a_2y_1y_2 \leq b_2y_1x_2b_1.$$

Cancelando b_1y_1 (que é diferente de 0), temos $a_2y_2 \leq b_2x_2$, isto é, $[(a_2, b_2)] \leq [(x_2, y_2)]$ como queríamos. □

Proposição 3.9.12. *A relação $\leq$ definida acima é uma ordem total sobre $\mathbb{Q}$.*

Demonstração. Ver o exercício 3.10.4 □

Definição 3.9.13. Seja $[(a, b)] \in \mathbb{Q}$ escrito na forma canônica. Denotamos $[(a, b)]$ por $\frac{a}{b}$. No caso em que $b = 1$, utilizamos simplesmente a.

Observação 3.9.14. Note que tal notação fica coerente com o que tínhamos antes. Isto é, $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = a + b$, onde a última soma é entre inteiros. Note que temos a mesma coisa para o produto.

3.10 Exercícios

Exercício 3.10.1. Qual o problema com a relação $\sim$ se deixarmos A conter pontos da forma $(x, 0)$?

Exercício 3.10.2. Mostre que o produto dos racionais está bem definido. Atenção, mostre também que o resultado de tal operação pertence a $\mathbb{Q}$ (veja o começo da demonstração da Proposição **3.9.5**).

Exercício 3.10.3. Mostre que a soma e o produto são associativas, comutativas e que vale a distributiva.

Exercício 3.10.4. Mostre que a relação $\leq$ definida acima é uma ordem total sobre $\mathbb{Q}$.

Exercício 3.10.5. Encontre um elemento neutro para a soma. Mostre que ele é único.

Exercício 3.10.6. Encontre um elemento neutro para o produto. Mostre que ele é único.

Exercício 3.10.7. Mostre que se $q \in \mathbb{Q}$ e $q \neq 0$, então existe $r \in \mathbb{Q}$ tal que $qr = 1$. Neste caso dizemos que r é o **inverso** de q e o denotamos por q^{-1}. Mostre que tal inverso é único.

Exercício 3.10.8. Definimos a **divisão** em $\mathbb{Q}$ como sendo, dados $a, b \in \mathbb{Q}$, com $b \neq 0$, $\frac{a}{b} = ab^{-1}$. Mostre que isso é coerente com a notação que já tínhamos, isto é, se $a, b \in \mathbb{Z}$ com $b \neq 0$, então $[(a, b)] = \frac{a}{b} = ab^{-1}$.

3.11 Números reais

Definição 3.11.1. Seja $(X, \leq)$ conjunto totalmente ordenado. Dizemos que $I \subset X$ é um **intervalo** se, para todo $a, b \in I$, se $x \in X$ é tal que $a < x$ e $x < b$, então $x \in I$.

Exemplo 3.11.2. O conjunto $\{n \in \mathbb{N} : 3 < n \text{ e } n < 20\}$ é um intervalo nos naturais. O conjunto $\{q \in \mathbb{Q} : 3 < q \text{ e } q < 20\}$ também é um intervalo em $\mathbb{Q}$. Mas o conjunto $\{n \in \mathbb{Q} : 3 < n, n < 20 \text{ e } n \in \mathbb{N}\}$ não é um intervalo em $\mathbb{Q}$.

Definição 3.11.3. Chamamos de um **corte de Dedekind** um par (I, J) onde $I, J \subset \mathbb{Q}$ são intervalos não vazios tais que

- $I \cup J = \mathbb{Q}$;
- se $i \in I$, então existe $k \in I$ tal que $i < k$;
- dados $i \in I$ e $j \in J$ temos que $i < j$.

Exemplo 3.11.4. (I, J) é um corte de Dedekind, onde $I = \{q \in \mathbb{Q} : q < 0\}$ e $J = \{q \in \mathbb{Q} : q \geq 0\}$ (exercício).

Vamos dar mais um exemplo de corte de Dedekind, mas antes precisamos mais um resultado sobre os racionais.

Exemplo 3.11.5. (I, J) é um corte de Dedekind onde $I = \{q \in \mathbb{Q} : qq < 2 \vee q < 0\}$ e $J = \{q \in \mathbb{Q} : 2 < qq \wedge q > 0\}$. Primeiramente, precisamos provar que I e J são intervalos. Vamos provar que J é um intervalo (I fica como exercício). Sejam $a, b \in J$ com $a < b$. Seja $q \in \mathbb{Q}$ tal que $a < q < b$. Como $0 < a$, temos que $0 < q$. Assim, só falta mostrar que $2 < qq$. De fato, como $a < q$, temos $aa < qa$ e $aq < qq$. Logo, $aa < qq$ e, portanto, $2 < qq$.

Vejamos que $I \cup J = \mathbb{Q}$. Note que é suficiente mostrarmos que $\mathbb{Q} \subset I \cup J$. Seja $q \in \mathbb{Q}$. Se $q < 0$, $q \in I$. Se $q \geq 0$, temos dois casos. Se $qq < 2$, então $q \in I$. Se $qq > 2$, temos que $qq \in J$.

Note que o caso $qq = 2$ é impossível.

Se $i \in I$, precisamos mostrar que existe $k \in I$ tal que $i < k$. Se $i < 0$, basta tomarmos $k = \frac{i}{2}$. Se $i > 0$ e $ii < 2$, considere

$$k = \frac{2i + 2}{i + 2}$$

Primeiramente, note que $k > i$ pois

$$\begin{aligned} i &= \frac{i(i+2)}{i+2} \\ &= \frac{ii+2i}{i+2} \\ &< \frac{2+2i}{i+2} \\ &= k \end{aligned}$$

Note também que $kk < 2$, pois

$$\begin{aligned} 2 - kk &= 2 - \frac{2i+2}{i+2}\frac{2i+2}{i+2} \\ &= 2 - \frac{4i^2+8i+4}{i^2+4i+4} \\ &= \frac{2i^2+8i+8-(4i^2+8i+4)}{i^2+4i+4} \end{aligned}$$

Note que, como o denominador é positivo, só precisamos analisar o sinal do numerador. Assim

$$\begin{aligned} 2i^2 + 8i + 8 - 4i^2 - 8i - 4 &= 4 - 2i^2 \\ &> 4 - 2 \cdot 2 \\ &= 0 \end{aligned}$$

Ou seja, tal diferença é positiva, como queríamos.

Finalmente, só precisamos mostrar que, dados $i \in I$ e $j \in J$, temos que $i < j$ - vamos deixar isso como exercício.

Lema 3.11.6. *Seja (I, J) um corte de Dedekind. Se $a \in I$ e $b < a$, então $b \in I$.*

Demonstração. Suponha que não. Então $b \in J$. Mas isso contraria a última propriedade da definição de corte. □

Proposição 3.11.7. *Dados (A, B) e (X, Y) dois cortes de Dedekind, dizemos que $(A, B) \leq (X, Y)$ se $A \subset B$. Tal relação é uma ordem total sobre o conjunto dos cortes.*

Demonstração. Que é uma relação de ordem, não há nada a provar, já que a inclusão é uma relação de ordem. Resta mostrar tal relação é total. Sejam (A, B) e (X, Y) dois cortes. Suponha que $(A, B) \not\leq (X, Y)$, isto é, $A \not\subset X$. Vamos provar que $X \subset A$. Seja $x \in X$. Como $A \not\subset X$, existe $a \in A \setminus X$. Note que $a \in Y$. Assim, para todo $z \in X$, temos que $z < a$. Em particular, temos $x < a$. Asim, $x \in A$ pelo lema. □

Definição 3.11.8. Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ um conjunto não vazio. Dizemos $m \in X$ é um **majorante** para A se $a \leq m$

para todo $a \in A$. Dizemos que $A \subset X$ é **limitado superiormente** se A admite um majorante.

Exemplo 3.11.9. 1 e 3 são majorantes para o conjunto $[0, 1]$ em $\mathbb{R}$.

Definição 3.11.10. Seja $(X, \leq)$ um conjunto totalmente ordenado. Seja $A \subset X$ um conjunto limitado superiormente. Dizemos que $a \in X$ é um **supremo** de A (notação $\sup A$), se $a = \min\{m : m \text{ é majorante de } A\}$.

Um supremo pode não existir:

Exemplo 3.11.11. Em $\mathbb{Q}$, não existe $\sup A$, onde $A = \{q \in \mathbb{Q} : q > 0 \wedge q^2 < 2\}$.

Mas se o supremo existe, ele é único:

Proposição 3.11.12. *Seja $(X, \leq)$ conjunto totalmente ordenado e seja $A \subset X$ conjunto limitado superiormente. Sejam a, b supremos de A. Então $a = b$.*

Demonstração. Como a é o menor dos majorantes de A e como b é um majorante de A, temos que $a \leq b$. A outra desigualdade é análoga. □

Definição 3.11.13. Seja $(X, \leq)$ conjunto totalmente ordenado. Dizemos que $\leq$ é uma **ordem completa** se, para todo $A \subset X$ limitado, existe $a = \sup A$.

Proposição 3.11.14. *A ordem definida acima para o conjunto de todos os cortes de Dedekind é completa.*

Demonstração. Seja $\mathcal{A}$ um conjunto de cortes que seja limitado. Isto é, existe (I, J) tal que, para todo $(A, B) \in \mathcal{A}$, temos que $A \subset I$. Vamos provar que existe um supremo para $\mathcal{A}$. Considere (X, Y) onde

$$X = \bigcup \{A : (A, B) \in \mathcal{A}\}$$

$$Y = \mathbb{Q} \setminus X$$

Vamos provar que $(X, Y) = \sup \mathcal{A}$. Primeiramente, note que $X \neq \emptyset$, pois qualquer A tal que $(A, B) \in \mathcal{A}$ é tal que $A \neq \emptyset$ e $A \subset X$. Note também que existe $j \in J$ e que tal $j \notin A$ para qualquer $(A, B) \in \mathcal{A}$. Logo, $j \in B$ e, portanto, B é não vazio.

Vamos provar que X é um intervalo. De fato, sejam $a, b \in X$ e $c \in \mathbb{Q}$ tais que $a < c < b$. Seja A tal que $(A, B) \in \mathcal{A}$ e tal que $b \in A$ (existe pela definição de X). Pelo Lema 3.11.6, temos que $c \in A$ e, portanto, $c \in X$

como queríamos. Vamos deixar o restante da prova de que (X, Y) é um corte como exercício.

Note que, pela definição de (X, Y), temos automaticamente que $A \subset X$ para todo $(A, B) \in \mathcal{A}$. Isto é, (X, Y) é um majorante para $\mathcal{A}$. Resta mostrar que é o menor. Para isso, basta mostrar que $X \subset I$. De fato, dado $x \in X$, temos que $x \in A$ para algum $(A, B) \in \mathcal{A}$. Como (I, J) é majorante, temos que $A \subset I$. Logo, $x \in I$ como queríamos. □

Definição 3.11.15. Chamamos de $\mathbb{R}$ o conjunto de todos os cortes de Dedekind com a ordem apresentada acima.

As operações sobre $\mathbb{R}$ podem ser definidas de maneira natural a partir das operações definidas sobre $\mathbb{Q}$. Por exemplo, $(A, B)+(X, Y) = (A \oplus X, B \oplus Y)$, onde $I \oplus J = \{i + j : i \in I, j \in j\}$.

Exercícios

Exercício 3.11.16. Seja (I, J) um corte de Dedekind. Prove as seguintes afirmações:

(a) Se $q \notin I$, então $q \in J$.

(b) $I \cap J = \emptyset$.

(c) Se $q \in \mathbb{Q}$ é tal que existe $j \in J$ tal que $j < q$, então $q \in J$.

Exercício 3.11.17. Seja $(X, \leq)$ conjunto ordenado completo. Sejam A, B não vazios tais que B é limitado superiormente e $A \subset B$.

(a) Mostre que A é limitado superiormente.

(b) Mostre que $\sup A \leq \sup B$.

(c) Dê um exemplo nessas condições em que $A \neq B$ mas $\sup A = \sup B$.

(d) Dê um exemplo nessas condições em que $\sup A < \sup B$.

3.12 Números reais (de novo)

Nesta seção vamos apresentar uma segunda maneira de definir números reais.

Definição 3.12.1. Seja $(q_n)_{n \in \mathbb{N}}$ uma sequência de racionais. Dizemos que tal sequência converge para q se, para todo $\varepsilon \in \mathbb{Q}_{>0}$, existe $n_0 \in \mathbb{N}$ tal que, para todo $m \geq n_0$, temos que $|q_m - q| < \varepsilon$.

Exemplo 3.12.2. Considere $(q_n)_{n\in\mathbb{N}}$ dada por $q_n = q$ para todo $n \in \mathbb{N}$. Vamos provar que $(q_n)_{n\in\mathbb{N}}$ converge para q. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, temos

$$|q_n - q| = 0 < \varepsilon$$

Ou seja, podemos tomar $n_0 = 0$.

Exemplo 3.12.3. A sequência $(\frac{1}{n+1})_{n\in\mathbb{N}}$ **converge** para 0. De fato, dado $\varepsilon \in \mathbb{Q}_{>0}$, note que $q = \frac{a}{b}$ com $a, b > 0$. Seja $n_0 = b$. Note que

$$\frac{1}{b} < \frac{a}{b}$$

Assim, dado $m \geq n_0$, temos

$$\frac{1}{m+1} < \frac{1}{m} \leq \frac{1}{n_0} = \frac{1}{n} < \frac{a}{b}$$

Como $|\frac{1}{m+1} - 0| = \frac{1}{m+1}$, temos o resultado.

Definição 3.12.4. Seja $(q_n)_{n\in\mathbb{N}}$ uma sequência de racionais. Dizemos que $(q_n)_{n\in\mathbb{N}}$ é uma **sequência de Cauchy** se, para todo $\varepsilon \in \mathbb{Q}_{>0}$, existe $n_0 \in \mathbb{N}$ tal que, para todo $m, n \geq n_0$ temos $|q_n - q_m| < \varepsilon$.

Proposição 3.12.5. *Se $(q_n)_{n\in\mathbb{N}}$ é uma sequência convergente, então $(q_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy.*

Demonstração. Seja q tal que $(q_n)_{n\in\mathbb{N}}$ converge para q. Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(q_n)_{n\in\mathbb{N}}$ converge para q, existe n_0 tal que, para todo $k \geq n_0$, temos

$$|q_k - q| < \frac{\varepsilon}{2}$$

Em vez de usar ε na definição de converge, usamos $\frac{\varepsilon}{2}$ - como era para qualquer ε, podemos fazer isso.

Sejam $n, m \geq n_0$. Temos

$$\begin{aligned} |q_n - q_m| &= |q_n - q + q - q_m| \\ &\leq |q_n - q| + |q - q_m| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

□

Definição 3.12.6. Sejam $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ sequências de Cauchy. Dizemos que $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ se $(x_n - y_n)_{n\in\mathbb{N}}$ converge para 0.

Note que essa condição é equivalente a para todo $\varepsilon \in \mathbb{Q}_{>0}$ existe n_0 tal que para todo $n \geq n_0$ $|x_n - y_n| < \varepsilon$.

Proposição 3.12.7. *A relação $\cong$ definida acima é uma relação de equivalência.*

Demonstração. É claro que $(x_n)_{n\in\mathbb{N}} \cong (x_n)_{n\in\mathbb{N}}$ pois $(x_n - x_n)_{n\in\mathbb{N}}$ é a sequência constante igual a 0.

Se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, então a sequência $(x_n - y_n)_{n\in\mathbb{N}}$ converge para 0. Ou seja, dado $\varepsilon \in \mathbb{Q}_{>0}$, existe n_0 tal que, para todo $k \geq n_0$, temos que $|x_k - y_k| < \varepsilon$. Como $|x_k - y_k| = |y_k - x_k|$, temos o resultado.

Finalmente, se $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$, precisamos mostrar que $(x_n)_{n\in\mathbb{N}} \cong (z_n)_{n\in\mathbb{N}}$.

Seja $\varepsilon \in \mathbb{Q}_{>0}$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$ temos

$$|x_k - y_k| < \frac{\varepsilon}{2}.$$

Analogamente, existe n_2 tal que, para todo $k \geq n_2$, temos

$$|y_k - zk| < \frac{\varepsilon}{2}.$$

Note que, assim, $k \geq n_1$ e $k \geq n_2$.

Assim, considere $n_0 = \max\{n_1, n_2\}$. Dado $k \geq n_0$, temos:

$$\begin{aligned} |x_k - z_k| &= |x_k - y_k + y_k - z_k| \\ &\leq |x_k - y_k| + |y_k - z_k| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

□

Proposição 3.12.8. *Se $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ convergem para x e y respectivamente, então $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$ se, e somente se, $x = y$.*

Demonstração. Suponha $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$. Suponha que $x \neq y$. Então $\varepsilon = |x - y| > 0$. Como $(x_n)_{n\in\mathbb{N}} \cong (y_n)_{n\in\mathbb{N}}$, existe n_1 tal que, para todo $k \geq n_1$,

$$|x_k - y_k| < \frac{\varepsilon}{3}.$$

Como $(x_n)_{n\in\mathbb{N}}$ converge para x, existe n_2 tal que, para todo $k \geq n_2$,

$$|x - x_k| < \frac{\varepsilon}{3}.$$

Analogamente, existe n_3 tal que, para todo $k \geq n_3$,

$$|y - y_k| < \frac{\varepsilon}{3}.$$

Assim, seja $k = \max\{n_1, n_2, n_3\}$. Temos

$$\begin{aligned} |x-y| &= |x - x_k + x_k - y_k + y_k - y| \\ &\leq |x - x_k| + |x_k - y_k| + |y_k - y| \\ &< \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} + \tfrac{\varepsilon}{3} \\ &= \varepsilon \end{aligned}$$

contrariando a definição de ε.

Agora suponha $x = y$. Seja $\varepsilon > 0$. Seja n_1 tal que, para todo $k \geq n_1$,

$$|x - x_k| < \frac{\varepsilon}{2}.$$

Seja n_2 tal que, para todo $k \geq n_2$,

$$|y - y_k| < \frac{\varepsilon}{2}.$$

Considere $n_0 = \max\{n_1, n_2\}$. Assim, dado $k \geq n_0$, temos

$$\begin{aligned} |x_k - y_k| &= |x_k - x + x - y_k| \\ &\leq |x_k - x| + |x - y_k| \\ &= |x_k - x| + |y - y_k| \\ &< \varepsilon \end{aligned}$$

□

Definição 3.12.9. Podemos definir $\mathbb{R}$ como sendo o conjunto de todas as classes de equivalência de sequências de Cauchy de racionais pela relação acima.

Exercícios

Exercício 3.12.10. Mostre que a sequência $(q_n)_{n\in\mathbb{N}}$ dada por $q_n = 0$ se n é par e $q_n = 1$ se n é ímpar não converge.

Exercício 3.12.11. Suponha que $(x_n)_{n\in\mathbb{N}}$ converge para a e para b. Mostre que $a = b$.

Exercício 3.12.12. Sejam $q, a \in \mathbb{Q}$. Suponha que $(q_n)_{n\in\mathbb{N}}$ converge para q. Mostre que a sequência $(q_n + a)_{n\in\mathbb{N}}$ converge para $q + a$.

3.13 Mais um pouco de congruência modular

O nome não é bem esse, mas todo mundo usa na hora de falar.

Definição 3.13.1. Dado $n \in \mathbb{N}_{>1}$, vamos chamar de **inteiros mod n** o conjunto $\mathbb{Z}/\equiv_n$ com as operações usuais. Por comodidade, vamos os elementos de tal conjunto por $0, ..., n-1$. Vamos denotar tal conjunto por MOD_n.

Vamos adotar o seguinte abuso: dados $a, b \in MOD_n$, podemos nos referir a eles como $a = b$ (pensando neles como as clases) ou $a \equiv_n b$ (pensando neles com representantes das classes). Note que isso não dá problema pois existe um único representante entre $0, ..., n-1$.

Proposição 3.13.2. *Seja p primo. Sejam $a, binMOD_p$. Se $ab \equiv_p 0$, então $a \equiv_p 0$ ou $b \equiv 0$.*

Demonstração. Note que se $ab \equiv_p= 0$, então $p|ab$. Como p é primo, temos que $p|a$ ou $p|b$. O primeiro caso implica que $a \equiv_p 0$ e o segundo implica que $b \equiv_p 0$. □

Proposição 3.13.3. *Seja p primo e sejam a, x, y inteiros módulo p, com $a \not\equiv_p 0$. Se $ax \equiv_p ay$, então $x \equiv_p y$.*

Demonstração. Como $ax \equiv_p ay$, temos que $ax - ay \equiv_p 0$. Isto é,

$$a(x-y) \equiv_p 0$$

Pelo resultado anterior, temos que $a \equiv_p 0$ ou $(x-y) \equiv_p 0$. Como $a \not\equiv_p 0$, temos que $x \equiv_p y$ como queríamos. □

Lema 3.13.4. *Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é injetora.*

Demonstração. Suponha $x, y \in MOD_p$. Note que $\pi_a(x) = \pi_a(y)$ quer dizer $ax \equiv_p ay$. Pelo resultado anterior, temos que $x = y$. □

Corolário 3.13.5. *Seja p primo. Seja a um inteiro mod p tal que $a \not\equiv_p 0$. Temos que $\pi_a : MOD_p \to MOD_p$ dada por $\pi_a(x) = ax$ é bijetora.*

Note que esse argumento não vale para conjuntos infinitos.

Demonstração. Note que, como a função é injetora, ela tem p elementos na imagem. Como o contradomínio também tem p elementos na imagem, temos que a função é sobrejetora. □

Proposição 3.13.6. *Seja p primo. Seja $a \in MOD_p$ com $a \neq 0$. Então existe um único $b \in MOD_p$ tal que $ab = 1$. Muitas vezes vamos denotar tal elemento por a^{-1}.*

Demonstração. Considere a função π_a acima. Como ela é sobrejetora, existe $b \in MOD_p$ tal que $\pi_a(b) = 1$. Isto é, $ab = 1$.

Vejamos agora que ele é único. Sejam $b, c \in MOD_p$ tais que $ab = 1$ e $ac = 1$. Então, pela Proposição 3.13.3, temos de $ab = ac$ que $b = c$. □

Definição 3.13.7. Dizemos que $(F, \oplus, \odot)$ é um **corpo** se $\oplus$ e $\odot$ são associativas, comutativas e ainda valem, para todo $a, b, c \in F$:

Normalmente vamos denotar $\oplus$ por $+$ e $\odot$ por $\cdot$ (ou mesmo omitir o símbolo, como usualmente).

(i) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$;

(ii) Existe $0 \in F$ tal que $0 \oplus x = x$ para todo $x \in F$;

(iii) Existe $1 \in F$ tal que $1 \odot x = x$ para todo $x \in F$;

(iv) Existe $x \in F$ tal que $a \oplus x = 0$;

(v) Se $a \neq 0$, existe $x \in F$ tal que $x \odot a = 1$.

Exemplo 3.13.8. Tanto os racionais como os reais satisfazem a definição de corpo com as operações usuais.

Proposição 3.13.9. *Seja p primo. Então MOD_p é um corpo com as operações usuais é um corpo.*

Demonstração. Note que as operações serem associativas, comutativas e a regra de distributividade seguem diretamente das mesmas propriedades sobre $\mathbb{Z}$. Note que 0 e 1 também fazem os papeis de elementos neutros em MOD_p. Dado $a \in MOD_p$, note que $a + (p - a) = p \equiv_p 0$. Já a última propriedade é simplesmente a Proposição 3.13.6. □

Vamos ver algumas propriedades simples sobre corpos:

Lema 3.13.10. *Seja F um corpo. Dado $x \in F$, temos que $0x = 0$.*

Demonstração. Seja $y \in F$ tal que $0x + y = 0$. Temos

$$0x = (0 + 0)x = 0x + 0x$$

Somando y dos dois lados, obtemos

$$0 = 0x + a = 0x + 0x + a = 0x$$

como queríamos. □

Proposição 3.13.11. *Seja F um corpo. Sejam $a, b \in F$ tais que $ab = 0$. Então $a = 0$ ou $b = 0$.*

Espaços que satisfazem isso chamados de **domínios de integridade**.

Demonstração. Suponha que $a \neq 0$. Vamos provar que $b = 0$ (note que isso é suficiente para o que queremos). Então existe $x \in F$ tal que $ax = 1$. Assim, de $0 = ab$, temos $0x = xab$. Como $0x = 0$ pelo lema anterior, temos que $0 = b$. □

No caso em que $m \in \mathbb{Z}_{>1}$ mas não é primo, temos que MOD_m não é corpo.

Proposição 3.13.12. *Seja $m \in \mathbb{Z}_{>1}$ não primo. Então MOD_m não é corpo.*

Demonstração. Note que, pelo resultado anterior, basta mostrarmos que existem $a, b \in MOD_n$ não nulos tais que $ab = 0$. Como m não é primo, existe a tal que $a|m$ e $a \neq 1$ e $a \neq m$. Seja b tal que $ab = m$. Note que $b \neq 1$ e $b \neq m$. Note também que $a, b \neq 0$. Mas temos

$$ab = m \equiv_m 0$$

□

Exercícios

Exercício 3.13.13. Considere $\mathbb{R}^2$ com as seguintes operações:

$$(a, b) \oplus (x, y) = (a + x, b + y)$$

$$(a, b) \odot (x, y) = (ax, by)$$

Com essas operações, $\mathbb{R}^2$ é um corpo?

3.14 Teorema chinês do resto

Definição 3.14.1. Dizemos que $a, b \in \mathbb{Z}_{>1}$ são **primos entre si** se $mdc(a, b) = 1$.

Lema 3.14.2. *Seja a, b primos entre si. Seja $z \in \mathbb{Z}$. Se $a|z$ e $b|z$, então $ab|z$.*

Demonstração. Como $a|z$, existe m tal que $am = z$. Como $b|z$, existe n tal que $bn = z$. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando tal equação por z dos dois lados, temos

$$\begin{aligned} z &= z(ax + by) \\ &= zax + zby \\ &= bnax + amby \\ &= ab(nx + my) \end{aligned}$$

Ou seja, $ab|z$. □

Lema 3.14.3. *Sejam $a, b, c \in \mathbb{N}$ primos entre si. Então ab e c são primos entre si.*

Demonstração. Seja x divisor comum entre ab e c. Suponha que $x \neq 1$. Então existe p primo tal que $p|x$. Logo, $p|ab$ e $p|c$. Como $p|ab$, temos que $p|a$ ou $p|b$. Logo, a e c não são primos entre si, ou b e c não são primos entre si. □

Corolário 3.14.4. *Sejam $a_1, ..., a_n, b \in \mathbb{N}_{>1}$ primos entre si. Então $a_1 \cdots a_n$ e b são primos entre si.*

Demonstração. Por indução sobre n. Se $n = 2$, é exatamente o lema anterior. Note que, porr hipótese de indução, temos que $a_1 \cdots a_n$, a_{n+1} e b são primos entre si. Então, novamente pelo lema, temos que $a_1 \cdots a_{n+1}$ e b são primos entre si. □

Proposição 3.14.5. *Sejam a, b primos entre si. Sejam r e s inteiros. Então o sistema*

$$\begin{cases} x \equiv_a r \\ x \equiv_b s \end{cases}$$

Admite alguma solução c e é equivalente a

$$x \equiv_{ab} c$$

Demonstração. Como a e b são primos entre si, existem $\alpha, \beta \in \mathbb{Z}$ tais que

$$\alpha a + \beta b = 1$$

Considere

$$c = s\alpha a + r\beta b$$

Vejamos que tal c é, de fato, uma solução para o sistema
Primeiramente, temos que

$$\begin{aligned} c - r &= s\alpha a + r\beta b - r \\ &= s\alpha a + r(\beta b - 1) \\ &= s\alpha a - \alpha a r \\ &= a(s\alpha - r\alpha) \end{aligned}$$

Ou seja, temos que

$$c \equiv_a r.$$

De forma análoga, podemos mostrar que $c \equiv_b s$.

Agora suponha x uma solução para o sistema. Então

$$x \equiv_a c$$

$$x \equiv_b c$$

Ou seja, $a|(x-c)$ e $b|(x-c)$. Como a, b são primos entre si, pelo Lema 3.14.2, temos que $ab|(x-c)$. Ou seja, $x \equiv_{ab} c$. □

Corolário 3.14.6 (Teorema chinês do resto)**.** *Sejam $a_1, ..., a_n$ primos entre si e sejam $r_1, ..., r_n \in \mathbb{Z}$. Então o sistema*

$$\begin{cases} x & \equiv_{a_1} & r_1 \\ & \vdots & \\ x & \equiv_{a_n} & r_n \end{cases}$$

admite solução b e é equivalente à equação $x \equiv_A b$, onde $A = a_1 \cdots a_n$.

Demonstração. Vamos provar por indução sobre n. O caso n é o resultado anterior. Suponha então que temos $n+1$ equações como no enuciado. Por hipótese de indução, existe b' tal que o sistema formado pelas primeiras n equações é equivalente a $x \equiv_{A'} b'$, onde $A' = a_1 \cdots a_n$. Pelo Corolario 3.14.4, temos que a_{n+1} e A' são primos entre si. Assim, novamente pelo resultado anterior, temos que existe b tal que o sistema

$$\begin{cases} x & \equiv_{A'} & b' \\ x & \equiv_{a_{n+1}} & r_{n+1} \end{cases}$$

é equivalente a

$$x \equiv_A b$$

onde $A = A'a_{n+1} = a_1 \cdots a_{n+1}$. Ou seja, a última equação é equivalente ao sistema do enunciado. □

Exemplo 3.14.7. Qual o menor natural k tal que k dividido por 3 tem resto 2, dividido por 5 tem resto 3 e divido por 7 tem resto 2?

Primeiramente, note que a pergunta é equivalente a perguntar qual a menor solução positiva para

$$\begin{cases} x & \equiv_3 & 2 \\ x & \equiv_5 & 3 \\ x & \equiv_7 & 2 \end{cases}$$

Já sabemos que tal sistema é equivalente a uma equação da forma

$$x \equiv_{105} a$$

para algum a. Podemos simplesmente repetir o processo da demonstração do resultado para calcular o a, mas há um modo mais fácil. A terceira equação é equivalente a encontrar b tal que $x = 7b + 2$. Substituindo na segunda equação, obtemos

$$7b + 2 \equiv_5 3$$

Ou seja

$$2b \equiv_5 1$$

Lembrando que 3 é o inverso de 2 em MOD_5, multiplicando ambos os lados por 3, temos

$$b \equiv_5 3$$

. Ou seja, existe c tal que $b = 5c + 3$. Substituindo o b, temos

$$x = 7b + 2 = 7(5c + 3) + 2 = 35c + 23$$

Substituindo na primeira equação

$$35c + 23 \equiv_3 2$$

Ou seja

$$2c \equiv_3 0.$$

Ou seja,

$$c \equiv_3 0.$$

Ou seja, existe d tal que $c = 3d$. Voltando na equação com x:

$$x = 35c + 21 = 35(3d) + 23 = 105d + 23$$

Para termos o menor k possível, fazemos $d = 0$ e, portanto, $k = 23$.

Exercícios

Compare com o enunciado do Teorema chinês do resto.

Exercício 3.14.8. Os seguintes sistemas admitem soluções?

(a) $\begin{cases} x & \equiv_2 & 1 \\ x & \equiv_6 & 3 \end{cases}$

(b) $\begin{cases} x & \equiv_2 & 1 \\ x & \equiv_6 & 4 \end{cases}$

Exercício 3.14.9. Considere uma pista circular. O carro A demora 5 minutos para dar uma volta completa. Já o carro B, demora 3 minutos para dar uma volta completa e larga 17 minutos depois do carro A. Finalmente, o carro C demora 4 minutos para dar uma volta e larga 8 minutos depois do carro B. Supondo que esses carros fiquem dando voltas com velocidades constantes, é verdade que eles passarão pela chegada ao mesmo tempo em algum momento? Se sim, quantos minutos depois da largada do carro A será o primeiro momento em que isso ocorre?

Capítulo 4

Teoria dos Conjuntos

4.1 Cardinalidade

Definição 4.1.1. Sejam A e B dois conjuntos. Dizemos que A e B tem a mesma **cardinalidade** se existe $f : A \longrightarrow B$ bijetora. Notação: $|A| = |B|$.

Proposição 4.1.2. $|NN| = |\mathbb{N} \setminus \{0\}|$

Demonstração. Basta considerar $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ dada por $f(n) = n+1$. □

Proposição 4.1.3. *Considere* $P = \{n \in \mathbb{N} : n \text{ é par}\}$. *Então* $|P| = |\mathbb{N}|$.

Demonstração. Basta notar que a função $f : \mathbb{N} \longrightarrow P$ dada por $f(n) = 2n$ é uma bijeção (exercício). □

Proposição 4.1.4. *Sejam* A, B, C *conjuntos. Se* $|A| = |B|$ *e* $|B| = |C|$, *então* $|A| = |C|$.

Demonstração. Sejam $f : A \longrightarrow B$ e $g : B \longrightarrow C$ funções bijetoras. Note que $g \circ f : A \longrightarrow C$ é bijetora (exercício). □

Proposição 4.1.5. *Considere* $I = \{n \in \mathbb{N} : n \text{ é ímpar}\}$. *Então* $|I| = |\mathbb{N}|$.

Demonstração. Basta notar que $f : \mathbb{N} \longrightarrow I$ dada por $f(n) = 2n + 1$ é bijetora (exercício). □

Corolário 4.1.6. $|P| = |I|$.

Proposição 4.1.7. $|\mathbb{Z}| = |\mathbb{N}|$.

Demonstração. Considere $f : \mathbb{N} \longrightarrow \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

Note que f é injetora (exercício). Vamos mostrar que ela é sobrejetora. Seja $z \in \mathbb{Z}$. Se $z \geq 0$, tome $n = 2z$. Note que $f(n) = \frac{2z}{2} = z$. Se $z < 0$, tome $n = -2z - 1$. Note que $f(n) = -\frac{-2z-1+1}{2} = z$. □

Nem sempre é fácil verificar a existência de funções injetoras. Por exemplo, pode-se provar que $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. Uma maneira é você perceber que a função $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ dada por

$$f(a, b) = \frac{1}{2}(a + b)(a + b + 1) + b$$

Não é tarefa simples encontrar uma função como acima, nem mostrar que ela de fato é bijetora (vale tentar um pouco).

Para contornar esse tipo de problema, o seguinte resultado ajuda bastante:

Teorema 4.1.8 (de Cantor-Bernstein-Schroeder). *Sejam A, B conjuntos e sejam $f : A \longrightarrow B$ e $g : B \longrightarrow A$ funções injetoras. Então $|A| = |B|$.*

Demonstração. Vamos provar o resultado supondo que $A \cap B = \emptyset$. Para ver como obter o caso geral a partir desse, veja o Exercício 4.1.15. Seja $x \in A \cup B$. Defina

- $s_0^x = x$
- $s_{n+1}^x = \begin{cases} f(s_n^x) & \text{se } s_n^x \in A \\ g(s_n^x) & \text{se } s_n^x \in B. \end{cases}$
- $s_{-(n+1)}^x = \begin{cases} f^{-1}(s_{-n}^x) & \text{se } s_{-n}^x \text{ está definido e pertence a } Im(f) \\ g^{-1}(s_{-n}^x) & \text{se } s_{-n}^x \text{ está definido e pertence a } Im(g) \end{cases}$

Note que s_z^x pode não estar definido para todo $z \in \mathbb{Z}$. Considere

$$S^x = \{s_z^x \in A \cup B : z \in \mathbb{Z} \text{ e } s_z^x \text{ está definido}\}$$

Note que $(S^x)_{x \in A \cup B}$ forma uma partição sobre $A \cup B$ (cuidado, pode acontecer que $S^x = S^y$ mesmo com $x \neq y$). De fato, sejam $s_z^y = s_k^x$. Note que, então $s_{z+m}^y = s_{k+m}^x$ para qualquer $m \in \mathbb{Z}$. Logo, $S^y = S^x$.

Pois cada um dos pedaços terá uma bijeção e depois é só juntar todas

Com isso, se mostrarmos que $|S^x \cap A| = |S^x \cap B|$, terminamos. Temos alguns casos:

- Se s_z^x está definido para todo z, f induz uma bijeção, pois é sobrejetora.
- Se z é o menor tal que s_z^x está definido e $s_z^x \in A$, então f induz uma bijeção (já que é sobrejetora).
- Se z é o menor tal que s_z^x está definido e $s_z^x \in B$, então g induz uma bijeção (já que é sobrejetora).

□

Assim, fica fácil mostrar o resultado que comentamos:

Proposição 4.1.9. $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Demonstração. Considere $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ dada por $f(n) = (n, n)$ e $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $g(a, b) = 2^a 3^b$. Note que as duas funções são injetoras facilmente. □

Também podemos provar o seguinte:

Proposição 4.1.10. $|\mathbb{Q}| = |\mathbb{N}|$.

Demonstração. Como podemos ver $\mathbb{N} \subset \mathbb{Q}$, já temos a função $f : \mathbb{N} \to \mathbb{Q}$ injetora. Por outro lado, podemos tomar a função $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(\frac{a}{b}) = (a, b)$, onde $\frac{a}{b}$ está na forma simplificada. Note que tal função é injetora. Como $|\mathbb{N}| = |\mathbb{Z}|$, temos que $|\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$ (veja o Alongamento 4.1.11) e como $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, temos que $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$. Assim, existe $h : \mathbb{Q} \to \mathbb{N}$ injetora. □

Alongamentos

Alongamento 4.1.11. Sejam A, B, X, Y conjuntos tais que $|A| = |X|$ e $|B| = |Y|$. Mostre que $||A \times B| = |X \times Y|$.

Alongamento 4.1.12. Mostre que se existe $f : A \to B$ sobrejetora, então existe $g : B \to A$ injetora.

Alongamento 4.1.13. Mostre que se existe $f : A \to B$ injetora, então existe $g : B \to A$ sobrejetora.

Exercícios

Exercício 4.1.14. Mostre que $|\mathbb{N}^n| = |\mathbb{N}|$ para todo $n \in \mathbb{N}_{>0}$.

Exercício 4.1.15. Este é um um roteiro para mostrar que, se vale o Teorema de Cantor-Bernstein-Schoroeder para conjuntos disjuntos, então vale para o caso geral. Sejam $f : A \to B$ e $g : B \to A$ injetoras.

(a) Considere os conjuntos $A' = \{(a, 0) : a \in A\}$ e $B' = \{(b, 1) : b \in B\}$. Note que tais conjuntos são disjuntos.

(b) Mostre que $|A| = |A'|$ e $|B| = |B'|$.

(c) Conclua o resultado.

Exercício 4.1.16. Enuncie e prove uma segunda versão do Teorema de Cantor-Bernstein-Schoroeder, onde as funções f e g do enunciado original são sobrejetoras em vez de injetoras.

4.2 Conjunto das partes e mais cardinalidades

Um dos resultados que vamos mostrar nesta seção é que o conjunto dos reais tem cardinalidade maior que a dos naturais. Faremos isso de uma maneira indireta, mas os resultados intermediários também são úteis em outras situações.

Vamos começar com o conjunto das partes, que nada mais é que o conjunto de todos os subconjuntos de um conjunto fixado:

Definição 4.2.1. Considere X um conjunto. Chamamos de $\wp(X)$ (**conjunto das partes** de X) o conjunto de todos os subconjuntos de X.

Exemplo 4.2.2. Seja $A = \{1, 2, 3\}$. Então

$$\wp(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Proposição 4.2.3. *Se A tem n elementos, então $\wp(A)$ tem 2^n elementos.*

Demonstração. Vamos mostrar o resultado por indução sobre n. Se $n = 0$, então $A = \emptyset$ e, como $\emptyset \subset \emptyset$, temos que $\wp(\emptyset) = \{\emptyset\}$. Ou seja, $\wp(\emptyset)$ tem um elemento, como queríamos.

Agora suponha o resultado para n e vamos provar para $n + 1$. Seja A com $n + 1$ elementos. Seja $a \in A$. Considere $P(A) = \{X \subset A : a \notin X\}$. Ou seja, $P(A) = \wp(A \setminus \{a\})$. Assim, por hipótese de indução, temos que

$P(A)$ tem 2^n elemento. Considere $Q(A) = \{X \subset A : a \in A\}$. Note que $f : P(A) \to Q(A)$ dada por

$$f(X) = X \cup \{a\}$$

é uma bijeção (exercício). Logo, $P(A)$ e $Q(A)$ tem 2^n elementos cada. Finalmente, note que $\wp(A) = P(A) \cup Q(A)$ e que $P(A) \cap Q(A) = \emptyset$. Assim, $\wp(A)$ tem $2^n + 2^n = 2^{n+1}$ elementos como queríamos. □

Notação: indicaremos por $|X| \neq |Y|$ quando não existe uma bijeção entre X e Y.

Proposição 4.2.4. $|\mathbb{N}| \neq |\wp(\mathbb{N})|$.

Demonstração. Suponha que exista $f : \mathbb{N} \longrightarrow \wp(\mathbb{N})$ bijeção. Considere o conjunto $A = \{a \in \mathbb{N} : a \notin f(a)\}$. Como f é uma bijeção e $A \in \wp(\mathbb{N})$, temos que existe $b \in \mathbb{N}$ tal que $f(b) = A$. Vamos ver que isso dá uma contradição. Note que se $b \in A$, então $b \in f(b)$ e, portanto, $b \notin A$. Por outro lado, se $b \notin A$, então $b \notin f(b)$ e, portanto, $b \in A$. □

Note que, claramente, existe uma função injetora de $|\mathbb{N}|$ em $wp(\mathbb{N})|$. Por exemplo, podemos tomar $f(n) = \{n\}$. Assim, o que o resultado anterior nos diz é que não existe uma função injetora de $\wp(\mathbb{N})$ em $\mathbb{N}$ (ou, equivalentemente, que não existe uma função sobrejetora de $\mathbb{N}$ em $\wp(\mathbb{N})$.

Proposição 4.2.5. *Existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{N})$.*

Para uma demonstração alternativa, veja o Exercício 4.2.14

Demonstração. Note que basta provarmos que existe uma função injetora de $\mathbb{R}$ em $\wp(\mathbb{Q})$ (veja o Alongamento 4.2.12). Para cada $r \in \mathbb{R}$, existe $(q_n^r)_{n\in\mathbb{N}}$ sequência de racionais que converge para r. Podemos tomar tal sequência de forma que $x_n^r \neq x_m^r$ se $n \neq m$ (pense um pouco para se convencer disso). Vamos provar que a função $f : \mathbb{R} \to \wp(\mathbb{Q})$ dada por

$$f(r) = \{x_n^r : n \in \mathbb{N}\}$$

é injetora.

Sejam $r \neq s \in \mathbb{R}$. Considere $\varepsilon = |r - s|$. Como $(x_n^r)_{n\in\mathbb{N}}$ converge para r, existe n_r tal que, se $n \geq n_r$, temos

$$|x_n^r - r| < \frac{\varepsilon}{2}$$

Analogamente, existe n_s tal que, se $n \geq n_s$, temos

$$|x_n^s - s| < \frac{\varepsilon}{2}$$

Podemos fazer isso pois existem infinitos x_m^r distintos.
Tem um ponto num conjunto que não está no outro - ou seja, os dois conjuntos são distintos.

Assim, considere $m \geq n_r$ e de forma que $x_m^r \neq= x_0^s, ..., x_{n_s}^s$. Note que $x_m^r \in f(x_r)$. Assim, se mostrarmos que $x_m^r \notin f(x_s)$, teremos os resultado. Suponha que $x_m^r \in f(s)$. Como $x_m^r \neq x_0^s, ..., x_{n_s}^s$, temos que existe $k > n_s$ tal que $x_m^r = x_k^s$. Assim

$$\begin{aligned} |r-s| &= |r - x_m^r + x_m^r - x_k^s + x_k^s - s| \\ &\leq |r - x_m^r| + |x_m^r - x_k^s| + |x_k^s - s| \\ &< \tfrac{\varepsilon}{2} + 0 + \tfrac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

contradição. □

Já temos "metade" da igualdade $|\mathbb{R}| = |\wp(\mathbb{N})|$. Vamos agora à outra metade.

Definição 4.2.6. Dados conjuntos $A \subset B$, denotamos por $\chi_A^B : B \to \{0,1\}$ a função dada por

$$\chi_A^B(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

Chamamos tal função de **função característica** de A em B. Normalmente, quando B está claro no contexto, o omitimos.

Proposição 4.2.7. $|\mathcal{F}| = |\wp(\mathbb{N})|$ *onde* $\mathcal{F} = \{\chi_A^{\mathbb{N}} : A \subset \mathbb{N}\}$.

Demonstração. Basta notar que a função $\varphi : \mathcal{F} \to \wp(\mathbb{N})$ dada por $\varphi(\chi_A) = A$ é bijetora. □

Cuidado aqui - temos uma função onde cada elemento de seu domínimo é uma função e cada elemento de sua imagem é um conjunto.

Proposição 4.2.8. *Existe uma função injetora de* $\wp(\mathbb{N})$ *em* $\mathbb{R}$.

Demonstração. Note que é suficiente mostrarmos que existe uma função injetora de $\mathcal{F}$ em $\mathbb{R}$. Considere $\varphi : \mathcal{F} \to \mathbb{R}$ dada por

Você pode escrever essa função em termos de uma somatória se preferir.

$$\varphi(\chi_A) = 0, \chi_A(0)\chi_A(1)\cdots\chi_A(n)\cdots$$

□

Corolário 4.2.9. $|\mathbb{R}| = |\wp(\mathbb{N})|$

Corolário 4.2.10. *Não existe* $f : \mathbb{R} \to \mathbb{N}$ *injetora.*

Alongamentos

Alongamento 4.2.11. Determine $\wp(X)$ onde:

(a) $X = \{a, b, c, d\}$;

(b) $X = \{\emptyset\}$;

(c) $X = \emptyset$;

(d) $X = \wp(\{1, 2\})$.

Alongamento 4.2.12. Mostre que se $|A| = |B|$, então $|\wp(A)| = |\wp(B)|$.

Exercícios

Exercício 4.2.13. Mostre que, dado X um conjunto, então $|X| \neq |\wp(X)|$.

Exercício 4.2.14. Lembre-se que cada $r \in \mathbb{R}$ pode ser visto como um par (I_r, J_r) que é um corte de Dedekind. Mostre que a função $f : \mathbb{R} \to \wp(\mathbb{Q})$ dada por $f(r) = I_r$ é injetora. Use isso para uma demonstração alternativa da Proposição 4.2.5

4.3 Enumerabilidade

Nesta seção vamos apresentar os resultados na forma de exercícios.

Definição 4.3.1. Dizemos que um conjunto X é **enumerável**[1] se $|X| = |\mathbb{N}|$.

Exercício 4.3.2. Sejam A e B conjuntos enumeráveis. Mostre que $A \cup B$ é enumerável (para facilitar, mostre o caso em que eles são disjuntos).

Exercício 4.3.3. Mostre que, se para cada $n \in \mathbb{N}$, X_n é enumerável, então $\bigcup_{n\in\mathbb{N}} X_n$ é enumerável (novamente, faça o caso em que eles são todos dois a dois disjuntos).

Exercício 4.3.4. Seja X um conjunto enumerável. Para cada $n \in \mathbb{N}_{>0}$, considere $X_n = \{A \subset X : A \text{ tem } n \text{ elementos}\}$.

(a) Mostre que X_1 é enumerável.

(b) Seja $x \in X$. Lembre-se que existe $f : X \to X \setminus \{x\}$ bijetora. Mostre que $|X_n| = |Y|$, onde $Y = \{B \subset X \setminus \{x\} : B \text{ tem } n \text{ elementos}\}$.

[1] Em geral, um conjunto finito também é dito enumerável, mas vamos supor nestes exercícios que todos os conjuntos são infinitos para facilitar.

(c) Dado $x \in X$, mostre que $|W| = |X_n|$, onde $W = \{B \subset X : x \in B \text{ e } B \text{ tem } n+1 \text{ elementos}\}$.

(d) Mostre que cada X_n é enumerável.

Definição 4.3.5. Dizemos que um conjunto A é **finito** se A tem n elementos para algum n.

(e) Mostre que $\mathcal{F}$ é enumerável, onde $\mathcal{F} = \{F \subset X : F \text{ é finito}\}$.

Um conjunto que não seja nem finito, nem admita uma bijeção com $\mathbb{N}$ é dito **não enumerável**. Já vimos que $\wp(\mathbb{N})$ é não enumerável. E, com os exercícios acima, vimos em particular que o conjunto $\mathcal{F}$ dos subconjuntos finitos de $\mathbb{N}$ é enunumerável. Desta forma, se considerarmos que $\mathcal{I}$ é o conjunto dos subconjuntos infinitos de $\mathbb{N}$, temos automaticamente que $\mathcal{I}$ é não enumerável, já que

$$\wp(\mathbb{N}) = \mathcal{F} \cup \mathcal{I}$$

Vamos terminar essa seção apresentando um resultado interessante sobre os números reais:

Definição 4.3.6. Dizemos que $r \in \mathbb{R}$ é um **número algébrico** se existe um polinômio p não nulo com coeficientes racionais tal que $p(r) = 0$.

Exemplo 4.3.7. Qualquer $q \in \mathbb{Q}$ é algébrico, já que $x - q$ é um polinômico como acima. $\sqrt{2}$ também é algébrico, já que $x^2 - 2$ também é como acima.

Proposição 4.3.8. *O conjunto dos números algébricos é enumerável.*

Demonstração. Seja P' o conjunto de todos os polinômios de coeficientes racionais. Note que, para qualquer $n \in \mathbb{N}_{>0}$, $\mathbb{Q}^n$ é enumerável. Assim, $Q = \bigcup_{n \in \mathbb{N}_{>0}} \mathbb{Q}^n$ é enumerável. Note que existe uma bijeção $\varphi : Q \to P$ dada por

$$\varphi(q_0, ..., q_n) = q_0 + q_1 x + \cdots + q_n x^n$$

Assim, se considerarmos P o conjunto dos polinômios não nulos de coeficientes racionais, temos que P também é enumerável. Seja $f : \mathbb{N} \to P$ bijeção. Dado $n \in \mathbb{N}$, considere

$$Z_n = \{r \in \mathbb{R} : p(r) = 0, \text{onde } p = f(n)\}$$

Note que cada Z_n é finito (isso foge do escopo desse texto, mas não é tão ruim de provar). Note também que $\bigcup_{n \in \mathbb{N}} Z_n$ é o conjunto de todos os números algébricos. Assim, como tal união é enumerável, temos os resultados. □

4.4 Axiomas

Qual a ideia intuitiva que temos de conjuntos? Normalmente pensamos que um conjunto é qualquer coleção de coisa. Seguindo esse raciocínio, poderíamos fazer:

$$T = \{X : X \text{ é um conjunto}\}$$

Este seria o conjunto de todos os conjuntos. Como o próprio T é um conjunto, temos que $T \in T$. Isso é estranho, mas ainda assim não parece ser uma contradição. Como isso é estranho, poderíamos então criar o conjunto dos conjuntos não estranhos:

$$R = \{X \in T : X \notin X\}$$

Teríamos, por exemplo, que $T \notin R$. Por outro lado, $\mathbb{N} \in R$. Mas e R? Note que não temos opção para R: se $R \in R$, pela definição de R, temos que $R \notin R$. Por outro lado, se $R \notin R$, novamente pela definição de R, temos que $R \in R$. Ou seja, a existência de R implica numa contradição. Este é conhecido como o **paradoxo de Russel**. Quem quiser saber mais sobre a história deste problema, recomendamos [2].

Para evitar problemas como o Paradoxo de Russel, apresentamos uma lista do que podemos fazer com conjuntos. Esta lista é conhecida como ZFC (Zermelo, Fraenkel e Axioma da Escolha). Vamos apresentar a lista aqui, com alguns comentários.

Quem quiser saber mais sobre o assunto, recomendamos [4].

Existência Existe um conjunto que não possui elementos. Em símbolos, $\exists x\ \forall y\ y \notin x$. Denotamos tal conjunto por $\emptyset$.

Extensão Dois conjunto são iguais se possuem os mesmos elementos. Em símbolos: $\forall x\ \forall y(\forall z\ (z \in x \to z \in y) \wedge (z \in y \to z \in x)) \to x = y$.

Quando ocorre $\forall z\ z \in y \to z \in x$, usamos a seguinte notação: $y \subset x$. Desta forma, podemos denotar o último axioma como $\forall x\ \forall y(x \subset y \wedge y \subset x) \to x = y$.

Separação Se P é uma propriedade e x é um conjunto, existe o subconjunto y que contém exatamente os elementos de x que satisfazem a propriedade P. Em símbolos $\forall x\ \exists y((\forall z \in x\ P(z) \to z \in y) \wedge (\forall z \in y \to (z \in x \wedge P(z))))$. A notação usual para isso é $y = \{z \in x : P(z)\}$.

Par Se x e y são conjuntos, então existe um conjunto z que contém os dois como elementos. Em símbolos: $\forall x\ \forall y\ \exists z\ x \in z \wedge y \in z$. Note que

tal axioma não garante que os únicos elementos de z sejam x e y mas, para isso, podemos usar o axioma da Separação. No caso em que os únicos elementos de z sejam x e y a notação fica $z = \{x, y\}$. Se, além disso, se $x = y$, usamos a notação $z = \{x\}$.

União Para todo conjunto x, existe um conjunto y que contém todos os elementos dos elementos de x. Em símbolos: $\forall x\ \exists y\ \forall a\ \exists z \in x\ a \in z \to a \in y$. Novamente, tal axioma não garante que os únicos elementos de y sejam esses, mas isso pode ser feito utilizando-se o axioma da Separação. No caso em que o conjunto y contém exatamente tais elementos, a notação usual é $y = \bigcup_{z \in x} z$. Agora podemos provar que dados conjuntos A e B, existe o conjunto $A \cup B$. Primeiramente mostramos que existe o conjunto $\{A, B\}$ (exercício). Depois, mostramos que existe $y = \bigcup_{z \in \{A,B\}} z$ (note que este é o conjunto desejado).

Partes Dado x um conjunto, existe um conjunto y que contém todos os subconjuntos de x. Em símbolos: $\forall x\ \exists y\ \forall z\ z \subset x \to z \in y$. Novamente, não temos garantido que os únicos elementos de y sejam os subconjuntos de x, mas podemos contornar isso com o axioma da separação. Se for o caso em que os elementos de y forem os subconjuntos de x, usamos a notação $y = \wp(x)$.

Infinito Dado um conjunto x, denotamos por $S(x)$ o conjunto $x \cup \{x\}$ (podemos fazer isso pelo axioma do par (veja o Exercício **4.4.3** e da união). O axioma do infinito diz que existe um conjunto A tal que $\emptyset \in A$ e tal que para todo $x \in A$, $S(x) \in A$. Em símbolos: $\exists A\ \emptyset \in A \wedge (\forall x \in A\ S(x) \in A)$.

Há mais alguns axiomas, mas os deixaremos para a próxima seção.

Exercícios

4.4.1. Mostre que o conjunto vazio é único. Isto é, que só existe um conjunto sem elementos.

4.4.2. Mostre que existem os seguintes conjuntos:

(a) $\{\emptyset\}$;

(b) $\{\{\emptyset\}\}$;

(c) $\{\emptyset, \{\emptyset\}\}$.

4.4.3. Se x é um conjunto, mostre que $\{x\}$ também é um conjunto.

4.4.4. Mostre que se $\{x\}$ é um conjunto, então x também é.

4.4.5. A ideia deste exercício é formalizar o conceito de intersecção. Seja A um conjunto não vazio. Seja $b \in A$. Defina $\bigcap_{a\in A} a = \{x \in b : \forall a \in A\ x \in a\}$.

(a) Justifique a existência de tal conjunto.

(b) Mostre que tal definição independe da escolha do b. Isto é, seja $c \in A$. Mostre que $\{x \in b : \forall a \in A\ x \in a\} = \{x \in c : \forall a \in A\ x \in a\}$;

(c) Se A e B são conjuntos, defina $A \cap B$ com o que foi feito acima.

4.4.6. Mostre que podemos omitir o axioma da existência. Isto é, que a existência do conjunto vazio pode ser obtida a partir dos outros axiomas.

4.4.7. Mostre que não existe o conjunto de todos os conjuntos.

4.4.8. Mostre que se a, b, c são conjuntos, então existe o conjunto $\{a, b, c\}$.

4.5 Funções e o restante dos axiomas

Começamos com a ideia principal de uma função: associar a cada elemento de um lado, um único elemento do outro. Com isso em mente, podemos definir uma fórmula do "tipo função". Basicamente é uma fórmula P, que a cada $a_1, ..., a_n$ conjuntos, associa um único conjunto b tal que $P(b, a_1, ..., a_n)$ seja satisfeita. Muitas vezes usamos uma notação mais parecida com função $b = f(a_1, ..., a_n)$.

Exemplo 4.5.1. Considere $P(x, y)$ sendo $y \in x \wedge (\forall z \in x\ z = x)$. Note que a cada a que tomarmos, só existe um conjunto b satisfazendo $P(b, a)$ (a saber, $b = \{a\}$).

Exemplo 4.5.2. Se omitirmos a parte "$y \in x$" na propriedade P anterior, não temos mais que P é do tipo função. Pois $b_1 = \{a, \emptyset\}$ como $b_2 = \{a\}$ (suponha $a \neq \emptyset$) são distintos e $P(b_1, a)$ e $P(b_2, a)$ são satisfeitas.

Podemos formalizar a ideia do que é uma função usando o que já temos até aqui. Comecemos com a ideia do par ordenado:

Definição 4.5.3. Sejam x, y dois conjuntos. Definimos o **par ordenado** como o conjunto $\{\{x\}, \{x, y\}\}$. Notação (x, y). Neste caso, dizemos que x é a primeira coordenada do par e que y é a segunda.

Observação 4.5.4.

- Existe uma fórmula P tal que $P(x)$ é verdadeira se, e somente se, x é um par ordenado;
- Existe uma fórmula P_1 tal que $P_1(a, x)$ é verdadeira se, e somente se x é um par ordenado e a é a primeira coordenada de x;
- Existe uma fórmula P_2 tal que $P_2(a, x)$ é verdadeira se, e somente se x é um par ordenado e a é a segunda coordenada de x;

Proposição 4.5.5. *Sejam (x, y) e (a, b) dois pares ordenados. Então $(x, y) = (a, b)$ se, e somente se, $x = a$ e $y = b$.*

Definição 4.5.6. Se X e Y são conjuntos, denotamos por $X \times Y$ o conjunto de todos os pares ordenados (x, y) tais que $x \in X$ e $y \in Y$.

Observação 4.5.7. Na verdade, é necessário provar que se X e Y são conjuntos, então $X \times Y$ é de fato um conjunto. Isso é possível usando o fato que $X \cup Y$ é conjunto e depois que $\wp(X \cup Y)$ também é. Finalmente, usamos o axioma da separação para tomarmos apenas os pares ordenados desejados.

Definição 4.5.8. Chamamos de uma função f de X em Y um subconjunto de $X \times Y$ tal que, para todo $x \in X$, existe $y \in Y$ tal que $(x, y) \in f$ e que se $(x, y_1), (x, y_2) \in f$, então $y_1 = y_2$. Neste caso, denotamos $(x, y) \in f$ como $f(x) = y$.

Agora podemos continuar com a lista dos axiomas de ZFC:

Substituição Considere P uma fórmula do tipo função. Se x é um conjunto, então existe o conjunto y de todos os elementos associados ao aplicar-se P aos elementos de x. Em símbolos: $\forall x \ \ (\forall a_1, ..., a_n \in x \exists! z \ P(z, a_1, ..., a_n)) \rightarrow (\exists y \forall z \ \forall a_1, ..., a_n \in x P(z, a_1, ..., a_n) \rightarrow z \in y)$. O $\exists! z$ quer dizer "existe um único z satisfazendo o que vem a seguir". No caso em que y contém exatamente tais elementos, denotamos $y = \{z : P(z, a_1, ..., a_n), a_1, ..., a_n \in x\}$. Ou, usando a notação de função, $y = \{f(a_1, ..., a_n) : a_1, ..., a_n\}$.

Fundação Todo conjunto x não vazio possui um elemento que é disjunto de x. Em símbolos $\forall x \ x \neq \emptyset \rightarrow (\exists y \in x \ y \cap x = \emptyset)$. Este é o axioma de ZFC que é menos usado em matemática em geral. Apesar disso, serve, por exemplo, para impedir que existam conjuntos x tais que $x \in x$ (veja o Exercício **4.5.2**). Também o usaremos para mostrar a propriedade fundamental do par ordenado.

Escolha Se x é um conjunto de conjuntos não vazios, então existe uma função $f : x \longrightarrow \bigcup_{a \in x} a$ tal que $f(x) \in x$. Ou seja, se temos uma família de conjuntos não vazios, podemos "escolher" um elemento de cada conjunto.

Exercícios

4.5.1. (a) Escreva numa fórmula "x tem exatamente um elemento" (um conjunto desta forma é dito **unitário**);

(b) Escreva numa fórmula "x tem exatamente dois elementos".

4.5.2. Mostre que não existe x tal que $x \in x$.

4.5.3. Mostre que não existem conjuntos a, b tais que $a \in b \in a$.

4.5.4. Seja X um conjunto. Mostre que existe o conjunto A formado por todos os unitários de elementos de X. (Isto é, $A = \{\{x\} : x \in X\}$).

4.6 Exercícios do Capítulo

4.6.1. Dizemos que um conjunto X é **indutivo** se $\emptyset \in X$ e, para todo $x \in X$, $S(x) = x \cup \{x\} \in X$. Considere A o conjunto dado pelo axioma da inifinito. Considere $\mathcal{A} = \{a \in \wp(A) : a \text{ é indutivo}\}$.

(a) Mostre que $A \in \mathcal{A}$;

(b) Mostre que, para todo $a \in \mathcal{A}$, $\emptyset \in a$;

(c) Considere $N = \bigcap_{a \in \mathcal{A}} a$. Mostre que $\emptyset \in N$;

(d) Mostre que $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\} \in N$.

(e) Mostre que N é indutivo.

Observação 4.6.1. Esta é a maneira usual de se construir o conjunto $\mathbb{N}$ dos naturais. Chamamos de 0 o elemento de N que possui 0 elementos (isto é, o $\emptyset$), chamamos de 1 o elemento de N que possui 1 elemento (isto é, o $\{\emptyset\}$), chamamos de 2 o elemento de N que possui 2 elementos (isto é, o $\{\emptyset, \{\emptyset\}\}$) etc.

Capítulo 5

Aplicações

5.1 Boa ordenação

Definição 5.1.1. Dizemos que uma ordem $\preceq$ é uma **boa ordem** sobre X se para qualquer $A \subset X$ não vazio é tal que A possui elemento mínimo.

Exemplo 5.1.2. A ordem usual sobre $\mathbb{N}$ é uma boa ordem (pelo Princípio do Menor Elemento).

Exemplo 5.1.3. A ordem usual sobre $]0,1[$ não é uma boa ordem pois o próprio conjunto $]0,1[$ não possui mínimo.

Teorema 5.1.4. *Para todo conjunto existe uma boa ordem.*

Na verdade, podemos colocar o teorema anterior no lugar do axioma da escolha - para isso, deveríamos provar que com o axioma da escolha podemos provar o teorema anterior (não vamos fazer isso aqui) e depois provar que, supondo o teorema anterior, podemos provar o axioma da escolha. É o que faremos no próximo resultado:

Proposição 5.1.5. *Se todo conjunto pode ser bem ordenado, então vale o axioma da escolha.*

Demonstração. Seja X um conjunto de conjuntos não vazios. Precisamos mostrar que existe uma função $f : X \longrightarrow \bigcup_{x \in X} x$ tal que $f(x) \in x$ para todo $x \in X$. Como X é um conjunto, temos que $\bigcup_{x \in X} x$ é um conjunto. Logo, existe $\preceq$ uma boa ordem sobre $\bigcup_{x \in X} x$. Defina $f : X \longrightarrow \bigcup_{x \in X} x$ como $f(x) = \min x$ (a ideia aqui é que sabendo que existe a boa ordem, podemos fazer uma única "escolha" de antemão). □

Teorema 5.1.6. *Todo espaço vetorial possui base.*

Demonstração. Seja V um espaço vetorial. Dado $A \subset V$, vamos denotar por $[A]$ o subespaço gerado por A (lembre-se que este é o subconjunto de V que contém A e todas as combinações lineares dos elementos de A). Por convenção, adotemos $[\emptyset] = \{0\}$. Seja $\preceq$ uma boa ordem sobre V. Defina B da seguinte maneira

$$B = \{v \in V : v \notin [\{w \in V : w \prec v\}]$$

Vamos mostrar que B é uma base para V. Suponha que B não seja linearmente independente. Sejam $b_1, ..., b_n \in B$ e $\alpha_1, ..., \alpha_n \in \mathbb{R}$ tais que $\sum_{i=1}^{n} \alpha_i b_i = 0$ e $\alpha_i \neq 0$ para todo i. Seja b_j o máximo de $\{b_1, ..., b_n\}$ (com relação a $\preceq$). Note que $b_j \in [\{b_1, ..., b_n\} \setminus \{b_j\}]$ e, portanto, $b_j \in [\{w \in V : w \prec b_j\}]$. Logo, $b_j \notin B$, contradição.

Agora vamos mostrar que B é gerador. Isto é, que $[B] = V$. Suponha que não. Então existe $b \notin [B]$. Seja o menor b com tal propriedade (estamos usando que $\preceq$ é boa ordem). Logo, para todo $w \prec b$, $w \in [B]$. Ou seja, $[\{w \in V : w \prec b\}] \subset [B]$ (isso é um exercício de álgebra linear). Como $b \notin [B]$, temos que $b \notin [\{w \in V : w \prec b\}]$ e, portanto, $b \in B$ contradição (pois $B \subset [B]$). □

Proposição 5.1.7 (Indução para boa ordem)**.** *Seja X um conjunto bem ordenado por $\preceq$. Seja P uma propriedade tal que, dado qualquer $x \in X$, se $P(y)$ vale para todo $y \prec x$, então vale $P(x)$.. Então para todo $x \in X$ vale $P(x)$.*

Leia essa hipótese sobre P como "se vale para todo y ants de x, vale para x também".

Demonstração. Suponha que não. Então o conjunto

$$\{a \in X : \text{ não vale } P(a)\}$$

é não vazio. Seja $m = \min\{a \in X : \text{não vale } P(a)\}$ (estamos usando a boa ordem). Note que, pela minimalidade de m, todo $k \prec m$ é tal que vale $P(k)$. Logo, pela hipótese sobre P, temos que vale $P(m)$. Mas isso contradiz o fato de $m \in \{a \in X : \text{não vale } P(a)\}$. □

Vamos chamar de um ω_1 um conjunto bem ordenado por $\preceq$ tal que ω_1 é não enumerável e tal que, para qualquer $x \in \omega_1$, o conjunto

Essa não é a definição usual de ω_1, mas optamos por essa por simplicidade.

$$\{y \in \omega_1 : y \preceq x\}$$

é enumerável.

Pode-se mostrar que dados quaisquer dois conjuntos com a propriedade acima, eles são "isomorfos no sentido de ordem". Isto é, existe uma bijeção entre eles que preserva a ordem. Isso nos dá a "unicidade" de tal conjunto. Falta mostrar que existe algum conjunto com tal propriedade. Vamos mostrar isso agora.

Seja $\preceq$ uma boa ordem sobre $\mathbb{R}$. Já sabemos que $\mathbb{R}$ é não enumerável - isto é, não não existe uma sobrejeção de $\mathbb{N}$ em $\mathbb{R}$ (note que a outra sobrejeção obviamente existe). Suponha que não exista $x \in \mathbb{R}$ tal que

$$\{y \in \mathbb{R} : y \prec x\}$$

seja não enumerável. Se isso acontece, o próprio $\mathbb{R}$ com essa ordem serve como ω_1. Se existe tal x, então podemos tomar o menor com tal propriedade. Fazendo isso, pela minimalidade, obtemos que, para qualquer $y \in x$:

$$\{z \in \mathbb{R} : z \prec y\}$$

é enumerável e, portanto

$$\{y \in \mathbb{R} : y \prec x\}$$

serve como ω_1.

Pela maneira como ω_1 foi construido, pode-se mostrar que, dado qualquer conjunto X não enumerável, existe $f : \omega_1 \to X$ injetora. Ou seja, ω_1 represnenta o menor tamanho possível para um conjunto não enumerável.

Nesse contexto, muitas vezes denota-se ω_1 por $\aleph_1$.

Finalmente, poderíamos nos perguntar se $|\omega_1| = |\mathbb{R}|$. Essa é conhecida como a hipótese do contínuo. Essa afirmação não é consequência dos axiomas de ZFC, nem sua negação é.

Exercícios

5.1.1. Mostre que se $\preceq$ é uma boa ordem sobre X, então $\preceq$ é uma ordem total.

5.1.2. Encontre o erro na seguinte argumentação: O Teorema da boa ordem diz que todo conjunto tem uma boa ordem. Mas o seguinte subconjunto $]0, 1[$ de $\mathbb{R}$ não possui menor elemento, logo esta não é uma boa ordem e, portanto, o teorema não vale.

5.1.3. Considere os seguintes conjuntos ordenados. Decida quais ordens são boas:

(a) $\mathbb{R}$ com a ordem usual;

(b) $\mathbb{Q}$ com a ordem usual;

(c) $[0, 1]$ com a ordem usual;

(d) $\{1\}$ com a igualdade como ordem;

(e) $\mathbb{N} \setminus \{0\}$ com a $|$ como ordem (lembrete: $a|b$ se a divide b).

Dicas de alguns exercícios

1.1.9 O que é falar uma mentira sobre uma verdade? E falar a verdade sobre uma mentira?

1.2.8 No item (a), basta notar que para a ser igual a b, basta que a não seja maior que b nem que seja menor. Assim, uma proposição desejada é $(\sim p) \wedge (\sim q)$.

1.2.9 Escreva quando $p \wedge q$ é falso. Negue isso.

1.4.13 Tente ver qual a relação entre os seguintes pontos: $(1,1), (1,2), (2,1)$ e $(2,2)$.

1.4.17 Considere o conjunto $[0,1]$ com a ordem estrita usual.

1.4.18 Considere os conjuntos $\mathbb{Q}$ e $\mathbb{N}$ com as ordens estritas usuais.

2.2.4 Faça o caso com 2 cavalos $(n = 1)$.

2.3.13 Some tal elemento com 0.

2.3.14

a Suponha que $b \neq 0$. Então $b = s(c)$ para algum $c \in \mathbb{N}$.

b Use $b = 0$ dado pelo item anterior e faça a conta.

2.4.10 Considere R dado por $n + 1$ retas. Separe uma das retas. Escreva $2R = 2V + 2N$, onde V é quantidade de regiões que já se tinha antes da tal reta e N é a quantidade acrescida pela reta.

2.4.11

a Calcule $f(1)$ como $f(s(0))$ pela definição. Depois calcule $f(2)$ como $f(s(1))$ e use o que você já fez e a definição.

b Olhe as Proposições **2.3.5** e **2.4.2**.

2.5.4 Mostre por contradição. Use o fato que $\leq$ é total. Veja o Lema **2.5.4**.

2.6.1 Multiplique tal elemento por 1.

2.6.2 Mostre por indução no número de postos. Note que sempre tem um posto com combustível suficiente para se chegar no próximo posto.

3.2.13

b Suponha que $[x] \cap [y] \neq \emptyset$. Mostre que $[x] = [y]$.

3.2.14 Mostre que $\varphi([a]) = f(a)$ é bijetora (não esqueça de mostrar que ela está bem definida).

3.3.17 Olhe a demonstração da Proposição **3.3.4**. Suponha $(a, b) \sim (x, y)$, $(c, d) \sim (w, z)$. Obtenha as equações (multiplicando por termos adequados): $ac + yc = bc + cx$, $db + dx = da + dy$, $xc + xz = xd + wx$ e $dy + wy = cy + zy$. Some tais equações.

3.4.14 Escreva $[(x, y)]$ na forma canônica. Analise os casos.

3.4.17

a Use o Exercício **3.4.15**.

b Use o Exercício **3.4.15**. Atenção com o fato que produto de positivos é positivo (Proposicao **3.4.7**).

c Use o Exercício **3.4.15**. Lembre que $-a + a = 0$ e que se a é negativo, então $-a$ é positivo.

3.5.3

a Use que $a \leq |a|$ e o Exercício **3.4.17**.

b Use que $-|a| \leq a$ e o Exercício **3.4.17**.

c Separe os casos em que $a + b \geq 0$ e $a + b < 0$ e use os itens anteriores.

a Use o Teorema **3.5.8** para $-a$. Encontre um valor q' e r' para o $-a$. Escreva a em função de q' e r'. Some e subtraia b para encontrar q e r como desejados.

b Aplique o item anterior e o Teorema **3.5.8** para $-b$.

3.5.6 Use o princípio do menor elemento.

3.6.3

b Use o fato que $mdc(a, b)|a$;

c Note que ak é múltiplo de a e de b;

d Use o fato que $mmc(a, b) \leq ak$.

3.7.8 Considere o resto da divisão do número por 100.

3.7.9 Você quer achar o resto da divisão de $2^n + 1$ por 3. Lembre que $2 \equiv_3 -1$.

3.8.2 Veja a demonstração de **3.7.4** para mostrar que $r_1 - r_2 = 0$.

3.8.3

b Use o algoritmo da divisão de Euclides.

d Aplique o algoritmo da divisão de Euclides para dividir $2k+1$ por 2. Use a unicidade dada no exercício **3.8.2**.

e Num dos lados, suponha que n não é par e use o item (b).

3.8.4 Use a unicidade do algoritmo de Euclides.

3.8.5 Suponha que $p_1, ..., p_n$ sejam todos os primos. Use o exercício anterior.

3.10.1 Tente mexer com a transitiva.

4.2.13 Veja a demonstração da Proposição **4.2.4**

4.4.5

a Use o axioma da separação.

c Veja como fizemos com a união.

4.4.6 Use o axioma do infinito e o da separação.

4.4.7 Use o axioma da separação para reproduzir o paradoxo de Russel.

4.5.2 Considere o conjunto $\{x\}$ e use o axioma da fundação.

4.5.3 Considere o conjunto $\{a, b\}$ e use o axioma da fundação.

4.5.4 Use o axioma da susbtituição.

5.1.1 Considere conjuntos da forma $\{x, y\} \subset X$.

Referências Bibliográficas

[1] I. Dias and S. M. S. de Godoy. *Elementos de Matemática*. Notas de aulas, ICMC-USP, 2010.

[2] A. Doxiadis and C. H. Papadimitriou. *Logicomix*. WMF Martins Fontes, São Paulo, 2010.

[3] H. B. Enderton. *A mathematical introduction to logic*. Academic Press, New York, 1972.

[4] P. R. Halmos. *Naive set theory*. The University Series in Undergraduate Mathematics. D. Van Nostrand Co., Princeton, N.J.-Toronto-London-New York, 1960.

Notação

Índice Remissivo