Uma descida infinita em Matemática Pura

POR CLIVE NEWSTEAD
Com adaptações de Jonas Galvao Xavier/Tradução por George Galvao Moreira

Última atualização em Thursday 7th March 2024

Prévia da Primeira Edição(Em breve)

ISBN 978-1-950215-00-3 (Brochura)
ISBN 978-1-950215-01-0 (Capa dura)

Uma cópia gratuita de *Uma Descida Infinita Em Matemática Pura* pode ser obtido através do site do livro:
https://infinitedescent.xyz

Para meus Pais,
Imogen e Matthew (1952–2021),
Que me ensinaram tanto.

Contents

Preface **vii**

Reconhecimentos **xiii**

0 Começando **1**

0.E Chapter 0 exercises 20

I Conceitos centrais 23

Apêndice **27**

A Miscelânea matemática **27**

A.1 Definir fundamentos teóricos 28

A.2 Construções dos conjuntos de números 29

A.3 Limites de funções 47

B Dicas para exercícios selecionados **51**

Indices **55**

Índice de tópicos **55**

Índice de vocabulário **55**

Índice de notação **57**

Índices de comandos LaTeX **57**

Licence **61**

Prefácio

Olá, e obrigado por tirar tempo pra ler essa rápida introdução à *Uma Descida Infinita em Pura Matemática*! A versão mais recente do livro, em inglês, está gratuitamente disponível para download no seguinte site:

https://infinitedescent.xyz

O site também inclui informações sobre mudanças entre diferentes versões do livro, um arquivo de versões prévias, e alguns recursos para usar LaTeX (veja também **??**).

Sobre o livro

Um estudante em uma típica classe de cálculo vai aprender sobre a "regra da cadeia" e posteriormente a como usa-lá para resolver alguns problemas pré-escritos de "regra da cadeia" assim como calcular a derivada de $\sin(1+x^2)$ com respeito a x, ou talvez resolver um problema de palavras envolvendo taxas de variação relacionadas a mudança. A expectativa é que o estudante aplique corretamente a regra da cadeia para derivar a resposta correta, e mostrar trabalho suficiente para ser crível . Nesse sentido, o estudante é um *consumidor* da matemática. Eles recebem a regra da cadeia como uma ferramenta, a ser aceita sem questionamento, para então resolver um grupo pequeno de problemas.

O objetivo desse livro é ajudar o leitor a fazer a transição: de um *consumidor* da matemática para um *produtor* dela. É isso que significa 'pura' matemática. Enquanto um consumidor da matemática pode aprender a regra da cadeia e usa-la para calcular uma derivada, um produtor da matemática pode derivar a regra da cadeia a partir de uma rigorosa definição de uma derivada, e então provar mais versões abstratas da regra da cadeia em contextos mais gerais (como análise multivariável).

Dos consumidores da matemática é esperado que digam como usaram suas ferramentas para encontrar suas respostas. Produtores da matemática, por outro lado, tem muito mais a fazer: Eles precisam estar prontos para acompanhar as definições e hipóteses, juntar os dados em novas e interessantes formas, e fazer suas próprias definições de conceitos matemáticos. Ainda mais, uma vez que eles fizeram isso, eles devem comunicar suas descobertas de uma forma que outros considerem inteligível, e eles precisam convencer outros que aquilo que eles fizeram está correto, apropriado e que vale a pena.

É essa a transição do consumo para produção de matemática que guiou os princípios usados para planejar e escrever esse livro. Em particular:

- **Comunicação.** Acima de tudo, este livro visa ajudar o leitor a obter alfabetização matemática e se expressar matematicamente. Isso ocorre em muitos níveis de ampliação. Por exemplo, considere a seguinte expressão:

  $$\forall x \in \mathbb{R}, [\neg(x = 0) \Rightarrow (\exists y \in \mathbb{R}, y^2 < x^2)]$$

  Depois de trabalhar com esse livro, você será capaz de dizer o que os símbolos $\forall$, $\in$, $\mathbb{R}$, $\neg$, $\Rightarrow$ e $\exists$ significam intuitivamente e como eles são definidos precisamente. Mas você terá também que saber interpretar o que a expressão significa como um todo, explicar o que significa em termos simples para que outra pessoa entenda *sem* usar símbolos confusos, provar que aquilo é verdade, e comunicar sua prova para outra pessoa de uma forma clara e concisa.

  Os tipos de ferramentas necessárias para fazer isso estão desenvolvidas nos capítulos principais do livro, e mais foco é dado para o lado escrito das coisas em **??**.

- **Inquérito.** As pessoas aprendem mais quando elas descobrem as coisas por elas mesmas. Usando esse principio ao extremo o livro estaria em branco. No entanto, eu acredito que é importante incorporar aspectos da aprendizagem baseada em investigação no texto.

  Este principio manifesta-se na medida que existem exercícios espalhados pelo texto, muitos dos quais simplesmente requerem que você prove um resultado. Muitos leitores vão achar isso frustrante, mas isso é por um bom motivo: esses exercícios servem como pontos de controle para garantir que seu entendimento desse material é suficiente para proceder. Aquele sentimento de frustração é o que se chamaria de aprendizado — abrace-o!

- **Estrategia.** Uma prova matemática é muito parecida com um quebra-cabeça. Em qualquer fase dada em uma prova, você vai ter algumas definições, premissas e resultados que estão disponíveis para ser usados, e você precisa junta-los usando as regras lógicas à sua disposição. Por todo livro, e particularmente nos primeiros capítulos, eu fiz um esforço para destacar estratégias úteis de prova em qualquer lugar que elas surjam.

- **Conteúdo.** Não há muito sentido em aprender matemática se você não tem nenhum conceito para prova. Com isso em mente, **??** inclui vários capítulos dedicados à introdução de algumas áreas temáticas em matemática pura, tanto quanto teoria dos números, combinatórias, análise e teoria da probabilidade.

- **LaTeX.** O *de facto* padrão para composição matemática é o LaTeX. Eu acho que é importante para matemáticos aprender sobre ele cedo de uma forma guiada, então eu escrevi um breve tutorial no **??** e inclui código LaTeX para toda nova notação conforme definida ao longo do livro.

Navegando o livro

Esse livro não precisa, e enfaticamente *não deve*, ser lido de frente para trás. A ordem desse material foi escolhida de forma que o material que aparece depois depende apenas do material que aparece antes, mas seguir o material na ordem que é apresentado pode ser uma experiência bastante seca.

A maioria do cursos introdutórios de matemática pura abrange, no mínimo, lógica simbólica, conjuntos, funções e relações. Este material é o conteúdo do Part I. Tais cursos frequentemente abrangem tópicos adicionais da matemática pura, com exatamente *quais* tópicos dependendo do que o curso está preparando os estudantes. Com isso em mente, **??** serve como uma introdução para uma gama de áreas de matemática pura, incluindo teoria dos números, combinatórias, teoria dos conjuntos, análise real, teoria das probabilidade e teoria da ordem.

Não é necessário cobrir toda a Part I antes de seguir os tópicos na **??**. Na verdade, intercalar material da **??** pode ser uma maneira útil de motivar muitos dos conceitos abstratos que surgem na Part I.

A seguinte tabela mostra dependências entre seções. Seções prévias dentro do mesmo capítulo que uma seção deveria ser considerado 'essencial' pré-requisitos, a menos que indicado de outra forma.

Parte	Seção	Essencial	Recomendado	útil
I	??	0		
	??	??		
	??	??		
	??	??	??	??
	??	??	??	??, ??
	??	??, ??	??	
??	??	??	??, ??	??
	??		??	
	??	??		
	??	??, ??		??
	??	??	??	
	??	??	??	??, ??
	??	??		
	??	??		
	??	??	??, ??	
	??	??		
	??	??, ??	??	??

Pré-requisitos são cumulativos. Por exemplo, a fim de cobrir **??**, você deveria primeiro cobrir 0–**??** e **????????**.

O que os números, cores e símbolos significam

Falando amplamente, o material nesse livro está fragmentado em itens enumerados que em em uma de cinco categorias: definições, resultados, observações, exemplos e exercícios. Na **??**, nós também temos extratos de provas. Para melhorar navegabilidade, essas categorias são distintas por nome, cor e símbolo, como indicado na seguinte tabela.

Categoria	Símbolo	Cor
Definições	✦	Vermelho
Resultados	✣	Azul
Observações	❖	Roxo

Categoria	Símbolo	Cor
Exemplos	✐	Verde
Exercícios	✎	Dourado
Extratos de provas	❝	Verde

Estes itens estão enumerados de acordo com próprias seções —por exemplo, **??** é em **??**. Definições e teoremas (Resultados importantes) aparecem em uma caixa.

Você também vai encontrar os símbolos □ e ◁ cujos significados são os seguintes:

□ **Fim de uma prova.** É um padrão em documentos matemáticos para identificar quando uma prova acabou por desenhar um pequeno quadrado ou por escrever '*Q.E.D.*' (Este último significa *quod erat demonstrandum*, que é latin para *que deveria ser mostrado*.)

◁ **Fim do item.** Isso *não é* um uso padrão, e está incluído apenas para ajudá-lo a identificar quando um item foi concluído e o conteúdo principal do livro continua.

Algumas subjeções são rotuladas com o símbolo $\star$. Isso indica que o material dessa subseção pode ser ignorada sem consequências drásticas.

Licença

Comentários e correções

Qualquer feedback, seja de alunos, professores assistentes, instrutores ou quaisquer outros leitores, será muito apreciado. Particularmente úteis são correções de erros tipográficos, sugestões de formas alternativas de descrever conceitos ou provar teoremas e solicitações de novos conteúdos. (e.g. se você conhecer um bom exemplo que possa ilustrar um conceito,ou se tiver um conceito relevante que você desejaria ver nesse livro).

Tal feedback pode ser mandado para o autor e adaptador por email (clive@infinitedescent.xyz e jonas.agx@gmail.com, respectivamente).

xii

Reconhecimentos

Quando reflito sobre o tempo que passei escrevendo este livro, fico impressionado com o número de pessoas que tiveram algum tipo de influência em seu conteúdo.

Este livro nunca teria existido se não fosse pelo curso 38-801 de Chad Hershock*Ensinos Baseados em Evidências ciêntificas*,No qual fiz no outono de 2014 como estudante de pós-graduação na Carnegie Mellon University. Seu curso influenciou fortemente minha abordagem de ensino e, em primeiro lugar, motivou-me a escrever este livro. Muitas das decisões pedagógicas que tomei ao escrever este livro foram informadas por pesquisas às quais fui exposto quando era aluno da turma de Chad.

O lendário professor da Carnegie Mellon, John Mackey, tem usado este livro (em vários formatos) como notas de curso para 21-128 *Conceitos Matemáticos e Provas* e 15-151 *Fudamentos Matemáticos da Ciência da Computação* Desde o outono de 2016. Sua influência pode ser sentida ao longo de todo o livro: graças às discussões com John, muitas provas foram reformuladas, seções reestruturadas e explicações melhoradas. Como resultado, há alguma sobreposição entre os exercícios deste livro e as questões nas folhas de problemas. Estou extremamente grato por seu apoio contínuo.

Steve Awodey, que foi meu orientador de tese de doutorado, tem sido uma fonte de inspiração para mim há muito tempo. Muitas das escolhas que fiz ao escolher como apresentar o material deste livro baseiam-se no meu desejo de fazer matemática. *O caminho certo*—foi esse desejo que me levou a estudar a teoria das categorias e, por fim, a me tornar aluno de doutorado de Steve. Aprendi muito com ele e apreciei muito sua paciência e flexibilidade em ajudar a direcionar minha pesquisa, apesar de minha agenda lotada de ensino e de meus interesses extracurriculares (como escrever este livro).

Talvez sem o conhecimento deles, muitas conversas esclarecedoras com as seguintes pessoas ajudaram a moldar o material deste livro de uma forma ou de outra: Jeremy Avigad, Deb Brandon, Santiago Cañez, Heather Dwyer, Thomas Forster, Will Gunther, Kate Hamilton, Jessica Harrell, Bob Harper, Brian Kell, Marsha Lovett, Ben Millwood,

David Offner, Ruth Poproski, Emily Riehl, Hilary Schuldt, Gareth Taylor, Katie Walsh, Emily Weiss e Andy Zucker.

Uma rede *Stack Exchange* influenciou o desenvolvimento deste livro de duas maneiras importantes. Primeiro, sou um membro ativo do *Mathematics Stack Exchange* (https://math.stackexchange.com/) desde o início de 2012 e aprendi muito sobre como explicar conceitos matemáticos de maneira eficaz; ocasionalmente, uma pergunta sobre Mathematics Stack Exchange me inspira a adicionar um novo exemplo ou exercício ao livro. Em segundo lugar, tenho feito uso frequente do *LaTeX Stack Exchange* (https://tex.stackexchange.com) para implementar alguns dos aspectos mais técnicos de escrever um livro usando o LaTeX .

O Departamento de Ciências Matemáticas da Carnegie Mellon University apoiou-me academicamente, profissionalmente e financeiramente ao longo do meu doutoramento e me apresentou mais oportunidades do que eu poderia esperar para me desenvolver como professor. Este apoio é agora continuado pelo Departamento de Matemática da Northwestern University, onde trabalho atualmente como professor.

Gostaria também de agradecer a todos nos centros de ensino da Carnegie Mellon e da Northwestern, no Eberly Center e no Searle Center, respectivamente. Através de vários workshops, programas e bolsas em ambos os centros de ensino, aprendi muito sobre como as pessoas aprendem e transformei-me como professor. Sua abordagem da ciência do ensino e da aprendizagem, centrada no aluno e baseada em evidências, está subjacente a tudo o que faço como professor, inclusive ao escrever este livro — sua influência não pode ser subestimada.

Finalmente, e mais importante, sou grato aos mais de 1.000 alunos que já usaram este livro para aprender matemática. Cada vez que um aluno entra em contato comigo para tirar uma dúvida ou apontar um erro, o livro fica melhor; isso se reflete nas dezenas de erros tipográficos que foram corrigidos como consequência.

Clive Newstead
Janeiro de 2020
Evanston, Illinois

Chapter 0

Começando

Antes de podermos começar a provar coisas, precisamos eliminar certos tipos de afirmações que poderíamos tentar provar. Considere a seguinte afirmação:

Essa sentença é falsa.

Isso e verdadeiro ou falso? Se você pensar sobre isso por alguns segundos, você ficará em apuros.

Agora considere a seguinte sentença :

O burro mais feliz do mundo.

Isso e verdadeiro ou falso? Bem, não é nem uma frase; não faz sentido nem *perguntar* se é verdadeiro ou falso!

É claro que estaremos desperdiçando nosso tempo tentando escrever provas de afirmações como as duas listadas acima – precisamos restringir nosso escopo a afirmações que possamos realmente ter uma chance de provar (ou talvez refutar)! Isso motiva a seguinte definição (informal).

✦ **Definition 0.0.1**
Uma **proposição** é a declaração na qual é possível atribuir a **Valor verdadeiro** (‘verdadeiro’ ou ‘falso’). Se uma proposição é verdadeira, uma **prova** da preposição é um argumento logicamente válido que demonstra que é verdadeiro, apresentado a um nível tal que um membro do público-alvo possa verificar a sua veracidade.

Assim, as afirmações dadas acima são proposições porque não há forma possível de lhes atribuir um valor de verdade. Observe que, em Definition 0.0.1, tudo o que importa é que *faz sentido* dizer que é verdadeiro ou falso, independentemente de realmente *ser* verdadeiro ou falso — o valor de verdade de muitas proposições é desconhecida, mesmo as muito simples.

✎ **Exercise 0.0.2**
Pense em um exemplo de proposição verdadeira, de proposição falsa, de proposição cujo valor de verdade você não conhece e de uma afirmação que não é uma proposição.

◁

Os resultados em artigos e livros didáticos de matemática podem ser chamados de *proposições*, mas também podem ser chamados de *teoremas*, *lemas* ou *corolários* dependendo do uso pretendido.

- Uma **proposição** é um termo abrangente que pode ser usado para qualquer resultado.
- Um **teorema** é um resultado chave que é particularmente importante.
- Um **lema** é um resultado que é provado com o propósito de ser usado na prova de um teorema.
- Um **corolário** é um resultado que segue de um teorema sem muito esforço adicional.

Estas não são definições precisas e não pretendem ser — você poderia chamar cada resultado de *proposição* se quisesse — mas usar essas palavras apropriadamente ajuda os leitores a descobrir como ler um artigo. Por exemplo, se você quiser apenas folhear um artigo e encontrar seus principais resultados, procure resultados rotulados como *teoremas*.

Não adianta muito tentar provar resultados se não temos nada para provar os resultados. Com isso em mente, apresentaremos agora os *conjuntos de números* e provaremos alguns resultados sobre eles no contexto de quatro tópicos, a saber: divisão de inteiros, bases numéricas, números racionais e irracionais e polinômios. Estes tópicos fornecerão contexto para o material em Part I, e servirão como uma introdução aos tópicos abordados em **??**.

Não nos aprofundaremos muito neste capítulo. Em vez disso, pense nisso como um exercício de aquecimento – uma introdução rápida e leve, com mais provas a serem fornecidas no restante do livro.

Conjuntos

Fundamental para a matemática é a noção de *conjunto*. Estudaremos conjuntos detalhadamente em **??**, mas você os encontrará em todos os capítulos do livro, então levaremos algum tempo para pensar sobre eles agora. Não trataremos conjuntos formalmente neste estágio – por enquanto, a definição a seguir será o suficiente.

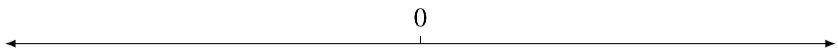
✦ **Definition 0.0.3** (a ser revisado em **??**)
Um **conjunto** é uma coleção de objetos. Os objetos nesse conjunto são chamados **elementos** do conjunto. Se X é um conjunto e x é um objeto, então escrevemos $x \in X$ (LaTeX code: `x \ in X`) para denotar a afirmação que x é um elemento de X.

Os conjuntos que nos interessam em primeiro lugar são os *conjuntos de números*—isto é, conjuntos cujos elementos são tipos particulares de *número*. Neste nível introdutório, muitos detalhes serão temporariamente varridos para debaixo do tapete; trabalharemos com um nível de precisão apropriado ao nosso estágio atual, mas que ainda nos permita desenvolver uma quantidade razoável de intuição.

Então aqui vamos nós. Aqui está uma linha infinita:

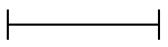
As setas indicam que se supõe que se estenda em ambas as direções sem fim. Os pontos na linha representarão números (especificamente, *números reais*, um termo enganoso que será definido em Definition 0.0.25).

Agora vamos fixar um ponto nesta linha e rotulá-lo ‘0’:



Este ponto pode ser considerado como uma representação do número zero; é o ponto contra o qual todos os outros números serão medidos. Os números à esquerda de 0 na reta numérica são considerados *negativos*, e os à direita são *positivos*; 0 em si não é positivo nem negativo.

Finalmente, vamos fixar uma unidade de comprimento:



Esta unidade de comprimento será utilizada, entre outras coisas, para comparar até que ponto os outros números diferem de zero.

Definition 0.0.4
Uma linha infinita acima, junto com seu ponto zero fixo e comprimento unitário fixo, constituem a (**real**)**linha numérica**.

Usaremos a reta numérica para construir cinco conjuntos de números de nosso interesse: o conjunto $\mathbb{N}$ de *números naturais* (Definition 0.0.5), o conjunto $\mathbb{Z}$ de *inteiros* (Definition 0.0.11), o conjunto $\mathbb{Q}$ de *números racionais* (Definition 0.0.24), o $\mathbb{R}$ de *números reais* (Definition 0.0.25), e

Cada um desses conjuntos tem um caráter diferente e é usado para propósitos diferentes, como veremos mais adiante neste capítulo e ao longo deste livro.

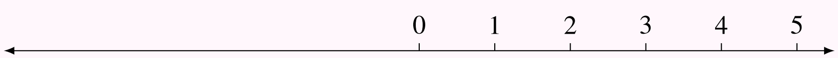
Números Naturais ($\mathbb{N}$)

Os *números naturais* são os números usados para contar—são as respostas a questões da forma ‘quantos’—por exemplo, tenho *três* tios, *três* guinéus porcos e *zero* gatos.

Contar é uma habilidade que os humanos possuem há muito tempo; sabemos disso porque há evidências de pessoas que usaram marcadores há dezenas de milhares de anos. As marcas de contagem fornecem um método de contar números pequenos: começando do zero, prossiga pelos objetos que deseja contar um por um e faça uma marca para cada objeto. Quando terminar, haverá tantas marcas quantos objetos. Somos ensinados desde pequenos a contar com os dedos; este é outro exemplo de fazer marcas de registro, onde agora, em vez de fazer uma marca, levantamos um dedo.

Fazer uma marca representa um *incremento* na quantidade — isto é, adicionar um. Na nossa reta numérica, podemos representar um incremento na quantidade movendo para a direita pela unidade de comprimento. Então, a distância do zero que nos movemos, que é igual ao número de vezes que nos movemos para a direita pela unidade de comprimento, é portanto, igual ao número de objetos que estão sendo contados.

Definition 0.0.5
Os **números naturais** são representados pelos pontos na reta numérica que podem ser obtidos começando em 0 e movendo-se para a direita pela unidade de comprimento qualquer número de vezes:



Em termos mais familiares, eles são *os números inteiros não negativos*. Nós escrevemos $\mathbb{N}$ (LaTeX code: `\mathbb{N}`) para o conjunto de todos os números naturais; assim, a notação ‘$n \in \mathbb{N}$’ significa que n é um número natural.

Os números naturais possuem uma estrutura matemática muito importante e interessante, e são centrais no material em **??**. Uma caracterização mais precisa dos números naturais será fornecida em **??**, e uma construção matemática do conjunto de números naturais pode ser encontrada em Section A.1 (ver Construction A.2.5). No centro destas caracterizações mais precisas estarão as noções de "zero" e de "adicionar um" – tal como fazer marcas de contagem.

Alguns autores definem os números naturais como sendo os números inteiros *positivos*, excluindo assim o zero. Consideramos 0 um número natural, pois nosso principal uso dos números naturais será para contar conjuntos finitos, e um conjunto sem nada é certamente finito! Dito isto, como acontece com qualquer definição matemática, a escolha sobre se $0 \in \mathbb{N}$ ou $0 \notin \mathbb{N}$ é uma questão de gosto ou conveniência, e é apenas uma convenção — não é algo que possa ser provado ou refutado.

Bases Numéricas

Escrever números é algo que pode parecer fácil para você agora, mas provavelmente levou vários anos quando criança para realmente entender o que estava acontecendo. Historicamente, existiram muitos sistemas diferentes para representar números simbolicamente, chamados *sistemas numéricos*. Primeiro veio o mais primitivo de todos, os marcadores de contagem, aparecendo na Idade da Pedra e ainda sendo usados para alguns propósitos hoje. Milhares de anos e centenas de sistemas de numeração depois, existe um sistema de numeração dominante, compreendido em todo o mundo: o **sistema de numeração hindu-árabe**. Este sistema de numeração consiste em dez símbolos, chamados *dígitos*. É um sistema numérico *posicional*, o que significa que a posição de um símbolo em uma cadeia determina seu valor numérico.

Em inglês, os *algarismos arábicos* são usados como os dez dígitos:

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9$$

O dígito mais à direita em uma cadeia está na casa das unidades e o valor de cada dígito aumenta por um fator de dez movendo-se para a esquerda. Por exemplo, quando escrevemos '2812', o '2' mais à esquerda representa o número dois mil, enquanto o último '2' representa o número dois.

O fato de existirem dez dígitos e de o sistema numérico ser baseado em potências de dez é um acidente biológico que corresponde ao fato de a maioria dos humanos ter dez dedos. Para muitos propósitos, isso é inconveniente. Por exemplo, dez não tem muitos divisores positivos (apenas quatro: 1, 2, 5 e 10) — isto tem implicações para a facilidade de realizar aritmética; um sistema baseado no número doze, que possui seis divisores positivos (1, 2, 3, 4, 6 e 12), pode ser mais conveniente. Outro exemplo é na computação e na eletrônica digital, onde é mais conveniente trabalhar em um sistema *binário*, com apenas dois dígitos —0 e 1—que representam ‘off’ e ‘on’ (ou «baixa tensão» e «alta tensão»), respetivamente; a aritmética pode então ser realizada diretamente usando sequências de *portas lógicas* em um circuito elétrico.

Portanto, vale a pena ter alguma compreensão dos sistemas numéricos posicionais baseados em números diferentes de dez. A abstração matemática que fazemos leva à definição de *expansão base-b*.

✦ **Definition 0.0.6**
Seja b um número natural maior que 1. A **base-b expansão** de um número natural n é a[a] cadeia $d_r d_{r-1} \dots d_0$ tal que:

(i) $n = d_r \cdot b^r + d_{r-1} \cdot b^{r-1} + \cdots + d_0 \cdot b^0$;

(ii) $0 \leqslant d_i < b$ para cada i; e

(iii) If $n > 0$ então $d_r \neq 0$—a base de expansão-b de zero é 0 em todas as bases b.

Certas bases numéricas têm nomes; por exemplo, as expansões base 2, 3, 8, 10 e 16 são chamadas respectivamente de *binário*, *ternário*, *octal*, *decimal* e *hexadecimal*.

[a]Essa frase é problemática, pois assume que todo número natural tem apenas uma base-b expansão. Na verdade, esse fato requer prova — veja **??**.

Antes de olharmos um exemplo de Definition 0.0.6 em ação, vamos examinar a definição, que é um pouco concisa à primeira vista.

- Condição (i) nos diz que os dígitos na cadeia nos dizem quantos de cada potência de b são somados para obter n. Por exemplo, quando $b = 10$, os dígitos da direita para a esquerda indicam as unidades, dezenas, centenas, milhares e assim por diante.
- Condição (ii) nos diz que os dígitos em uma expansão de base b devem ser menores que b — por exemplo, os dígitos de base 4 são 0, 1, 2 e 3. Se permitíssemos mais dígitos, então coisas bobas aconteceriam — por exemplo, se ‘X’ fosse um novo dígito de base 10 representando o número dez, então ‘X2’ e ‘102’ seriam cadeias diferentes, ambas representando o número cento e dois.
- Condição (iii) garante que a cadeia que representa um número positivo não tenha nenhum ‘0’ inicial — caso contrário, por exemplo, ‘01423’ e ‘1423’ seriam cadeias diferentes representando o mesmo número natural.

✐ **Example 0.0.7**
Considere o número 1023. Sua expansão decimal (base-10) é 1023, já que

$$1023 = 1 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$$

Sua expansão binária (base-2) é 1111111111, já que

$$1023 = 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Podemos expressar números na base 36 usando os dez dígitos usuais de 0 a 9 e as vinte e seis letras de A a Z; por exemplo, A representa 10, M representa 22 e Z representa 35. A expansão de base 36 de 1023 é SF, já que:

$$1023 = 28 \cdot 36^1 + 15 \cdot 36^0 = \mathrm{S} \cdot 36^1 + \mathrm{F} \cdot 36^0$$

◁

✎ **Exercise 0.0.8**

Encontre as expansões binária, ternária, octal, decimal, hexadecimal e de base 36 do número 21127, usando as letras A–F como dígitos adicionais para a expansão hexadecimal (representando os números 10–15, respectivamente) e as letras A–Z como dígitos adicionais para a expansão da base 36. ◁

Às vezes desejamos especificar um número natural em termos de sua expansão de base b; temos alguma notação para isso.

✦ **Notation 0.0.9**

Seja $b > 1$. Se os números $d_0, d_1, \dots, d_r$ são dígitos base-b (no sentido de Definition 0.0.6), então nós escrevemos:

$$d_r d_{r-1} \dots d_{0(b)} = d_r \cdot b^r + d_{r-1} \cdot b^{r-1} + \cdots + d_0 \cdot b^0$$

para o número natural cuja expansão de base b é $d_r d_{r-1} \dots d_0$. Se não houver subscrito (b) e uma base não for especificada explicitamente, a expansão será assumida como base-10.

✐ **Example 0.0.10**

Usando nossa nova notação,nós temos:

$$1023 = 1111111111_{(2)} = 1101220_{(3)} = 1777_{(8)} = 1023_{(10)} = 3\mathrm{FF}_{(16)} = \mathrm{SF}_{(36)}$$

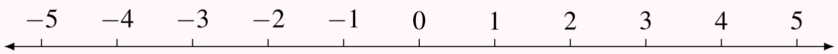
◁

Inteiros ($\mathbb{Z}$)

inteiros podem ser usados para medir a diferença entre dois números naturais. Por exemplo, suponha que eu tenha cinco maçãs e cinco bananas. Outra pessoa, também segurando maçãs e bananas, deseja negociar. Após a nossa troca, tenho sete maçãs e apenas uma banana. Assim, tenho mais duas maçãs e quatro bananas a menos.

Como um incremento na quantidade pode ser representado movendo-se para a direita na reta numérica pela unidade de comprimento, um *decremento* na quantidade pode, portanto, ser representado movendo-se para a *esquerda* pela unidade de comprimento. Fazer isso dá origem aos inteiros.

✦ **Definition 0.0.11**
Os **inteiros** são representados pelos pontos na reta numérica que podem ser obtidos começando em 0 e movendo-se em qualquer direção pela unidade de comprimento qualquer número de vezes:



Nós escrevemos $\mathbb{Z}$ (LaTeX code: `\mathbb{Z}`) para o conjunto de todos os inteiros; portanto,a notação '$n \in \mathbb{Z}$' significa que n é um inteiro.

Os inteiros têm uma estrutura tão fascinante que um capítulo inteiro deste livro é dedicado a eles — veja **??**. Isso tem a ver com o fato de que, embora seja possível somar, subtrair e multiplicar dois números inteiros e obter outro número inteiro, o mesmo não acontece com a divisão. Este "mau comportamento" da divisão é o que torna os números inteiros interessantes. Veremos agora alguns resultados básicos sobre divisão.

Divisão de Inteiros

A motivação que daremos em breve para a definição dos números racionais (Definition 0.0.24) é que o resultado da divisão de um inteiro por outro inteiro não é necessariamente outro inteiro. Contudo, o resultado é *às vezes* outro número inteiro; por exemplo, posso dividir seis maçãs entre três pessoas e cada pessoa receberá um número inteiro de maçãs. Isto torna a divisão interessante: como podemos medir o fracasso da divisibilidade de um número inteiro por outro? Como podemos deduzir quando um número inteiro é divisível por outro? Qual é a estrutura do conjunto de inteiros quando visto pelas lentes da divisão? Isso motiva Definition 0.0.12.

✦ **Definition 0.0.12** (Para ser repetido in **??**)
Seja $a, b \in \mathbb{Z}$. Dizemos b **divide** a se $a = qb$ para algum inteiro q. Existem muitas outras maneiras de dizer que b divide a, como: a é *divisível por* b, b é um *divisor* de a, b é um *fator* de a, ou a é um *múltiplo* de b.

Observe que, talvez de forma contraintuitiva, a definição de divisibilidade não envolve a operação aritmética de divisão: ela é definida em termos de multiplicação.

Example 0.0.13

O inteiro 12 é divisível por 1, 2, 3, 4, 6 e 12, desde que

$$12 = 12 \cdot 1 = 6 \cdot 2 = 4 \cdot 3 = 3 \cdot 4 = 2 \cdot 6 = 1 \cdot 12$$

Também é divisível pelos negativos de todos esses números; por exemplo, 12 é divisível por -3 desde que $12 = (-4) \cdot (-3)$. ◁

Exercise 0.0.14

Prove que 1 divide todo número inteiro e que todo número inteiro divide 0. ◁

Uma consequência de Exercise 0.0.14 é que 0 é divisível por 0. Isto é surpreendente: durante toda a nossa vida ouvimos que não podemos dividir por zero, mas agora descobrimos que podemos dividir zero por zero como pode ser isso? Isso destaca por que era tão importante que a definição de divisibilidade (Definition 0.0.12) fosse dada em termos de multiplicação, sem usar a operação de divisão: dizer que 0 divide 0 significa simplesmente que 0 pode ser multiplicado por um inteiro para obter 0 (o que é verdade)—mas isso não implica que a expressão '$\frac{0}{0}$' possa (ou deva) ser definida de forma significativa.

usando Definition 0.0.12, podemos provar alguns fatos básicos gerais sobre a divisibilidade.

Proposition 0.0.15

Seja $a, b, c \in \mathbb{Z}$. Se c divide b e b divide a, então c divide a.

Proof

Suponha que c divide b e b divide a. Por Definition 0.0.12, segue que

$$b = qc \quad \text{e} \quad a = rb$$

para alguns inteiros q e r. Usando a primeira equação, podemos substituir qc por b na segunda equação, para obter

$$a = r(qc)$$

Mas $r(qc) = (rq)c$, e rq é um número inteiro, então segue de Definition 0.0.12 que c divide a. □

Exercise 0.0.16

Sejam $a, b, d \in \mathbb{Z}$. Suponha que d divide a e d divide b. Dados inteiros u e v, prove que d divide $au + bv$. ◁

Alguns conceitos familiares, como par e impar, podem ser caracterizados em termos de divisibilidade.

Definition 0.0.17

Um inteiro n é **par** se é divisível por 2; de outra forma, n é **impar**.

Não é apenas interessante saber quando um inteiro *divide* outro; entretanto, provar que um inteiro *não* divide outro é muito mais difícil. Na verdade, para provar que um inteiro b não divide um inteiro a, devemos provar que $a \neq qb$ para *qualquer* inteiro q. Veremos métodos para fazer isso em **??**; esses métodos usam o seguinte resultado extremamente importante, que será a base de toda a **??**.

Theorem 0.0.18 (Teorema da divisão, para ser repetido in **??**)
Seja $a, b \in \mathbb{Z}$ com $b \neq 0$. Existe exatamente uma maneira de escrever

$$a = qb + r$$

de tal modo que q e r são inteiros, e $0 \leqslant r < b$ (se $b > 0$) ou $0 \leqslant r < -b$ (se $b < 0$).

O número q em Theorem 0.0.18 é chamado o **quociente** de a quando dividido por b, e o número r é chamado o **restante**.

Example 0.0.19
O número 12 deixa um restante de 2 quando dividido por 5, desde que $12 = 2 \cdot 5 + 2$. ◁

Aqui está um exemplo um pouco mais complicado.

Proposition 0.0.20
Suponha um número inteiro a deixa um resto de r quando dividido por um número inteiro b, e que $r > 0$. Então $-a$ deixa um resto de $b - r$ quando dividido por b.

Proof
Suponha que a deixa um resto de r quando dividido por b. Então

$$a = qb + r$$

Para algum número inteiro q. Um pouco de rendimento de álgebra

$$-a = -qb - r = -qb - r + (b - b) = -(q+1)b + (b - r)$$

Since $0 < r < b$, Nós temos $0 < b - r < b$. Por isso $-(q+1)$ é o quociente de $-a$ quando dividido por b, e $b - r$ é o restante. □

Exercise 0.0.21
Prove que se um inteiro a deixa um resto de r quando dividido por um inteiro b, então a deixa um resto de r quando dividido por $-b$. ◁

Terminaremos esta parte sobre divisão de inteiros conectando-a com o material em bases numéricas — podemos usar o teorema da divisão (Theorem 0.0.18) para encontrar a expansão de base b de um determinado número natural. É baseado na seguinte observação: o número natural n cuja expansão de base b é $d_r d_{r-1} \cdots d_1 d_0$ é igual a

$$d_0 + b(d_1 + b(d_2 + \cdots + b(d_{r-1} + bd_r) \cdots))$$

Além disso, $0 \leqslant d_i < b$ para todo i. Em particular, n deixa um resto de d_0 quando dividido por b. Por isso

$$\frac{n-d_0}{b} = d_1 + d_2 b + \cdots + d_r b^{r-1}$$

A base -b b expansão de $\frac{n-d_0}{b}$ é portanto

$$d_r d_{r-1} \cdots d_1$$

Em outras palavras, o resto de n quando dividido por b é o último dígito de base b de n, e então subtrair esse número de n e dividir o resultado por b trunca o final dígito. Repetir esse processo nos dá d_1, e depois d_2, e assim por diante, até chegarmos a 0. Isso sugere o seguinte algoritmo para calcular a expansão de base b de um número n:

- **Passo 1.** Seja d_0 seja o resto quando n é dividido por b, e Seja $n_0 = \frac{n-d_0}{b}$ seja o quociente. Conserte $i = 0$.
- **Step 2.** Suponha n_i e d_i foram definidos. Se $n_i = 0$, em seguida, prossiga para o Passo 3. Por outro lado define d_{i+1} o seja o resto quando n_i é dividido por b e defina $n_{i+1} = \frac{n_i - d_{i+1}}{b}$. Aumente i e repita a Etapa 2.
- **Etapa 3.** A expansão base-b de n é

$$d_i d_{i-1} \cdots d_0$$

Example 0.0.22

Calculamos a expansão de base 17 de 15213, usando as letras A–G para representar os números 10 até 16.

- $15213 = 894 \cdot 17 + 15$, então $d_0 = 15 = \mathrm{F}$ e $n_0 = 894$.
- $894 = 52 \cdot 17 + 10$, então $d_1 = 10 = \mathrm{A}$ e $n_1 = 52$.
- $52 = 3 \cdot 17 + 1$, então $d_2 = 1$ and $n_2 = 3$.
- $3 = 0 \cdot 17 + 3$, então $d_3 = 3$ e $n_3 = 0$.
- A base -17 expansão de 15213 é portanto 31AF.

Uma rápida verificação

$$31\mathrm{AF}_{(17)} = 3 \cdot 17^3 + 1 \cdot 17^2 + 10 \cdot 17 + 15 = 15213$$

como desejado. ◁

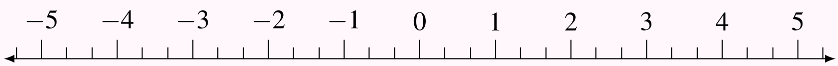
Exercise 0.0.23

Encontre a expansão de base 17 de 408 735 787 e a expansão de base 36 de 1 442 151 747. ◁

Números Racionais ($\mathbb{Q}$)

Cansado de comer maçã e banana, compro uma pizza dividida em oito fatias. Um amigo e eu decidimos dividir a pizza. Não tenho muito apetite, então como três fatias e meu amigo come cinco. Infelizmente, não podemos representar a proporção da pizza que cada um de nós comeu usando números naturais ou inteiros. Porém, não estamos muito longe: podemos contar o número de partes iguais em que a pizza foi dividida e, dessas partes, podemos contar quantas tivemos. Na reta numérica, isso poderia ser representado dividindo o segmento de reta unitária de 0 a 1 em oito partes iguais e procedendo a partir daí. Este tipo de procedimento dá origem aos *números racionais*.

✦ **Definition 0.0.24**
Os **números racionais** são representados pelos pontos na reta numérica que podem ser obtidos dividindo qualquer um dos segmentos da reta unitária entre inteiros em um número igual de partes.



Os números racionais são aqueles da forma $\frac{a}{b}$, onde $a,b \in \mathbb{Z}$ e $b \neq 0$. Escrevemos $\mathbb{Q}$ (LaTeX code: `\mathbb{Q}`) para o conjunto de todos os números racionais; portanto, a notação '$q \in \mathbb{Q}$' significa que q é um número racional.

Os números racionais são um exemplo muito importante de um tipo de estrutura algébrica conhecida como *campo* — eles são particularmente centrais para a teoria algébrica dos números e para a geometria algébrica.

Números reais ($\mathbb{R}$)

Quantidade e mudança podem ser medidas abstratamente usando *números reais*.

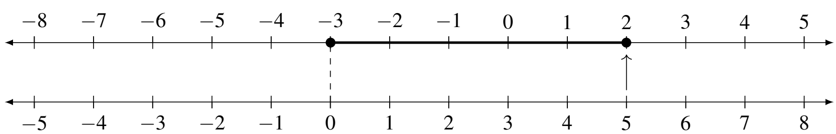
✦ **Definition 0.0.25**
Os **números reais** são os pontos na reta numérica. Escrevemos $\mathbb{R}$ (LaTeX code: `\mathbb{R}`) para o conjunto de todos os números reais; portanto, a notação '$a \in \mathbb{R}$' significa que a é um número real.

Os números reais são centrais para a análise real, um ramo da matemática introduzido em **??**. Eles transformam os racionais em um *continuum* ao 'preencher as lacunas'— especificamente, eles têm a propriedade de *completude*, o que significa que se uma quantidade pode ser aproximada com precisão arbitrária por números reais, então essa quantidade é em si um número real.

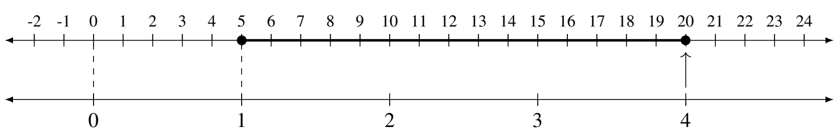
Podemos definir as operações aritméticas básicas (adição, subtração, multiplicação e divisão) sobre os números reais, e uma noção de ordenação dos números reais, em termos da reta numérica infinita.

- **Ordenando.** Um número real a é menor que um número real b, escrito $a < b$, se a estiver à esquerda de b na reta numérica. As convenções usuais para os símbolos $\leqslant$ (LaTeX code: `\le`), $>$ e $\geqslant$ (LaTeX code: `\ge`) se aplicam, por exemplo '$a \leqslant b$' significa que $a < b$ ou $a = b$.

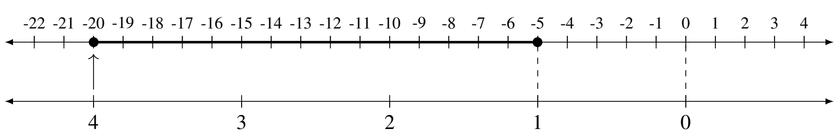
- **Adição.** Suponha que queremos adicionar um número real a a um número real b. Para fazer isso, *traduzimos* a em b unidades para a direita — se $b < 0$ então isso equivale a traduzir a em um número equivalente de unidades para a esquerda. Concretamente, faça duas cópias da reta numérica, uma acima da outra, com a mesma escolha de comprimento unitário; mova o 0 da reta numérica inferior abaixo do ponto a da reta numérica superior. Então $a+b$ é o ponto na reta numérica superior situado acima do ponto b da reta numérica inferior. $(-3)+5=2$:



- **Multiplicação.** Essa é divertida. Suponha-se que queiramos multiplicar um número real a por um número real b. Para fazer isso, escala-se a reta numérica e talvez ambas as partes se refletirão. Concretamente, façamos duas cópias da reta numérica, uma acima da outra; alinhe os pontos 0 em ambas as retas numéricas e estique a reta numérica inferior uniformemente até que o ponto 1 na reta numérica inferior esteja abaixo do ponto a na reta numérica superior — observe que se a < 0 então a reta numérica deve ser refletida para que isso aconteça. Então a·b é o ponto na reta numérica superior situado acima de b na reta numérica inferior. 5·4 = 20. $5 \cdot 4 = 20$.



  e aqui está uma ilustração do fato de que $(-5)\cdot 4 = -20$:



✎ **Exercise 0.0.26**
Interprete as operações de subtração e divisão como transformações geométricas da reta numérica real. ◁

Tomaremos como certas as propriedades aritméticas dos números reais neste capítulo, esperando até **??** para afundar nossos dentes nos detalhes. Por exemplo, tomaremos como certas as propriedades básicas dos números racionais, por exemplo

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Números Racionais e Irracionais

Antes de podermos falar sobre números irracionais, devemos dizer o que são.

✦ **Definition 0.0.27**
An **Número irracional**é um número que não é racional.

Ao contrário de $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, não existe uma única letra padrão que expresse os números irracionais. No entanto, até ao final de **??**, seremos capazes de escrever o conjunto de números irracionais como '$\mathbb{R} \setminus \mathbb{Q}$'.

Provar que um número real é *irracional* não é particularmente fácil, em geral. Colocaremos o pé na porta permitindo-nos assumir o seguinte resultado, que é reafirmado e provado em **??**.

✣ **Proposition 0.0.28**
O número real $\sqrt{2}$ é irracional. □

Podemos usar o fato de que $\sqrt{2}$ é irracional para provar alguns fatos sobre a relação entre números racionais e números irracionais.

✣ **Proposition 0.0.29**
Sejam a e b números irracionais. É possível que ab seja racional.

Proof
Seja $a = b = \sqrt{2}$. Então a e b são irracionais,e $ab = 2 = \frac{2}{1}$, o que é racional. □

✎ **Exercise 0.0.30**
Seja r um número racional e a um número irracional. Prove que é possível que ra seja racional, e é possível que ra seja irracional. ◁

Números Complexos ($\mathbb{C}$)

Vimos que a multiplicação por números reais corresponde ao escalar e reflexão da reta numérica – escalonamento sozinho quando o multiplicando é positivo, e escalando com reflexão quando é negativo. Poderíamos alternativamente interpretar esta reflexão como uma *rotação* de meia volta, uma vez que o efeito na reta numérica é o mesmo. Você pode então se perguntar o que acontece se girarmos em ângulos arbitrários, em vez de apenas meias voltas.

O que obtemos é um *plano* de números, não apenas uma linha — veja Figure 1. Além disso, acontece que as regras que esperamos que as operações aritméticas satisfaçam ainda são válidas – a adição corresponde à translação e a multiplicação corresponde à escala e à rotação. Este conjunto de números resultante é o dos *números complexos*.

✦ **Definition 0.0.31**
Os **números complexos** são aqueles obtidos pelos números reais não negativos após rotação de qualquer ângulo em torno do ponto 0. Escrevemos $\mathbb{C}$ (LaTeX code: `\mathbb{C}`) para o conjunto de todos os números complexos; portanto, a notação '$z \in \mathbb{C}$' significa que z é um número complexo.

Existe um número complexo particularmente importante, i, que é o ponto no plano complexo exatamente uma unidade acima de 0 — isso é ilustrado em Figure 1. A multiplicação por i tem o efeito de girar o plano um quarto de volta no sentido anti-horário. Em particular, temos $i^2 = i \cdot i = -1$; os números complexos têm a surpreendente propriedade de que existem raízes quadradas de *todos* os números complexos (incluindo todos os números reais).

Na verdade, todo número complexo pode ser escrito na forma $a+bi$, onde $a,b \in \mathbb{R}$; este número corresponde ao ponto no plano complexo obtido movendo a unidades para a direita e b unidades para cima, invertendo as direções como de costume se a ou b for negativo. A aritmética nos números complexos funciona da mesma forma que nos números reais; em particular, usando o fato de que $i^2 = -1$, obtemos

$$(a+bi)+(c+di) = (a+c)+(b+d)i \quad \text{e} \quad (a+bi)\cdot(c+di) = (ac-bd)+(anncio+bc)i$$

Discutiremos números complexos mais detalhadamente na parte deste capítulo sobre polinômios abaixo.

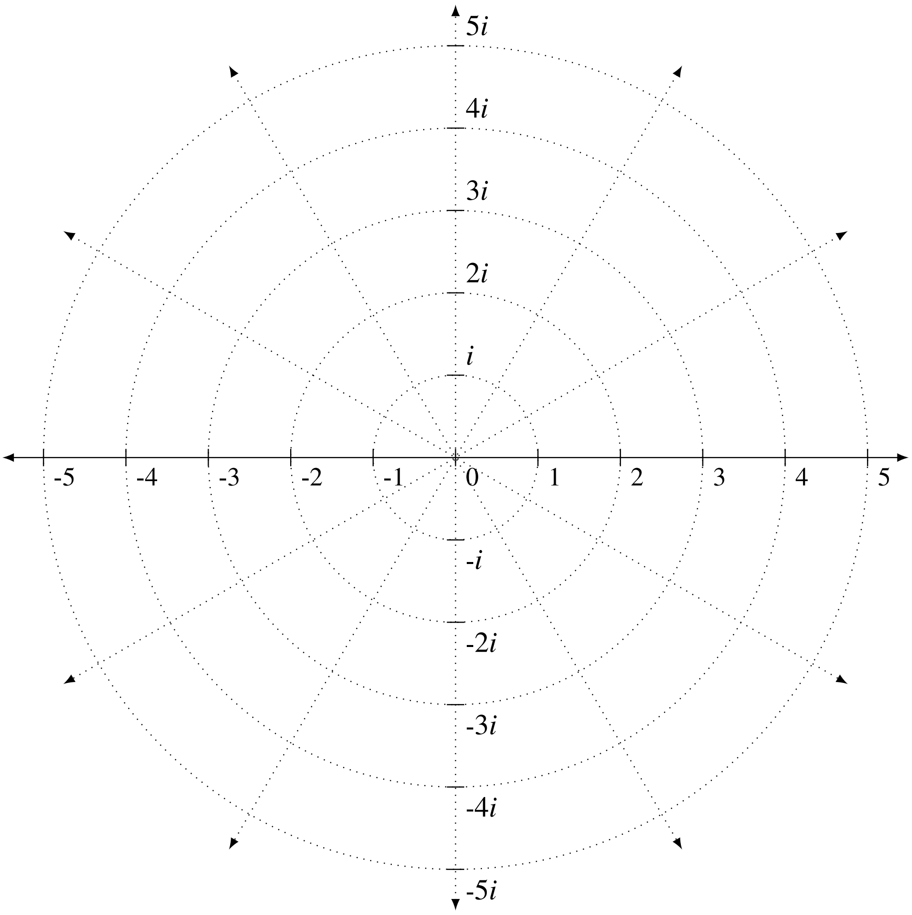


Figure 1: Ilustração do plano complexo, com alguns pontos rotulados.

Polinômios

Os números naturais, inteiros, números racionais, números reais e números complexos são todos exemplos de *semirings*, o que significa que eles vêm equipados com noções de adição e multiplicação bem comportadas.

✦ **Definition 0.0.32**
Seja $\mathbb{S} = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Um (**univariado**) **polinômio sobre** $\mathbb{S}$ no **indeterminado** x é uma expressão da forma

$$a_0 + a_1 x + \cdots + a_n x^n$$

onde $n \in \mathbb{N}$ e cada $a_k \in \mathbb{S}$. Os números a_k são chamados de **coeficientes** do polinômio. Se nem todos os coeficientes forem zero, o maior valor de k para o qual $a_k \neq 0$ é chamado de **grau** do polinômio. Por convenção, o grau do polinômio 0 é $-\infty$.

Polinômios de grau 1, 2, 3, 4 e 5 são respectivamente chamados *lineares*, *quadrático*, *cúbico*, *quártico* e *quíntico* polinomiais.

✐ **Example 0.0.33**
As seguintes expressões são todas polinômios:

$$3 \qquad 2x-1 \qquad (3+i)x^2 - x$$

Seus diplomas são 0, 1 e 2, respectivamente. Os dois primeiros são polinômios sobre $\mathbb{Z}$, e o terceiro é um polinômio sobre $\mathbb{C}$. ◁

✎ **Exercise 0.0.34**
Escreva um polinômio de grau 4 sobre $\mathbb{R}$ que não seja um polinômio sobre $\mathbb{Q}$. ◁

✦ **Notation 0.0.35**
Em vez de escrever os coeficientes de um polinômio todas as vezes, podemos escrever algo como $p(x)$ ou $q(x)$. O '(x)' indica que x é o indeterminado do polinômio. Se α for um número[a] e $p(x)$ é um polinômio em x indeterminado, escrevemos $p(\alpha)$ para o resultado de **substituir** α por x na expressão $p(x)$.

Note que, se A é qualquer um dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, e $p(x)$ é um polinômio sobre A, então $p(\alpha) \in A$ para toda $\alpha \in A$.

✐ **Example 0.0.36**
Seja $p(x) = x^3 - 3x^2 + 3x - 1$. então $p(x)$ é um polinômio sobre $\mathbb{Z}$ com indeterminado x. Para qualquer número inteiro α, o valor $p(\alpha)$ também será um número inteiro. Por

[a] Ao lidar com polinômios, normalmente reservaremos a letra x para a variável indeterminada e usaremos as letras gregas α, β, γ (LaTeX code: `\alpha, \beta, \gamma`) para números a serem substituídos em um polinômio.

exemplo

$$p(0) = 0^3 - 3 \cdot 0^2 + 3 \cdot 0 - 1 = -1 \quad \text{e} \quad p(3) = 3^3 - 3 \cdot 3^2 + 3 \cdot 3 - 1 = 8$$

◁

✦ **Definition 0.0.37**
Seja $p(x)$ m polinômio. Uma **raiz** de $p(x)$ é um número complexo α de tal modo que $p(\alpha) = 0$.

A *fórmula quadrática* (**??**) nos diz que as raízes do polinômio $x^2 + ax + b$, onde $a, b \in \mathbb{C}$, são precisamente o complexo números

$$\frac{-a + \sqrt{a^2 - 4b}}{2} \quad \text{e} \quad \frac{-a - \sqrt{a^2 - 4b}}{2}$$

Observe que evitamos o símbolo '±', que é comumente encontrado em discussões sobre polinômios quadráticos. O símbolo '±' é perigoso porque pode suprimir a palavra 'e' ou a palavra 'ou', dependendo do contexto — este tipo de ambigüidade não é algo com o qual desejaremos lidar ao discutir a lógica estrutura de uma proposição em **??**!

✐ **Example 0.0.38**
Seja $p(x) = x^2 - 2x + 5$. A fórmula quadrática nos diz que as raízes de p são

$$\frac{2 + \sqrt{4 - 4 \cdot 5}}{2} = 1 + \sqrt{-4} = 1 + 2i \quad \text{and} \quad \frac{2 - \sqrt{4 - 4 \cdot 5}}{2} = 1 - \sqrt{-4} = 1 - 2i$$

Os números $1 + 2i$ e $1 - 2i$ estão relacionados porque suas partes reais são iguais e suas partes imaginárias diferem apenas por um sinal. Exercise 0.0.39 generaliza esta observação. ◁

✎ **Exercise 0.0.39**
Seja $\alpha = a + bi$ um número complexo, onde $a, b \in \mathbb{R}$. Prove que α é a raiz de um polinômio quadrático sobre $\mathbb{R}$ e encontre a outra raiz desse polinômio. ◁

O exercício a seguir prova o conhecido resultado que classifica o número de raízes reais de um polinômio sobre $\mathbb{R}$ em termos de seus coeficientes.

✎ **Exercise 0.0.40**
Seja $a, b \in \mathbb{C}$ e seja $p(x) = x^2 + ax + b$. O valor $\Delta = a^2 - 4b$ é chamado de **discriminante** de p. Prove que p tem duas raízes se $\Delta \neq 0$ e uma raiz se $\Delta = 0$. Além disso, se $a, b \in \mathbb{R}$, prove que p não tem raízes reais se $\Delta < 0$, uma raiz real se $\Delta = 0$, e duas raízes reais se $\Delta > 0$. ◁

Example 0.0.41

Considere o polinômio $x^2 - 2x + 5$. Seu discriminante é igual a $(-2)^2 - 4 \cdot 5 = -16$, que é negativo. Exercise 0.0.40 nos diz que tem duas raízes, nenhuma das quais é real. Isto foi verificado por Example 0.0.38, onde descobrimos que as raízes de $x^2 - 2x + 5$ are $1 + 2i$ e $1 - 2i$.

Agora considere o polinômio $x^2 - 2x - 3$. Seu discriminante é igual a $(-2)^2 - 4 \cdot (-3) = 16$, o que é positivo. Exercise 0.0.40 nos diz que tem duas raízes, ambas reais; e realmente

$$x^2 - 2x - 3 = (x + 1)(x - 3)$$

então as raízes de $x^2 - 2x - 3$ são -1 e 3. ◁

Section 0.E

Chapter 0 exercises

0.1. O site de compartilhamento de vídeos *YouTube* atribui a cada vídeo um identificador único, que é uma cadeia de 11 caracteres do conjunto

$$\{\mathtt{A},\mathtt{B},\ldots,\mathtt{Z},\mathtt{a},\mathtt{b},\ldots,\mathtt{z},\mathtt{0},\mathtt{1},\mathtt{2},\mathtt{3},\mathtt{4},\mathtt{5},\mathtt{6},\mathtt{7},\mathtt{8},\mathtt{9},\mathtt{-},\mathtt{\_}\}$$

Esta cadeia é na verdade um número natural expresso em base 64, onde os caracteres no conjunto acima representam os números 0 a 63, na mesma ordem — portanto `C` representa 2, $mathttc$ representa 28, `3` representa 55 e `_` representa 63. De acordo com este esquema, encontre o número natural cuja expansão na base 64 é `dQw4w9WgXcQ`, e encontre a expansão na base 64 do número natural $7\,159\,047\,702\,620\,056\,984$.

0.2. Seja $a,b,c,d \in \mathbb{Z}$. Sob quais condições $(a+b\sqrt{2})(c+d\sqrt{2})$ é um número inteiro?

0.3. Suponha que um inteiro m deixe um resto de i quando dividido por 3, e um inteiro n deixe um resto de j quando dividido por 3, onde $0 \leqslant i,j < 3$. Prove que $m+n$ e $i+j$ deixam o mesmo resto quando divididos por 3.

0.4. Quais são os possíveis restos de n^2 quando dividido por 3, onde $n \in \mathbb{Z}$?

✦ **Definition 0.E.1**
set X é **closed** sob uma operação $\odot$ se, sempre que a e b são elementos de X, $a \odot b$ também é um elemento de X.

Em Questions 0.5 to 0.11, determine quais dos conjuntos de números $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são fechados em a operação $\odot$ definida na pergunta.

0.5. $a \odot b = a+b$

0.6. $a \odot b = a-b$

0.7. $a \odot b = (a-b)(a+b)$

0.8. $a \odot b = (a-1)(b-1)+2(a+b)$

0.9. $a \odot b = \dfrac{a}{b^2+1}$

0.10. $a \odot b = \dfrac{a}{\sqrt{b^2+1}}$

0.11. $a \odot b = \begin{cases} a^b & \text{if } b > 0 \\ 0 & \text{if } b \notin \mathbb{Q} \end{cases}$

✦ **Definition 0.E.2**
Um número complexo α é **algébrico** se $p(\alpha) = 0$ para algum polinômio diferente de zero $p(x)$ sobre $\mathbb{Q}$.

0.12. SeJA x seja um número racional. Prove que x é um número algébrico.

0.13. Prove que $\sqrt{2}$ é um número algébrico.

0.14. Prove que $\sqrt{2}+\sqrt{3}$ é um número algébrico.

0.15. Prove que $x+yi$ é um número algébrico, onde x e y são dois números racionais quaisquer.

Perguntas verdadeiras-falsas

Nas questões 1.16 a 1.23, determine (com prova) se a afirmação é verdadeira ou falsa

0.16. Todo número inteiro é um número natural.

0.17. Todo número inteiro é um número racional.

0.18. Todo número inteiro divide zero.

0.19. Todo número inteiro divide seu quadrado.

0.20. O quadrado de todo número racional é um número racional.

0.21. O quadrado de todo número racional é um número racional.

0.22. Quando um inteiro a é dividido por um inteiro positivo b, o resto é sempre menor que a.

0.23. Cada polinômio quadrático tem duas raízes complexas distintas.

Sempre - Às vezes - Nunca questiona

In Questions 0.24 to 0.32, determine (with proof) whether the conclusion is always, sometimes or never true under the given hypotheses.

0.24. Seja $n, b_1, b_2 \in \mathbb{N}$ com $1 < n < b_1 < b_2$. Então a expansão de base b_1 de n é igual à expansão de base b_2 de n.

0.25. Seja $n, b_1, b_2 \in \mathbb{N}$ com $1 < b_1 < b_2 < n$. Então a expansão de base b_1 de n é igual à expansão de base b_2 de n.

0.26. Seja $a, b, c \in \mathbb{Z}$ e suponha que a divida c e b divida c. Então ab divide c.

0.27. Seja $a, b, c \in \mathbb{Z}$ e suponha que a divida c e b divida c. Então ab divide c^2.

0.28. Seja $x, y \in \mathbb{Q}$ e seja $a, b, c, d \in \mathbb{Z}$ com $cy+d \neq 0$. Então $\dfrac{ax+b}{cy+d} \in \mathbb{Q}$.

0.29. Seja $\dfrac{a}{b}$ um número racional. Então $a \in \mathbb{Z}$ e $b \in \mathbb{Z}$.

0.30. Seja $x \in \mathbb{R}$ e assuma que $x^2 \in \mathbb{Q}$. Então $x \in \mathbb{Q}$.

0.31. Seja $x \in \mathbb{R}$ e assuma que $x^2 + 1 \in \mathbb{Q}$ e $x^5 + 1 \in \mathbb{Q}$. Então $x \in \mathbb{Q}$.

0.32. Seja $p(x) = ax^2 + bx + c$ um polinômio com $a, b, c \in \mathbb{R}$ e $a \neq 0$, e suponha que $u + vi$ seja uma raiz complexa de $p(x)$ com $v \neq 0$. Então $u - vi$ é uma raiz de $p(x)$.

Part I

Conceitos centrais

Apêndices

Appendix A

Miscelânea matemática

Houve diversas ocasiões no livro em que evitamos nos aprofundar muito nos aspectos mais técnicos ou obscuros de uma definição ou prova. Geralmente isso acontecia porque a exploração desses aspectos não era central para o tópico em questão, ou porque os detalhes envolvidos eram suficientemente confusos para que fornecer todos os detalhes ofuscasse as ideias principais em discussão.

Este apêndice fornece um espaço para os comentários que não fizemos, os teoremas que não provamos, os detalhes que não fornecemos e as obscuridades que não exploramos.

Começamos com uma rápida olhada nos *fundamentos da matemática* em Section A.1. Forneceremos os axiomas para a teoria dos conjuntos de Zermelo-Fraenkel (ZF), que codifica todos os objetos matemáticos como conjuntos e nos permite derivar todos os objetos matemáticos de uma coleção de axiomas. Também demonstraremos como codificar números naturais, inteiros, números racionais e números complexos dentro desta estrutura.

Section A.1

Definir fundamentos teóricos

Teoria ingênua dos conjuntos e o Paradoxo de Russel

Section A.2

Construções dos conjuntos de números

Na base da matemática mais comumente usada, a teoria dos conjuntos de Zermelo-Fraenkel com o axioma da escolha (discutido detalhadamente em Section A.1), todo objeto matemático é um conjunto. Isto levanta a questão: e os outros objetos matemáticos? Por exemplo, se os números são conjuntos, que conjuntos são eles? E quanto às funções e relações?

Para funções e relações, existe uma solução fácil: simplesmente as identificamos com seus gráficos. Por exemplo, podemos fingir que a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$ para todo $x \in \mathbb{R}$ ' é' o conjunto $\{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$.

Para números, entretanto, a resposta não é tão simples. Por exemplo, que conjunto deve ser o número 3? E faz diferença se considerarmos 3 um número natural ou um número real?

Esta seção apresenta uma das muitas maneiras possíveis de codificar números – isto é, números naturais, inteiros, números racionais, números reais e números complexos – como conjuntos.

Os Números Naturais

Podemos usar a estrutura fornecida pela teoria dos conjuntos de Zermelo-Fraenkel (Section A.1) para fornecer construções teóricas dos conjuntos de números $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Na verdade, se quisermos raciocinar sobre matemática dentro dos limites de ZF, devemos codificar tudo (incluindo números) como conjuntos!

Começaremos com uma construção teórica dos conjuntos dos números naturais — isto é, construiremos uma noção de números naturais no sentido de **??**. Codificaremos os números naturais como conjuntos, chamados *números naturais de von Neumann*. Identificaremos o número natural 0 com o conjunto vazio $\varnothing$, e identificaremos a operação sucessora s com uma operação envolvendo conjuntos.

✦ **Definition A.2.1**
Um **número natural de Von Neuman** ié qualquer conjunto que pode ser obtido de $\varnothing$ tomando repetidamente conjuntos sucessores (ver **??**). Escrito $0_{\mathsf{vN}} = \varnothing$ e $(n+1)_{\mathsf{vN}} = (n_{\mathsf{vN}})^+$; que é

$$0_{\mathsf{vN}} = \varnothing, \quad 1_{\mathsf{vN}} = \varnothing^{+}, \quad 2_{\mathsf{vN}} = \varnothing^{++}, \quad 3_{\mathsf{vN}} = \varnothing^{+++}, \quad 4_{\mathsf{vN}} = \varnothing^{++++}, \quad \ldots$$

Example A.2.2
Os três primeiros números naturais de von Neumann são:

- $0_{\mathsf{vN}} = \varnothing$;
- $1_{\mathsf{vN}} = \varnothing^+ = \varnothing \cup \{\varnothing\} = \{\varnothing\}$;
- $2_{\mathsf{vN}} = \varnothing^{++} = \{\varnothing\}^+ = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$.

◁

Exercise A.2.3
Escreva os elementos de 3_{vN} ($= \varnothing^{+++}$) e de 4_{vN}. ◁

Exercise A.2.4
Lembre-se da definição dos números naturais de von Neumann em Definition A.2.1. Prove que $|n_{\mathsf{vN}}| = n$ para todos $n \in \mathbb{N}$. ◁

Construction A.2.5
Construímos o conjunto $\mathbb{N}_{\mathsf{vN}}$ de todos os números naturais de von Neumann como segue. Seja X um conjunto arbitrário que satisfaça o axioma do infinito (**??**) e então defina $\mathbb{N}_{\mathsf{vN}}$ como a interseção de todos os subconjuntos de X que também satisfazem o axioma do infinito — isto é:

$$\mathbb{N}_{\mathsf{vN}} = \{x \in X \mid \forall U \in \mathscr{P}(X), [U \text{ satisfaz o axioma do infinito} \Rightarrow x \in U]\}$$

A existência de $\mathbb{N}_{\mathsf{vN}}$ segue dos axiomas do conjunto de potências (**??**) e separação (**??**).

Theorem A.2.6
O conjunto $\mathbb{N}_{\mathsf{vN}}$, elemento zero 0_{vN} e função sucessora $s : \mathbb{N}_{\mathsf{vN}}\ para \mathbb{N}_{\mathsf{vN}}$ definido por $\mathsf{s}(n_{\mathsf{vN}}) = n_{\mathsf{vN}}^+$ para todos $n_{\mathsf{vN}} \in \mathbb{N}_{\mathsf{vN}}$, defina uma noção de números naturais.

Proof
Devemos verificar os axiomas de Peano, que são condições (i)–(iii) de **??**.

Para provar (i), observe que para todos os conjuntos X temos $X^+ = X \cup \{X\}$, de modo que $X \in X^+$. Em particular, temos $n_{\mathsf{vN}} \in n_{\mathsf{vN}}^+$ para todos $n_{\mathsf{vN}} \in \mathbb{N}_{\mathsf{vN}}$ e, portanto, $n_{\mathsf{vN}}^+ \neq \varnothing = 0_{\mathsf{vN}}$.

Para (ii), seja $m_{\mathsf{vN}}, n_{\mathsf{vN}} \in \mathbb{N}_{\mathsf{vN}}$ e assuma que $m_{\mathsf{vN}}^+ = n_{\mathsf{vN}}^+$. Então $m_{\mathsf{vN}} = n_{\mathsf{vN}}$ por **??**.

Para (iii), seja X um conjunto e suponha que $0_{\mathsf{vN}} \in X$ e, para todo $n_{\mathsf{vN}} \in \mathbb{N}_{\mathsf{vN}}$, se $n_{\mathsf{vN}} X$, então $n_{\mathsf{vN}}^+ \in X$. Então X satisfaz o axioma do infinito (**??**), e então por Construction A.2.5 temos $\mathbb{N}_{\mathsf{vN}} \subseteq X$. □

À luz de Theorem A.2.6, podemos declarar que "os números naturais" são os números naturais de von Neumann, e pronto. Como tal, você pode - se quiser - pensar em todos os números naturais nessas notas como *sendo* seu número natural de von Neumann correspondente. Com isto em mente, omitimos agora o subscrito 'vN', deixando implícito o fato de que estamos nos referindo aos números naturais de von Neumann.

No entanto, existem muitas outras noções possíveis de números naturais. Em Theorem A.2.8, provamos que quaisquer duas noções de números naturais são essencialmente as mesmas e, portanto, as especificidades de como realmente definimos $\mathbb{N}$, o elemento zero e a operação sucessora, são irrelevantes para a maioria dos propósitos. .

Primeiro provaremos o seguinte lema útil, que fornece um meio conveniente de provar quando uma função é a função identidade (**??**).

Lemma A.2.7

Seja $(\mathbb{N}, z, s)$ seja uma noção de números naturais, e seja $j : \mathbb{N} \to \mathbb{N}$ uma função tal que $j(z) = 0$ e $j(s(n)) = s(j(n))$ para todo $n \in \mathbb{N}$. Então $j = \mathrm{id}_{\mathbb{N}}$.

Proof. Por **??**, existe uma função única $i : \mathbb{N} \to \mathbb{N}$ tal que $i(z) = 0$ e $i(s(n)) = s(i(n))$ para todo $n \in \mathbb{N}$. Mas então:

$j = i$ pela unicidade de i, já que j satisfaz as mesmas condições que i; e

$\mathrm{id}_{\mathbb{N}} = i$ pela exclusividade de i, já que $\mathrm{id}_{\mathbb{N}}(z) = z$ e $\mathrm{id}_{\mathbb{N}}(s(n)) = s(n) = s(\mathrm{id}_{\mathbb{N}}(n))$ para todos $n \in \mathbb{N}$. Portanto, $j = \mathrm{id}_{\mathbb{N}}$, conforme necessário. □

Theorem A.2.8

Quaisquer duas noções de números naturais são essencialmente iguais, num sentido muito forte. Mais precisamente, se $(\mathbb{N}_1, z_1, s_1)$ e $(\mathbb{N}_2, z_2, s_2)$ são noções de números naturais, então existe uma bijeção única $f : \mathbb{N}_1 \to \mathbb{N}_2$ tal que $f(z_1) = z_2$ e $f(s_1(n)) = s_2(f(n))$ para todo $n \in \mathbb{N}_1$.

Proof. Aplicando o teorema da recursão (**??**) para $(\mathbb{N}_1, z_1, s_1)$, com $X = \mathbb{N}_2$, $a = z_2$ e $h : \ mathbbN_1 \times \mathbb{N}_2 \to \mathbb{N}_2$ definido por $h(m,n) = s_2(n)$ para todos $m \in \mathbb{N}_1$ e $n \in \mathbb{N}_2$, obtemos uma função $f : \mathbb{N}_1 \to \mathbb{N}_2$ tal que $f(z_1) = z_2$ e $f(s_1(n)) = s_2(f(n))$ para todo $n \in \mathbb{N}_1$. Isso também nos dá a unicidade de f, então resta apenas provar que f é uma bijeção.

Da mesma forma, aplicando **??** a $(\mathbb{N}_2, z_2, s_2)$, com $X = \mathbb{N}_1$, $a = z_1$ e $h : \mathbb{N}_2 \times \mathbb{N}_1 \to \mathbb{N}_1$ definido por $h(m,n) = s_1(n)$ para todos $m \in \mathbb{N}_2$ e $n \in \mathbb{N}_1$, obtemos uma função (única!) $g : \mathbb{N}_2 \to \mathbb{N}_1$ tal que $g(z_2) = z_1$ e $g(s_2(n)) = s_1(g(n))$ para todos $n \in \mathbb{N}_2$. □

But then g(f (z1)) = g(z2) = z1 and, for all n N1, we have

g(f (s1(n))) = g(s2(f (n))) = s2(g(f (n)))

e assim g ◦ f = idN1 pelo Lema A.2.7. Com isso resolvido, vamos agora simplesmente trabalhar com uma noção fixa de números naturais $(\mathbb{N}, z, s)$, e não nos preocupar muito com como ela é construída — se quiser, pegue $\mathbb{N} = \mathbb{N}_{\mathsf{vN}}$, $z = 0_{\mathsf{vN}} = \varnothing$ and $s(n) = n^+ = n \cup \{n\}$ para todo $n \in \mathbb{N}$.

As operações aritméticas que conhecemos e amamos — adição, multiplicação e exponenciação — são definidas usando recursão em **??**; assim como os fatoriais e os coeficientes binomiais.

Podemos definir noções mais familiares envolvendo números naturais. Por exemplo, podemos definir a relação $\leqslant$ em $\mathbb{N}$ definindo $m \leqslant n$ como significando $\exists k \in \mathbb{N}, m+k = n$. Uma abordagem alternativa seria definir '$m \leqslant n$' para $m, n \in \mathbb{N}$ por uma recursão iterada em m e n — especificamente:

- $0 \leqslant 0$ é verdade;
- For all $m \in \mathbb{N}$, $m+1 \leqslant 0$ é falso;
- For all $n \in \mathbb{N}$, $0 \leqslant n+1$ é verdade; e
- For all $m, n \in \mathbb{N}$, $m+1 \leqslant n+1$ é verdade se e somente se $m \leqslant n$ é verdade.

✎ **Exercise A.2.9**

Prove que a definição recursiva de $\leqslant$ é equivalente à definição de '$m \leqslant n$' como '$\exists k \in \mathbb{N}, m+k = n$'. ◁

Inteiros

Agora que construímos os números naturais, é hora de construir os inteiros. A intuição por trás da definição que estamos prestes a dar é que um número inteiro nos diz a diferença entre dois números naturais. Assim, '3 como um número inteiro' refere-se ao aumento de 3 de um número natural para outro (digamos 0 a 3, ou 7 a 10); e '-4 como um número inteiro' refere-se a uma diminuição de 4 de um número natural para outro (digamos 4 para 0, ou 10 para 6).

Uma primeira tentativa pode ser definir $\mathbb{Z}$ como $\mathbb{N} \times \mathbb{N}$ e interpretar $(a, b) \in \mathbb{N} \times \mathbb{N}$ para representar o inteiro $b - a$. Infelizmente, isso não funciona muito bem, pois, por exemplo, o número inteiro 3 seria representado como $(0, 3)$ e como $(7, 10)$—e, mais geralmente, como $(n, n+3)$ para todos $n \in \mathbb{N}$.

Então, em vez disso, declararemos dois pares (a, b), $(c, d) \in \mathbb{N} \times \mathbb{N}$ para representar o mesmo número inteiro sempre que $b-a=d-c$. Para tornar isso formal, algumas coisas precisam acontecer:

(1) Precisamos esclarecer o que queremos dizer com 'declarar dois pares para representar o mesmo número inteiro' — isso será feito definindo uma relação de equivalência em $\mathbb{N}\times\mathbb{N}$ e depois passando para o quociente (veja **??**).

(2) Não podemos usar subtração em nossa definição da relação de equivalência, ou em nossa prova de que *é* uma relação de equivalência, pois ainda não definimos uma noção de subtração para $\mathbb{N}$.

Fortunately for us, (2) is easy to resolve: we can state the equation $b-a=d-c$ for $m,n\in\mathbb{N}$ equivalently as $a+d=b+c$; this is the equation that we will use to define the equivalence relation on $\mathbb{N}\times\mathbb{N}$ in (1).

✣ Lemma A.2.10

A relação $\sim$ em $\mathbb{N}\times\mathbb{N}$, definida para $(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}$ por $(a,b)\sim(c,d)$ se e somente se $a+d=b+c$, é uma relação de equivalência.

Proof

- (**Reflexividade**) Seja $(a,b)\in\mathbb{N}\times\mathbb{N}$. Então $a+b=b+a$, para que $(a,b)\sim(a,b)$.

- (**Simetria**) Seja $(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}$e assumindo que $(a,b)\sim(c,d)$. Então $a+d=b+c$, e assim $c+b=d+a$, $(c,d)\sim(a,b)$.

- (**Transitividade**) Seja $(a,b),(c,d),(e,f)\in\mathbb{N}\times\mathbb{N}$ e assuma que $(a,b)\sim(c,d)$ e $(c,d)\sim(e,f)$. Então $a+d=b+c$ e $c+f=d+e$. Mas então

$$(a+f)+(c+d)=(a+d)+(c+f)=(b+c)+(d+e)=(b+e)+(c+d)$$

  então cancelando $c+d$ de ambos os lados dá $a+f=b+e$, então $(a,b)\sim(e,f)$, como requerido

  Devemos ter o cuidado de observar que não assumimos a existência de uma operação de subtração quando cancelamos $c+d$ de ambos os lados da equação: o fato de $u+w=v+w$ implica $u=v$ pois todo $u,v,w\in\mathbb{N}$ pode ser provado por indução em w usando apenas os axiomas de Peano. □

Agora que temos uma relação de equivalência em $\mathbb{N}\times\mathbb{N}$, podemos considerar $\mathbb{Z}$ como o conjunto resultante de classes de equivalência (ou seja, o quociente).

Construction A.2.11
O **Conjunto dos inteiros** é o conjunto $\mathbb{Z}$ definido por

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$$

onde $\sim$ é a relação de equivalência em $\mathbb{N} \times \mathbb{N}$ definida por

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

for all $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$.

Interpretamos o elemento $[(a,b)]_\sim \in \mathbb{Z}$ como o número inteiro $b-a$. Então por exemplo temos

$$3 = [(0,3)]_\sim = [(7,10)]_\sim \quad \text{e} \quad -4 = [(4,0)]_\sim = [(10,6)]_\sim$$

Algumas observações são agora necessárias.

A primeira observação é que podemos definir operações de adição e multiplicação em $\mathbb{Z}$ usando aquelas em $\mathbb{N}$. Formalmente, definimos:

$[(a,b)]_\sim + [(c,d)]_\sim = [(a+c,b+d)]_\sim$—o a intuição aqui é que para todo $a,b,c,d \in \mathbb{N}$ temos $(b-a)+(d-c) = (b+d)-(a+c)$.

$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ad+bc,ac+bd)]_\sim$— a intuição aqui é que para todo $a,b,c,d \in \mathbb{N}$ temos $(b-a)(d-c) = (ac+bd)-(ad+bc)$. Como as operações $+$ e $\cdot$ são definidas em termos de representantes de classes de equivalência, devemos (mas não iremos) verificar se essas operações estão bem definidas — por exemplo, precisamos verificar se $[(a,b)]_\sim = [(a',b')]_\sim$ e $[(c,d)]_\sim = [(c',d')]_\sim$, então $[(a+c,b+d)]_\sim = [(a'+c',b'+d')]_\sim$.

O que torna os números inteiros especiais é que também podemos negá-los, o que por sua vez nos permite subtraí-los. Com isso em mente, podemos definir operações de negação e subtração em $\mathbb{Z}$ da seguinte forma:

$-[(a,b)]_\sim = [(b,a)]_\sim$—a intuição aqui é que para todo $a,b \in \mathbb{N}$ temos $-(b-a) = a-b$.

$[(a,b)]_\sim - [(c,d)]_\sim = [(a+d,b+c)]_\sim$—o a intuição aqui é que para todo $a,b,c,d \in \mathbb{N}$ temos $(b-a)-(d-c) = (b+c)-(a+d)$. As operações de negação e subtração podem ser definidas uma em relação à outra: elas estão relacionadas pelas identidades

$$-[(a,b)]_\sim = [(0,0)]_\sim - [(a,b)]_\sim \quad \text{e} \quad [(a,b)]_\sim - [(c,d)]_\sim = [(a,b)]_\sim + (-[(c,d)]_\sim)$$

Novamente, devemos, mas não iremos, provar que as operações de negação e subtração estão bem definidas.

A segunda e talvez mais alarmante observação é que esta construção de $\mathbb{Z}$ significa que não temos $\mathbb{N} \subseteq \mathbb{Z}$: os elementos de $\mathbb{Z}$ são classes de equivalência de pares de números naturais, o que significa que o número natural '3' não é igual ao inteiro '3' (que é realmente igual a $[(0,3)]_\sim$). No entanto, consideraremos $\mathbb{N}$ como sendo um subconjunto de $\mathbb{Z}$ identificando cada número natural n com o elemento $[(0,n)]_\sim \in \mathbb{Z}$. O que justifica esta identificação é o seguinte exercício.

✎ **Exercise A.2.12**

Prove que cada elemento de $\mathbb{Z}$, conforme definido em Construction A.2.11, é igual a exatamente um dos seguintes: $[(0,0)]_\sim$, ou $[(0,n)]_\sim$ para alguns $n > 0$, ou $[(n,0)]_\sim$ para alguns $n > 0$. ◁

Exercise A.2.12 implica que a função de 'inclusão' $i : \mathbb{N} \to \mathbb{Z}$ definida por $i(n) = [(0,n)]_\sim$ para todo $n \in \mathbb{N}$ é injetivo. Quando $n \in \mathbb{N}$, normalmente escreveremos apenas 'n' para denotar o inteiro $i(n) = [(0,n)]_\sim$.

Observe que $i(m+n) = i(m) + i(n)$ e $i(mn) = i(m)i(n)$, então quando escrevemos algo como '$m+n$' para $m,n \in \mathbb{N}$, não importa se estamos primeiro adicionando m e n como números naturais e depois interpretando o resultado como um número inteiro, ou primeiro interpretando m e n como inteiros e depois adicionando o resultado usando a operação de adição para inteiros.

Observe também que a identificação de $n \in \mathbb{N}$ com $i(n) = [(0,n)]_\sim \in \mathbb{Z}$ dá $-n = [(n,0)]_\sim$ para todos $n \in \mathbb{N}$, e então Exercise A.2.12 implica que todo número inteiro é igual a exatamente um de 0, n ou $-n$ para algum número natural positivo n.

O próximo resultado prova que $\mathbb{Z}$ é um *anel*—o que isso significa em essência é que as operações de adição, multiplicação e negação satisfazem as propriedades básicas que tomamos como certas ao fazer aritmética com inteiros.

✣ **Theorem A.2.13** ($\mathbb{Z}$ é um anel)

(a) **(Associatividade de adição)** $(a+b)+c = a+(b+c)$ para todo $a,b,c \in \mathbb{Z}$.

(b) **(Comutatividade de adição)** $a+b = b+a$ para todo $a,b \in \mathbb{Z}$.

(c) **(Zero)** $a+0 = a$ para todo $a \in \mathbb{Z}$.

(d) **(Negação)** $a+(-a) = 0$ para todo $a \in \mathbb{Z}$.

(e) **(Associatividade de multiplicação)** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a,b,c \in \mathbb{Z}$.

(f) **(Comutatividade da multiplicação)** $a \cdot b = b \cdot a$ para todo $a,b \in \mathbb{Z}$.

(g) **(Um)** $a \cdot 1 = a$ para todo $a \in \mathbb{Z}$.

(h) **(Distributividade)** $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ para todo $a,b,c \in \mathbb{Z}$.

Proof
Muitas páginas seriam desperdiçadas escrevendo a prova deste teorema em todos os detalhes. Em vez disso, provaremos apenas a parte (h); qualquer leitor particularmente masoquista é convidado a provar as partes (a)–(g) por conta própria.

Para ver se a lei da distributividade é válida, seja $a,b,c \in \mathbb{Z}$, e seja $m,n,p,q,r,s \in \mathbb{N}$ tal que $a = [(m,n)]_\sim$, $b = [(p,q)]_\sim$ e $c = [(r,s)]_\sim$. (Omitiremos o subscrito $\sim$ a seguir.)

Então:

$$\begin{aligned}
&a \cdot (b+c) \\
&= [(m,n)] \cdot ([(p,q)] + [(r,s)]) \\
&= [(m,n)] \cdot [(p+r,q+s)] \\
&= [(m(q+s)+n(p+r), m(p+r)+n(q+s))] \\
&= [(mq+ms+np+nr, mp+mr+nq+ns)] \\
&= [(mq+np, mp+nq)] + [(ms+nr, mr+ns)] \\
&= [(m,n)] \cdot [(p,q)] + [(m,n)] \cdot [(r,s)] \\
&= (a \cdot b) + (a \cdot c)
\end{aligned}$$

como requerido. □

Números racionais

Assim como construímos os números inteiros a partir dos números naturais, formalizando o que entendemos por "diferença" de dois números naturais, construiremos os números racionais a partir dos inteiros, formalizando o que entendemos por "proporção" de dois inteiros.

Como os números racionais devem assumir a forma $\dfrac{a}{b}$ com $a,b \in \mathbb{Z}$ e $b \neq 0$, uma primeira tentativa de construir $\mathbb{Q}$ pode ser pegar $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, e deixar o par (a,b) representar a fração $dfracab$. Mas assim como um número inteiro não pode ser expresso exclusivamente como a diferença de dois números naturais, um número racional não pode ser expresso exclusivamente como a razão de dois inteiros — por exemplo, temos $\dfrac{1}{2} = \dfrac{2}{4}$.

Isso significa que devemos identificar $(a,b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ com $(c,d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ sempre que $\dfrac{a}{b} = \dfrac{c}{d}$. Mas espere! Ainda não definimos uma operação de divisão, portanto não podemos usá-la em nossa construção de $\mathbb{Q}$—então, em vez disso, identificaremos (a,b) com (c,d) sempre que $ad = bc$, observando que isso será equivalente a $\dfrac{a}{b} = \dfrac{c}{d}$ depois de definirmos uma operação de divisão.

Lemma A.2.14
A relação $\sim$ em $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$, definida para $(a,b),(c,d)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ deixando $(a,b)\sim(c,d)$ se e somente se $ad=bc$, é uma relação de equivalência.

Sketch of proof
A prova é essencialmente a mesma de Lemma A.2.10, mas com adição substituída por multiplicação; a prova da transitividade usa o fato de que para $u,v,w\in\mathbb{Z}$ com $u\neq 0$, temos $uv=uw\Rightarrow v=w$, o que pode ser provado por indução em $|voc|\geqslant 1$ sem usar uma operação de divisão. □

Construction A.2.15
O **conjunto de números racionais** é o conjunto $\mathbb{Q}$ definido por

$$\mathbb{Q}=(\mathbb{Z}\times(\mathbb{Z}\setminus\{0\}))/\sim$$

onde $\sim$ é a relação de equivalência em $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ definida por

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

para todos $(a,b),(c,d)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$.

Escreveremos '$\frac{a}{b}$' para denotar o elemento $[(a,b)]_\sim\in\mathbb{Q}$, observando que $\frac{a}{b}=\frac{c}{d}$ se e somente se $ad=bc$. Agora podemos definir operações de adição, multiplicação, negação e subtração em $\mathbb{Q}$ em termos daquelas em $\mathbb{Z}$—ou seja, dado $a,b,c,d\in\mathbb{Z}$ com $b,d\neq 0$, definimos

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd},\quad -\frac{a}{b}=\frac{-a}{b},\quad \frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}$$

Como sempre, devemos (mas não iremos) verificar se essas operações estão bem definidas.

Novamente, não temos $\mathbb{Z}\subseteq\mathbb{Q}$, mas podemos incorporar $\mathbb{Z}$ em $\mathbb{Q}$ de uma forma que respeite as operações aritméticas de adição , multiplicação, negação e subtração.

Exercise A.2.16
Prove que a função $i:\mathbb{Z}\to\mathbb{Q}$ definida por $i(a)=\frac{a}{1}$ é uma injeção, e para todo $a,b\in\mathbb{Z}$ temos $i(a+b)=i(a)+i(b)$, $i(ab)=i(a)i(b)$, $i(-a)=-i(a)$ e $i(ab)=i(a)-i(b)$. ◁

À luz disso, dado $a\in\mathbb{Z}$, normalmente escreveremos apenas 'a' para o número racional $i(a)=\frac{a}{1}\in\mathbb{Q}$, então podemos fingir que $\mathbb{Z}\subseteq\mathbb{Q}$ mesmo que este não seja estritamente o caso.

A construção de $\mathbb{Q}$ também permite definir operações recíprocas e de divisão. Observe que $\frac{c}{d} = 0$ se e somente se $c = c \cdot 1 = 0 \cdot d = 0$; então se $a,b,c,d \in \mathbb{Q}$ com $b,c,d \neq 0$, então definimos

$$\left(\frac{c}{d}\right)^{-1} = \frac{d}{c} \quad \textbf{e} \quad \frac{a}{b} \div fraccd = \frac{ad}{bc}$$

O comentário usual sobre bem-definição se aplica. Observe que para todo $a,b \in \mathbb{Z}$ com $b \neq 0$ temos

$$a \div b = \frac{a}{1} \div \frac{b}{1} = \frac{a \cdot 1}{1 \cdot b} = \frac{a}{b}$$

Portanto, dispensaremos o símbolo '$\div$' e simplesmente usaremos a notação de fração.

Observe também que as operações recíprocas e de divisão podem ser definidas uma em função da outra: elas são relacionadas pelas identidades
] y$^{-1} = \frac{1}{y} \quad \textbf{e} \quad \frac{x}{y} = x \cdot y^{-1}$ para todo $x,y \in \mathbb{Q}$ com $y \neq 0$.

$\mathbb{Q}$ é um campo

Números Reais

✦ **Definition A.2.17** (A construção dos números reais por Dedekind)
O **conjunto de** (**Dedekind**) **números reais** é o conjunto $\mathbb{R}$ definido por

$$\mathbb{R} = \{D \subseteq \mathbb{Q} \mid D \text{ é limitado acima e fechado para baixo}\}$$

To do: Operações aritméticas, ordem

To do: Motivar Cauchy reais

✦ **Definition A.2.18** (A construção dos números reais por Cauchy)
O **conjunto de** (**Cauchy**) **números reais** é o conjunto $\mathbb{R}$ definido por

$$\mathbb{R} = \{(x_n) \in \mathbb{Q}^{\mathbb{N}} \mid (x_n) \text{ é Cauchy}\}/\sim$$

onde $\sim$ é a relação de equivalência definida por

$$(x_n) \sim (y_n) \text{ se e somente se } (x_n - y_n) \to 0$$

para todas as sequências de Cauchy $(x_n),(y_n)$ de números racionais.

To do: Operações aritméticas, ordem

To do: Motivar a definição de números complexos

✦ **Definition A.2.19**
O **conjunto dos números complexos** é o conjunto $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.

To do: Operações aritimeticas

Estruturas algébricas

To do: Monóides, grupos, anéis

Axiomatizando os números reais

To do:

Axioms A.2.20 (Axiomas de campo)
Seja X um conjunto equipado com elementos 0 ('zero') e 1 ('unidade'), e operações binárias $+$ ('adição') e $\cdot$ ('multiplicação'). A estrutura $(X,0,1,+,\cdot)$ é um **campo** se satisfizer os seguintes axiomas:

- **Zero e unidade**

  (F1) $0 \neq 1$.

- **Axiomas para adição**

(F2) (Associatividade) $x+(y+z) = (x+y)+z$ para todo $x,y,z \in X$.

(F3) (Identidade) $x+0 = x$ para todo $x \in X$.

(F4) (Inverso) Para todo $x \in X$, onde existe $y \in X$ tanto que $x+y = 0$.

(F5) (Comutatividade) $x+y = y+x$ para todo $x,y \in X$.

- **Axiomas por multiplicação**

  (F6) (Associatividade) $x\cdot(y\cdot z) = (x\cdot y)\cdot z$ para todo $x,y,z \in X$.

  (F7) (Identidade) $x\cdot 1 = x$ para todo $x \in X$.

  (F8) (Inverso) Para todo $x \in X$ com $x \neq 0$, onde existe $y \in X$ tanto que $x\cdot y = 1$.

  (F9) (Comutatividade) $x\cdot y = y\cdot x$ para todo $x,y \in X$.

- **Distributividade**

  (F10) $x\cdot(y+z) = (x\cdot y)+(x\cdot z)$ para todo $x,y,z \in X$.

Example A.2.21
Os racionais $\mathbb{Q}$ e os reais $\mathbb{R}$ formam campos com suas noções usuais de zero, unidade, adição e multiplicação. No entanto, os inteiros $\mathbb{Z}$ não, já que por exemplo 2 não tem inverso multiplicativo. $\triangleleft$

Example A.2.22
Seja $p > 0$ primo. O conjunto $\mathbb{Z}/p\mathbb{Z}$ (ver **??**) é um campo, com elemento zero $[0]_p$ e elemento unitário $[1]_p$, e com adição e multiplicação definida por

$$[a]_p + [b]_p = [a+b]_p \quad \text{e} \quad [a]_p \cdot [b]_p = [ab]_p$$

para todo $a,b \in \mathbb{Z}$. A boa definição dessas operações é imediata desde **??** e o teorema da aritmética modular (**??**).

O único axioma que não é fácil de verificar é o axioma do inverso multiplicativo (F8). Na verdade, se $[a]_p \in \mathbb{Z}/p\mathbb{Z}$ então $[a]_p \neq [0]_p$ se e somente se $p \nmid a$. Mas se $p \nmid a$ então $a \perp p$, então a tem um inverso multiplicativo u módulo p. Isso implica que $[a]_p \cdot [u]_p = [au]_p = [1]_p$. Então (F8) é válido. $\triangleleft$

✎ **Exercise A.2.23**
Seja $n > 0$ composto. Prove que $\mathbb{Z}/n\mathbb{Z}$ não é um corpo, onde zero, unidade, adição e multiplicação são definidos como em Example A.2.22. ◁

Axioms A.2.20 diga-nos que todo elemento de um corpo tem um inverso aditivo, e todo elemento *diferente de zero* de um corpo tem um inverso multiplicativo. Seria conveniente se os inversos fossem *[úicos* sempre que existissem. Proposition A.2.24 prova que este é o caso.

✣ **Proposition A.2.24** (Singularidade dos inversos)
Seja $(X, 0, 1, +, \cdot)$ e um campo e seja $x \in X$. Então

(a) Suponha que $y, z \in X$ sejam tais que $x + y = 0$ e $x + z = 0$. Então $y = z$.

(b) Suponha que $x \neq 0$ e $y, z \in X$ sejam tais que $x \cdot y = 1$ e $x \cdot z = 1$. Então $y = z$.

Proof *de (a)*
Por cálculo, temos

$$\begin{aligned}
y &= y + 0 && \text{por (F3)} \\
&= y + (x + z) && \text{por definição de } z \\
&= (y + x) + z && \text{por associatividade (F2)} \\
&= (x + y) + z && \text{by commutativity (F5)} \\
&= 0 + z && \text{por definição de } y \\
&= z + 0 && \text{por comutatividade (F5)} \\
&= z && \text{by (F3)}
\end{aligned}$$

então de fato $y = z$.

A prova de (b) é essencialmente a mesma e fica como exercício. □

Como os inversos são únicos, faz sentido ter uma notação para se referir a eles.

✦ **Notation A.2.25**
Seja $(X, 0, 1, +, \cdot)$ um campo e seja $x \in X$. Escreva $-x$ para o inverso aditivo (único) de x e, se $x \neq 0$ escreva x^{-1} para o inverso multiplicativo (único) de x.

✐ **Example A.2.26**
Nos campos $\mathbb{Q}$ e $\mathbb{R}$, o inverso aditivo $-x$ de um elemento x é simplesmente seu negativo, e o inverso multiplicativo x^{-1} de algum $x \neq 0$ é simplesmente seu recíproco $\frac{1}{x}$. ◁

✐ **Example A.2.27**
Seja $p > 0$ primo e seja $[a]_p \in \mathbb{Z}/p\mathbb{Z}$. Então $-[a]_p = [-a]_p$ e, se $p \nmid a$, então $[a]_p^{-1} = [u]_p$, onde u é qualquer número inteiro satisfatório $au \equiv 1 \bmod p$. ◁

✎ **Exercise A.2.28**

Seja $(X, 0, 1, +, \cdot)$ um campo. Prove que $-(-x) = x$ para todo $x \in X$, e que $(x^{-1})^{-1} = x$ para todo $x \in X$ diferente de zero. $\lhd$

Example A.2.29

Seja $(X, 0, 1, +, \cdot)$ um campo. Provamos que se $x \in X$ então $x \cdot 0 = 0$. Bem, $0 = 0 + 0$ por (F3). Portanto, $x \cdot 0 = x \cdot (0 + 0)$. Pela distributividade (F10), temos $x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0)$. Por isso

$$x \cdot 0 = (x \cdot 0) + (x \cdot 0)$$

Seja $y = -(x \cdot 0)$. Então

$$\begin{aligned} 0 &= x \cdot 0 + y && \text{by (F4)} \\ &= ((x \cdot 0) + (x \cdot 0)) + y && \text{como acima} \\ &= (x \cdot 0) + ((x \cdot 0) + y) && \text{by associativity (F2)} \\ &= (x \cdot 0) + 0 && \text{by (F4)} \\ &= x \cdot 0 && \text{by (F3)} \end{aligned}$$

então de fato nós temos $x \cdot 0 = 0$. $\lhd$

Exercise A.2.30

Seja $(X, 0, 1, +, \cdot)$ um campo. Prove que $(-1) \cdot x = -x$ para todo $x \in X$, e que $(-x)^{-1} = -(x^{-1})$ para todo $diferentedezeroxX$. $\lhd$

O que torna os números reais úteis não é simplesmente a nossa capacidade de adicioná-los, subtraí-los, multiplicá-los e dividi-los; também podemos comparar seu tamanho — na verdade, é isso que dá origem à noção informal de *reta numérica*. Axioms A.2.31 esclarece exatamente o que significa os elementos de um campo serem montados em uma 'reta numérica'.

Axioms A.2.31 (Axiomas de campo ordenados)
Seja X um conjunto, $0, 1 \in X$ sejam elementos, $+, \cdot$ sejam operações binárias e $\leqslant$ seja uma relação em X. A estrutura $(X, 0, 1, +, \cdot, \leqslant)$ é um **campo ordenado** se satisfaz os axiomas de campo (F1)–(F10) (veja **??**) e, adicionalmente, satisfaz os seguintes axiomas:

- **Axiomas de ordem linear**

  (PO1) (Reflexitividade) $x \leqslant x$ para todo $x \in X$.

  (PO2) (Antissimétria) Para todo $x, y \in X$, se $x \leqslant y$ e $y \leqslant x$, então $x = y$.

  (PO3) (Transitividade) Para todo $x, y, z \in X$, se $x \leqslant y$ e $y \leqslant z$, então $x \leqslant z$.

  (PO4) (Linearidade) Para todo $x, y \in X$, qualquer $x \leqslant y$ ou $y \leqslant x$.

- **Interação de ordem com aritmética**

  (OF1) Para todo $x, y, z \in X$, se $x \leqslant y$, então $x + z \leqslant y + z$.

  (OF2) Para todo $x, y \in X$, se $0 \leqslant x$ e $0 \leqslant y$, então $0 \leqslant xy$.

Example A.2.32
O corpo $\mathbb{Q}$ dos números racionais e o campo $\mathbb{R}$ dos números reais, com suas noções usuais de ordenação, podem ser facilmente vistos como campos ordenados. $\triangleleft$

Example A.2.33
Provamos que, em qualquer corpo ordenado, temos $0 \leqslant 1$. Observe primeiro que $0 \leqslant 1$ ou $1 \leqslant 0$ por linearidade (PO4). Se $0 \leqslant 1$ então terminamos, então suponha $1 \leqslant 0$. Então $0 \leqslant -1$; de fato:

$$\begin{aligned}
0 &= 1 + (-1) && \text{por (F4)} \\
&\leqslant 0 + (-1) && \text{por (OF1), desde } 1 \leqslant 0 \\
&= (-1) + 0 && \text{por comutatividade (F5)} \\
&= -1 && \text{by (F3)}
\end{aligned}$$

Por (OF2), segue-se que $0 \leqslant (-1)(-1)$. Mas $(-1)(-1) = 1$ por Exercise A.2.30 e, portanto, $0 \leqslant 1$. Como $1 \leqslant 0$ e $0 \leqslant 1$, temos $0 = 1$ por antisimetria (PO2). Mas isso contradiz o axioma (F1). Portanto, $0 \leqslant 1$. Na verdade, $0 < 1$ já que $0 \neq 1$. $\triangleleft$

Vimos que $\mathbb{Q}$ e $\mathbb{R}$ são campos ordenados (Examples A.2.26 and A.2.32), e que $\mathbb{Z}/p\mathbb{Z}$ é um campo para $p > 0$ prime (Example A.2.22). A seguinte proposição é um resultado interessante que prova que não existe noção de 'ordenação' sob a qual o campo $\mathbb{Z}/p\mathbb{Z}$ possa ser transformado em um campo ordenado!

Proposition A.2.34

Seja $p > 0$ primo. Não há relação $\leqslant$ em $\mathbb{Z}/p\mathbb{Z}$ que satisfaça os axiomas de campo ordenados.

Proof
Acabamos de mostrar que $[0] \leqslant [1]$. Segue-se que, para todo $a \in \mathbb{Z}$, temos $[a] \leqslant [a]+[1]$; de fato: [a] = [a]+[0] por (F3)
$\leqslant [a]+[1]$by (OF1), já que $[0] \leqslant [1]$
$= [a+1]$por definição de $+$ em $\mathbb{Z}/p\mathbb{Z}$ É uma indução direta provar que $[a] \leqslant [a+n]$ para todo $n \in \mathbb{N}$. Mas então temos

$$[1] \leqslant [1+(p-1)] = [p] = [0]$$

então $[0] \leqslant [1]$ e $[1] \leqslant [0]$. Isso implica $[0] = [1]$ por antissimetria (PO2), contradizendo o axioma (F1). $\square$

✎ **Exercise A.2.35**
Seja $(X, 0, 1, +, \cdot)$ um campo. Prove que se X é finito, então não há relação $\leqslant$ em X tal que $(X, 0, 1, +, \cdot, \leqslant)$ seja um corpo ordenado. $\lhd$

Theorem A.2.36 abaixo resume algumas propriedades de campos ordenados que são usados em nossas provas. Observe, entretanto, que esta certamente *não* é uma lista exaustiva de propriedades elementares de campos ordenados que usamos — para declarar explicitamente e provar que tudo isso não seria uma leitura brilhante.

Theorem A.2.36
Seja $(X, 0, 1, +, \cdot, \leqslant)$ seja um campo ordenado. Então

(a) Para todo $x, y \in X$, $x \leqslant y$ se e apenas se $0 \leqslant y - x$;

(b) Para todo $x \in X$, $-x \leqslant 0 \leqslant x$ ou $x \leqslant 0 \leqslant -x$;

(c) Para todo $x, x', y, y' \in X$, se $x \leqslant x'$ e $y \leqslant y'$, então $x + y \leqslant x' + y'$;

(d) Para todo $x, y, z \in X$, se $0 \leqslant x$ e $y \leqslant z$, então $xy \leqslant xz$;

(e) Para todo nonzero $x \in X$, if $0 \leqslant x$, então $0 \leqslant x^{-1}$.

(f) Para todo nonzero $x, y \in X$, if $x \leqslant y$, então $y^{-1} \leqslant x^{-1}$.

***Proof** de (a), (b) e (e)*

(a) $(\Rightarrow)$ suponha $x \leqslant y$. Então, por aditividade (OF1), $x + (-x) \leqslant y + (-x)$, isso é $0 \leqslant y - x$. $(\Leftarrow)$ Suponha $0 \leqslant y - x$. Por aditividade (OF1), $0 + x \leqslant (y - x) + x$; isto é, $x \leqslant y$.

(b) Sabemos por linearidade (PO4) que $0 \leqslant x$ ou $x \leqslant 0$. Se $0 \leqslant x$, então por (OF1) temos $0 + (-x) \leqslant x + (-x)$, ou seja $-x \leqslant 0$. Da mesma forma, se $x \leqslant 0$ então $0 \leqslant -x$.

(e) Suponha $0 \leqslant x$. Por linearidade (PO4), $0 \leqslant x^{-1}$ ou $x^{-1} \leqslant 0$. Se $x^{-1} \leqslant 0$, então por (d) temos $x^{-1} \cdot x \leqslant 0 \cdot x$, que é $1 \leqslant 0$. Isso contradiz Example A.2.33, então devemos ter $0 \leqslant x^{-1}$.

As demonstrações das demais propriedades ficam como exercício. □

Queríamos caracterizar os reais completamente, mas até agora não conseguimos fazê-lo — na verdade, Example A.2.32 mostrou que ambos $\mathbb{Q}$ e $\mathbb{R}$ são campos ordenados, então os axiomas de campo ordenados não são suficientes para distinguir $\mathbb{Q}$ de $\mathbb{R}$. A peça final do quebra-cabeça é *completude*. Este único axioma adicional distingue $\mathbb{Q}$ de $\mathbb{R}$, e de fato caracteriza completamente $\mathbb{R}$ (veja Theorem A.2.38).

Axioms A.2.37 (Axiomas de campo ordenados completos)
Seja X um conjunto, $0, 1 \in X$ sejam elementos, $+, \cdot$ sejam operações binárias e $\leqslant$ seja uma relação em X. A estrutura $(X, 0, 1, +, \cdot, \leqslant)$ é um **campo ordenado completo** se for um campo ordenado — isto é, satisfaz os axiomas (F1) –(F10), (PO1)–(PO4) e (OF1)–(OF2) (veja Axioms A.2.20 and A.2.31)—e, além disso, satisfaz o seguinte **axioma de completude** :

(C1) Seja $A \subseteq X$. Se A tiver um limite superior, então terá um limite superior mínimo. Especificamente, se existe $u \in X$ tal que $a \leqslant u$ para todo $a \in A$, então existe $s \in X$ tal que

- $a \leqslant s$ para todo $a \in A$; e
- Se $s' \in X$ é tanto que $a \leqslant s'$ para todo $a \in A$, então $s \leqslant s'$.

Chamamos esse valor $s \in X$ a **supremo** for A.

Theorem A.2.38
Os números reais $(\mathbb{R}, 0, 1, +, \cdot, \leqslant)$ formam um campo ordenado completo. Além disso, quaisquer dois campos ordenados completos são essencialmente iguais. □

A noção de 'semelhança' aludida em Theorem A.2.38 é mais apropriadamente chamada de *isomorfismo*. Uma prova deste teorema é complexa e está muito além do escopo deste livro, por isso foi omitida. O que isso nos diz é que não importa exatamente como definimos os reais, pois qualquer campo ordenado completo serve. Podemos, portanto, prosseguir com a confiança de que, independentemente da noção de «números reais» que escolhermos, tudo o que provarmos será verdadeiro relativamente a essa noção. Isso é melhor, já que na verdade ainda não definimos o conjunto $\mathbb{R}$ de números reais!

As duas abordagens mais comuns para construir um conjunto de números reais são:

Reais de Dedekind. Nesta abordagem, os números reais são identificados com subconjuntos particulares de $\mathbb{Q}$—falando informalmente, $r \in \mathbb{R}$ é identificado com o conjunto de números racionais menores que r.

Reais de Cauchy. Nesta abordagem, os números reais são identificados com classes de equivalência de sequências de números racionais — falando informalmente, $r \in \mathbb{R}$ é identificado com o conjunto de sequências de números racionais números que convergem para r (no sentido de **??**).

Section A.3

Limites de funções

No final de **??** mencionamos o uso de *limites* de funções sem definir corretamente o que queríamos dizer. Esta seção reconhecidamente brusca é dedicada a tornar preciso o que queremos dizer com matemática.

Limites

Definition A.3.1
Seja $D \subseteq \mathbb{R}$. Um **ponto limite** de D é um número real a tal que, para todo $\delta > 0$, existe algum $x \in D$ tal que $0 < |x-a| < \delta$.

Lemma A.3.2
Seja $D \subseteq \mathbb{R}$. Um número real a é um ponto limite de D se e somente se existe uma sequência (x_n) de elementos de D, que não é eventualmente constante, tal que $(x_n) \to a$
.

Proof

□

($\Rightarrow$) Seja $a \in \mathbb{R}$ e assuma que a é um ponto limite de D. Para cada $n \geqslant 1$, seja x_n algum elemento de D tal que $0 < |x_n - a| < \dfrac{1}{n}$.

Evidentemente $(x_n) \to a$: de fato, dado $\varepsilon > 0$, deixando $N \geqslant \max\{1, \frac{1}{\varepsilon}\}$ dá $|x_n - uma| < \varepsilon$ para todos $n \geqslant N$.

Além disso, a sequência (x_n) não é eventualmente constante: se fosse, existiriam $N \geqslant 1$ e $b \in \mathbb{R}$ tais que $x_n = b$ para todos $n\, geN$. Mas então, pelo teorema da compressão (**??**), teríamos

$$0 \leqslant \lim_{n\to\infty} |x_n - a| = |ba| \leqslant \lim_{n\to\infty} \frac{1}{n} = 0$$

e então $b = a$. Mas isso contradiz o fato de que $|x_n - a| > 0$ para todo $n \geqslant 1$.

($\Leftarrow$) Seja $a \in \mathbb{R}$ e assuma que existe uma sequência (x_n) de elementos de D, que não é eventualmente constante, tal que $(x_n) \to um$. Então para todo $\delta > 0$ existe algum $N \in \mathbb{N}$ tal que $|x_n - a| < \varepsilon$ para todos $n \geqslant N$. Como (x_n) não é eventualmente constante, existe algum $n \geqslant N$ tal que $|x_n - a| > 0$—caso contrário (x_n) seria eventualmente constante com valor a! Mas então $x_n \in D$ e $0 < |x_n - a| < \delta$, então a é um ponto limite de D.

✦ **Definition A.3.3**
Seja $D \subseteq \mathbb{R}$. O **fechamento** de D é o conjunto $\overline{D}$ (LaTeX code: `\overline{D}`) definido por

$$\overline{D} = D \cup \{a \in \mathbb{R} \mid a \text{ é um ponto limite de } D\}$$

Ou seja, $\overline{D}$ é dado por D junto com seus pontos limites.

✐ **Example A.3.4**
Temos $\overline{(0,1)} = [0,1]$. Na verdade, $(0,1) \subseteq \overline{(0,1)}$ já que $D \subseteq \overline{D}$ para todo $D \subseteq \mathbb{R}$. Além disso, as sequências $(\frac{1}{n})$ e $(1-\frac{1}{n})$ não são constantes, assumem valores em $(0,1)$ e convergem para 0 e 1 respectivamente, de modo que $0 \in \overline{(0,1)}$ e $1 \in \overline{(0,1)}$. Portanto $[0,1] \subseteq \overline{(0,1)}$.

Dado $a \in \mathbb{R}$, se $a > 1$, então deixar $\delta = 1 - a > 0$ revela que $|x-a| \geqslant \delta$ para todo $x \in D$; e da mesma forma, se $a < 0$, então deixar $\delta = -a > 0$ revela que $|x-a| \geqslant \delta$ para todo $x \in D$. Portanto, nenhum elemento de $\mathbb{R} \setminus [0,1]$ é um elemento de D, de modo que $\overline{(0,1)} = [0,1]$. ◁

✎ **Exercise A.3.5**
Seja $a, b \in \mathbb{R}$ com $a < b$. Prove que $\overline{(a,b)} = \overline{(a,b]} = \overline{[a,b)} = [a,b]$. ◁

❖ **Convention A.3.6**
Para o restante desta seção, sempre que declararmos $f : D \to \mathbb{R}$ como uma função, será assumido que o domínio D é um subconjunto de $\mathbb{R}$, e que todo ponto de D é um ponto limite de D. Em outras palavras, D não possui *pontos isolados*, que são pontos separados de todos os outros elementos de D por uma distância positiva. Por exemplo, no conjunto $(0,1] \cup \{2\}$, o elemento $2 \in \mathbb{R}$ é um ponto isolado. ◁

✦ **Definition A.3.7**
Seja $f : D \to \mathbb{R}$ uma função, seja $a \in \overline{D}$, e seja $\ell \in \mathbb{R}$. Dizemos que ℓ é um **limit** de $f(x)$ quando x **se aproxima de** a se

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in D,\ 0 < |x-a| < \delta \ \Rightarrow\ |f(x) - \ell| < \varepsilon$$

Em outras palavras, para valores de $x \in D$ próximos de a (mas não iguais a a), os valores de $f(x)$ tornam-se arbitrariamente próximos de ℓ.

Escrevemos '$f(x) \to \ell$ como $x \to a$' (LaTeX code: `\to`) para denotar a afirmação de que ℓ é um limite de $f(x)$ conforme x se aproxima a.

✐ **Example A.3.8**
Defina $f : \mathbb{R} \to \mathbb{R}$ por $f(x) = x$ para todo $x \in \mathbb{R}$. Então $f(x) \to 0$ como $x \to 0$. Para ver isso, seja $\varepsilon > 0$ e defina $\delta = \varepsilon > 0$. Então, para todo $x \in \mathbb{R}$, se $0 < |x-a| < \delta = \varepsilon$, então

$$|f(x) - f(uma)| = |x-a| < \varepsilon$$

como requerido. ◁

✎ **Exercise A.3.9**
Seja $f : D \to \mathbb{R}$ uma função, seja $a \in D$ e seja $\ell \in \mathbb{R}$. Corrija alguma sequência (x_n) de elementos de D, não eventualmente constante, tal que $(x_n) \to a$. Prove que se $f(x) \to \ell$ como $x \to a$, então a sequência $(f(x_n))$ converge para ℓ. ◁

O próximo exercício diz-nos que os limites das funções são únicos, desde que existam. Sua prova se parece muito com o resultado análogo que provamos para sequências em **??**.

✎ **Exercise A.3.10**
Seja $f : D \to \mathbb{R}$ uma função, seja $a \in D$, e $\ell_1, \ell_2 \in \mathbb{R}$. Prove que se $f(x) \to \ell_1$ como $x \to a$, e $f(x) \to \ell_2$ como $x \to a$, então $\ell_1 = \ell_2$. ◁

Quando o domínio D de uma função $f : D \to \mathbb{R}$ é ilimitado, também podemos estar interessados em descobrir como os valores de $f(x)$ se comportam como $x \in D$ fica (positiva ou negativamente) cada vez maior.

✦ **Definition A.3.11**
Seja $f : D \to \mathbb{R}$ uma função e seja $\ell \in \mathbb{R}$. Se D é ilimitado acima — isto é, para todo $p \in \mathbb{R}$, existe $x \in D$ com $x > p$ — então dizemos ℓ é um **limite** de $f(x)$ à medida que x **aumenta sem limites** se

$$\forall \varepsilon > 0,\ \exists p \in \mathbb{R},\ \forall x \in D,\ x > p\ \Rightarrow\ |f(x) - \ell| < \varepsilon$$

Escrevemos '$f(x) \to \ell$ as $x \to \infty$' (LaTeX code: `\infty`) para denotar a afirmação de que ℓ é um limite de $f(x)$ como x aumenta sem limite.

Da mesma forma, se D é ilimitado abaixo — isto é, para todo $p \in \mathbb{R}$, existe $x \in D$ com $x < p$— então dizemos *ell* é um **limite** de $f(x)$ conforme x **diminui sem limite** se

$$\forall \varepsilon > 0,\ \exists p \in \mathbb{R},\ \forall x \in D,\ x < p\ \Rightarrow\ |f(x) - \ell| < \varepsilon$$

Escrevemos '$f(x) \to \ell$ como $x \to -\infty$' para denotar a afirmação de que ℓ é um limite de $f(x)$ à medida que x diminui sem limite.

✐ **Example A.3.12**
Seja $f : \mathbb{R} \to \mathbb{R}$ a função definida por $f(x) = \dfrac{x}{1+|x|}$ para todo $x \in \mathbb{R}$. Então:

$f(x) \to 1$ como $x \to \infty$. Para ver isso, seja $\varepsilon > 0$ e defina $p = \max\{1, \frac{1}{\varepsilon}\}$. Então, para todo $x > p$, temos $x > 0$, de modo que $f(x) = \dfrac{x}{1+x}$, e $x > \frac{1}{\varepsilon} - 1$. Por isso:

$$\left|\frac{x}{1+x} - 1\right| = \left|\frac{-1}{1+x}\right| = \frac{1}{1+x} < \frac{1}{1+(\frac{1}{\varepsilon}-1)} = \varepsilon$$

como requerido.

$f(x) \to -1$ como $x \to \infty$. Para ver isso, seja $\varepsilon > 0$ e defina $p = \min\{-1, \frac{-1}{\varepsilon}\}$. Então, para todo $x < p$, temos $x < 0$, de modo que $f(x) = \frac{1}{1-x}$, e $x < \frac{-1}{\varepsilon} + 1$. Por isso:

$$\left|\frac{x}{1-x} - (-1)\right| = \left|\frac{1}{1-x}\right| = \frac{1}{1-x} < \frac{1}{1-(-\frac{1}{\varepsilon}+1)} = \varepsilon$$

como requerido. Então $f(x) \to 1$ como $x \to \infty$ e $f(x) \to -1$ como $x \to -\infty$. ◁

✎ **Exercise A.3.13**

Seja $f : D \to \mathbb{R}$ uma função e $\ell_1, \ell_2 \in \mathbb{R}$. Prove que se D é ilimitado acima, e se $f(x) \to \ell_1$ como $x \to \infty$ e $f(x) \to \ell_2$ como $x \to \infty$, então $\ell_1 = \ell_2$. Prove o resultado análogo para limites como $x \to -\infty$ no caso em que D é ilimitado abaixo. ◁

Os resultados de Exercises A.3.10 and A.3.13 justificam a seguinte definição.

✦ **Definition A.3.14**

Seja $f : D \to \mathbb{R}$ e seja $a \in [-\infty, \infty]$. Supondo que os limites em questão sejam bem definidos e existam, escrevemos $\lim\limits_{x \to a} f(x)$ para denotar o único número real $\ell \in \mathbb{R}$ tal que $f(x) \to \ell$ como $x \to a$.

Appendix B

Dicas para exercícios selecionados

Chapter 0

?? exercises

Section A.1

Section A.2

Hint for Exercise A.2.9
Defina duas relações $\leqslant$ e $\leqslant'$ em $\mathbb{N}$, uma usando a definição recursiva e a outra usando a definição como fórmula lógica; então use a indução para provar que $m \leqslant n \Leftrightarrow m \leqslant' n$ para todo $m, n \in \mathbb{N}$.

Hint for Exercise A.2.28
Prove que x é um inverso aditivo para $-x$ (no sentido de Axioms A.2.20(F4)) e use a unicidade dos inversos aditivos. Da mesma forma para x^{-1}.

Section A.3

Índices

Index of topics

axioma da completude, 45

base-*b* expansion, 6

campo, 40
campo ordenado completo, 45

discriminante, 18
divisor, 8
divisão, 8

fator, 8

Inteiro
    par, 9
    ´impar, 9

limites de umaa função, 48

múltiplo, 8

natural
    número, 29
number base, 6
numéro irracional, 14
número natural, 29
número natural
    von Neumann, 29
número natural de von Neumann , 29

polinômios, 17
proposição, 1
prova, 1

quociente, 10

raiz, 18
restante, 10

sistema de numeração
    Hindu–árabe, 5
sistema numérico, 5

teorema da divisão, 10

Index of notation

n_{vN} — *numéro natural de von neuman*, 29

Index of LaTeX commands

Math mode commands
`\ge`, $\geqslant$, 13
`\in`, $\in$, 3
`\le`, $\leqslant$, 13
`\mathbb`, $\mathbb{A}, \mathbb{B}, \ldots$, 4, 8, 12, 15

Licence

Licença Pública Internacional Creative Commons Attribution-ShareAlike 4.0

Ao exercer os Direitos Licenciados (definidos abaixo), Você aceita e concorda em ficar vinculado aos termos e condições desta Licença Pública Internacional Creative Commons Attribution-ShareAlike 4.0 ("Licença Pública"). Na medida em que esta Licença Pública possa ser interpretada como um contrato, são concedidos a Você os Direitos Licenciados em consideração à Sua aceitação destes termos e condições, e o Licenciador concede a Você tais direitos em consideração aos benefícios que o Licenciador recebe ao disponibilizar o Material Licenciado. sob estes termos e condições.

Section 1 — Definitions.

a. **Material Adaptado** significa material sujeito a Direitos Autorais e Direitos Similares que é derivado ou baseado no Material Licenciado e no qual o Material Licenciado é traduzido, alterado, organizado, transformado ou de outra forma modificado de uma maneira que requer permissão sob os Direitos Autorais e Similares. Direitos detidos pelo Licenciante. Para os fins desta Licença Pública, quando o Material

Licenciado for uma obra musical, performance ou gravação sonora, o Material Adaptado será sempre produzido quando o Material Licenciado for sincronizado em relação temporal com uma imagem em movimento.

b. **Licença do Adaptador** significa a licença que Você aplica aos Seus Direitos Autorais e Direitos Similares em Suas contribuições ao Material Adaptado de acordo com os termos e condições desta Licença Pública.

c. **Licença compatível com BY-SA** significa uma licença listada em creativecommons.org/compatívellicenses, aprovada pela Creative Commons como essencialmente equivalente a esta Licença Pública Licença.

d. **Direitos Autorais e Direitos Similares** significa direitos autorais e/ou direitos semelhantes intimamente relacionados aos direitos autorais, incluindo, sem limitação, desempenho, transmissão, gravação de som e Direitos de Banco de Dados Sui Generis, independentemente de como os direitos são rotulados ou categorizados. Para os fins desta Licença Pública, os direitos especificados na Seção 2(b)(1)-(2) não são Direitos Autorais e Direitos Similares.

e. **Medidas Tecnológicas Eficazes** significa aquelas medidas que, na ausência de autoridade adequada, não podem ser contornadas sob leis que cumprem obrigações sob o Artigo 11 do Tratado de Direitos Autorais da OMPI adotado em 20 de dezembro de 1996, e/ou acordos internacionais semelhantes .

f. **Exceções e Limitações** significa uso justo, negociação justa e/ou qualquer outra exceção ou limitação aos Direitos Autorais e Direitos Similares que se aplica ao Seu uso do Material Licenciado.

g. **Elementos de Licença** significa os atributos de licença listados no nome de uma Licença Pública Creative Commons. Os Elementos de Licença desta Licença Pública são Atribuição e Compartilhamento pela mesma Licença.

h. **Material Licenciado** significa a obra artística ou literária, banco de dados ou outro material ao qual o Licenciador aplicou esta Licença Pública.

i. **Direitos Licenciados** significa os direitos concedidos a Você sujeitos aos termos e condições desta Licença Pública, que são limitados a todos os Direitos Autorais e Direitos Similares que se aplicam ao Seu uso do Material Licenciado e que o Licenciador tem autoridade para licença.

j. **Licenciador** significa o(s) indivíduo(s) ou entidade(s) que concedem direitos sob esta Licença Pública.

k. **Compartilhar** significa fornecer material ao público por qualquer meio ou processo que exija permissão sob os Direitos Licenciados, como reprodução, exibição pública, apresentação pública, distribuição, disseminação, comunicação ou importação, e tornar material disponível ao público, inclusive de maneiras pelas quais os membros do público possam acessar o material em um local e em um horário escolhido individualmente por eles.

l. **Direitos Sui Generis sobre Bases de Dados** significa outros direitos que não os direitos de autor resultantes da Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de Março de 1996, relativa à protecção jurídica das bases de dados, conforme alterada e/ou sucedida, bem como outros essencialmente direitos equivalentes em qualquer parte do mundo.

m. **Você** significa o indivíduo ou entidade que exerce os Direitos Licenciados sob esta Licença Pública. **Seu** tem um significado correspondente.

Seção 2 - Escopo..

a. **Concessão de licença.**

   1. Sujeito aos termos e condições desta Licença Pública, o Licenciador concede a Você uma licença mundial, isenta de royalties, não sublicenciável, não exclusiva e irrevogável para exercer os Direitos Licenciados no Material Licenciado para:

      A. reproduzir e compartilhar o Material Licenciado, no todo ou em parte; e

      B. produzir, reproduzir e compartilhar material adaptado.

   2. <u>Exceções e Limitações</u>. Para evitar dúvidas, onde Exceções e Limitações se aplicam ao Seu uso, esta Licença Pública não se aplica e Você não precisa cumprir seus termos e condições.

   3. <u>Termo</u>. O prazo desta Licença Pública está especificado na Seção 6(a).

   4. <u>Mídias e formatos; modificações técnicas permitidas</u>. O Licenciante autoriza Você a exercer os Direitos Licenciados em todas as mídias e formatos, sejam agora conhecidos ou criados futuramente, e a fazer as modificações técnicas necessárias para fazê-lo. O Licenciador renuncia e/ou concorda em não reivindicar qualquer direito ou autoridade para proibi-lo de fazer modificações técnicas necessárias para exercer os Direitos Licenciados, incluindo modificações técnicas necessárias para contornar Medidas Tecnológicas Eficazes. Para os fins desta Licença Pública, simplesmente fazer modificações autorizadas por esta Seção 2(a)(4) nunca produz Material Adaptado.

   5. <u>Destinatários a jusante</u>.

      A. *<u>Oferta do Licenciador – Material Licenciado</u>. Cada destinatário do Material Licenciado recebe automaticamente uma oferta do Licenciante para exercer os Direitos Licenciados sob os termos e condições desta Licença Pública.*

B. *Oferta adicional do Licenciante – Material Adaptado.* *Cada destinatário do Material Adaptado seu recebe automaticamente uma oferta do Licenciante para exercer os Direitos Licenciados no Material Adaptado sob as condições da Licença do Adaptador que Você aplica.*

C. *Sem restrições downstream.* *Você não poderá oferecer ou impor quaisquer termos ou condições adicionais ou diferentes, ou aplicar quaisquer Medidas Tecnológicas Eficazes ao Material Licenciado, se isso restringir o exercício dos Direitos Licenciados por qualquer destinatário do Material Licenciado.*

6. Sem endosso. Nada nesta Licença Pública constitui ou pode ser interpretado como permissão para afirmar ou sugerir que Você está, ou que Seu uso do Material Licenciado está, conectado ou patrocinado, endossado ou concedido status oficial pelo Licenciador ou outros designados para receber atribuição conforme previsto na Seção 3(a)(1)(A)(i).

b. **Outros direitos.**

1. Os direitos morais, como o direito à integridade, não são licenciados sob esta Licença Pública, nem a publicidade, a privacidade e/ou outros direitos de personalidade semelhantes; no entanto, na medida do possível, o Licenciante renuncia e/ou concorda em não fazer valer quaisquer direitos detidos pelo Licenciante na medida limitada necessária para permitir que Você exerça os Direitos Licenciados, mas não de outra forma.
2. Os direitos de patentes e marcas registradas não são licenciados sob esta Licença Pública.
3. Na medida do possível, o Licenciante renuncia a qualquer direito de cobrar royalties de Você pelo exercício dos Direitos Licenciados, seja diretamente ou por meio de uma sociedade de gestão coletiva sob qualquer esquema de licenciamento obrigatório ou legal voluntário ou dispensável. Em todos os outros casos, o Licenciante reserva-se expressamente qualquer direito de cobrar tais royalties.

Seção 3 – Condições de Licença.

O exercício dos Direitos Licenciados está expressamente sujeito às seguintes condições.

a. **Atribuição.**

1. Se você compartilhar o Material Licenciado (inclusive na forma modificada), deverá:

A. reterá o seguinte se for fornecido pelo Licenciador com o Material Licenciado: identificação do(s) criador(es) do Material Licenciado e quaisquer outros designados para receber atribuição, de qualquer forma razoável solicitada pelo Licenciante (inclusive por pseudônimo, se designado); um aviso de direitos autorais;

i. um aviso referente a esta Licença Pública;
ii. um aviso que se refere à isenção de garantias;
iii. um URI ou hiperlink para o Material Licenciado na medida razoavelmente praticável;

B. indicar se Você modificou o Material Licenciado e reter uma indicação de quaisquer modificações anteriores; e

C. indica que o Material Licenciado está licenciado sob esta Licença Pública e inclui o texto, ou o URI ou hiperlink para esta Licença Pública.

2. Você pode satisfazer as condições da Seção 3(a)(1) de qualquer maneira razoável com base no meio, meio e contexto em que Você Compartilha o Material Licenciado. Por exemplo, pode ser razoável satisfazer as condições fornecendo um URI ou hiperlink para um recurso que inclua as informações necessárias.

3. Se solicitado pelo Licenciador, Você deverá remover qualquer informação exigida pela Seção 3(a)(1)(A) na medida razoavelmente praticável.

b. **ShareAlike.**

Além das condições da Seção 3(a), se você compartilhar material adaptado que você produz, as condições a seguir também se aplicam.

1. A licença do adaptador que você aplica deve ser uma licença Creative Commons com os mesmos elementos de licença, desta versão ou posterior, ou uma licença compatível com BY-SA.

2. Você deve incluir o texto ou o URI ou hiperlink para a Licença do Adaptador que Você aplica. Você pode satisfazer esta condição de qualquer maneira razoável com base no meio, meio e contexto em que você compartilha o Material Adaptado.

3. Você não pode oferecer ou impor quaisquer termos ou condições adicionais ou diferentes, nem aplicar quaisquer Medidas Tecnológicas Eficazes ao Material Adaptado que restrinja o exercício dos direitos concedidos sob a Licença do Adaptador que você aplica.

Seção 4 – Direitos Sui Generis sobre Banco de Dados.

Onde os Direitos Licenciados incluem Direitos de Banco de Dados Sui Generis que se aplicam ao Seu uso do Material Licenciado:

a. para evitar dúvidas, a Seção 2(a)(1) concede a Você o direito de extrair, reutilizar, reproduzir e compartilhar todo ou uma parte substancial do conteúdo do banco de dados;

b. se Você incluir todo ou uma parte substancial do conteúdo do banco de dados em um banco de dados no qual Você tem Direitos de Banco de Dados Sui Generis, então o banco de dados no qual Você tem Direitos de Banco de Dados Sui Generis (mas não seu conteúdo individual) é Material Adaptado, inclusive para fins da Seção 3(b); e

c. Você deverá cumprir as condições da Seção 3(a) se compartilhar todo ou uma parte substancial do conteúdo do banco de dados.

Para evitar dúvidas, esta Seção 4 complementa e não substitui Suas obrigações sob esta Licença Pública quando os Direitos Licenciados incluem outros Direitos Autorais e Direitos Similares.

Seção 5 – Isenção de Garantias e Limitação de Responsabilidade.

a. **A menos que de outra forma realizado separadamente pelo Licenciador, na medida do possível, o Licenciador oferece o Material Licenciado tal como está e conforme disponível, e não faz representações ou garantias de qualquer tipo em relação ao Material Licenciado, sejam expressas, implícitas, estatutárias ou outras . Isto inclui, sem limitação, garantias de título, comercialização, adequação a uma finalidade específica, não violação, ausência de defeitos latentes ou outros, precisão ou presença ou ausência de erros, conhecidos ou detectáveis ou não. Quando isenções de garantia não forem permitidas, no todo ou em parte, esta isenção de responsabilidade poderá não se aplicar a Você.**

b. **Na medida do possível, em nenhum caso o Licenciador será responsável perante Você em qualquer teoria legal (incluindo, sem limitação, negligência) ou de outra forma por quaisquer perdas diretas, especiais, indiretas, incidentais, consequenciais, punitivas, exemplares ou outras , custos, despesas ou danos decorrentes desta Licença Pública ou do uso do Material Licenciado, mesmo que o Licenciante tenha sido avisado da possibilidade de tais perdas, custos, despesas ou danos. Quando uma limitação de responsabilidade não for permitida, total ou parcialmente, esta limitação poderá não se aplicar a Você.**

c. A isenção de garantias e limitação de responsabilidade fornecidas acima devem ser interpretadas de uma maneira que, na medida do possível, se aproxime mais de uma isenção de responsabilidade absoluta e renúncia de toda responsabilidade.

Seção 6 – Vigência e Rescisão.

a. Esta Licença Pública se aplica pela vigência dos Direitos Autorais e Similares aqui licenciados. No entanto, se Você não cumprir esta Licença Pública, Seus direitos sob esta Licença Pública terminarão automaticamente.

b. Quando o Seu direito de usar o Material Licenciado for rescindido de acordo com a Seção 6(a), ele restabelecerá:

   [1.]

c. automaticamente a partir da data em que a violação for sanada, desde que seja sanada dentro de 30 dias após a descoberta da violação; ou

d. mediante reintegração expressa pela Licenciante.

   Para evitar dúvidas, esta Seção 6(b) não afeta nenhum direito que o Licenciador possa ter de buscar soluções para Suas violações desta Licença Pública.

e. Para evitar dúvidas, o Licenciante também poderá oferecer o Material Licenciado sob termos ou condições separados ou interromper a distribuição do Material Licenciado a qualquer momento; no entanto, isso não encerrará esta Licença Pública.

f. As Seções 1, 5, 6, 7 e 8 sobreviverão ao término desta Licença Pública.

Seção 7 – Outros Termos e Condições.

a. O Licenciante não estará vinculado a quaisquer termos ou condições adicionais ou diferentes comunicados por Você, a menos que expressamente acordado.

b. Quaisquer acordos, entendimentos ou acordos relativos ao Material Licenciado não declarados aqui são separados e independentes dos termos e condições desta Licença Pública.

Seção 8 – Interpretação.

a. Para evitar dúvidas, esta Licença Pública não reduz e não deve ser interpretada como reduzindo, limitando, restringindo ou impondo condições a qualquer uso do Material Licenciado que possa ser feito legalmente sem permissão sob esta Licença Pública.

b. Na medida do possível, se qualquer disposição desta Licença Pública for considerada inexequível, ela deverá ser automaticamente reformada na medida mínima necessária para torná-la exequível. Se a disposição não puder ser reformada, ela será separada desta Licença Pública sem afetar a aplicabilidade dos demais termos e condições.

c. Nenhum termo ou condição desta Licença Pública será renunciado e nenhum descumprimento será consentido, a menos que expressamente acordado pelo Licenciador.

d. Nada nesta Licença Pública constitui ou pode ser interpretado como uma limitação ou renúncia a quaisquer privilégios e imunidades que se apliquem ao Licenciador ou a Você, inclusive dos processos legais de qualquer jurisdição ou autoridade.