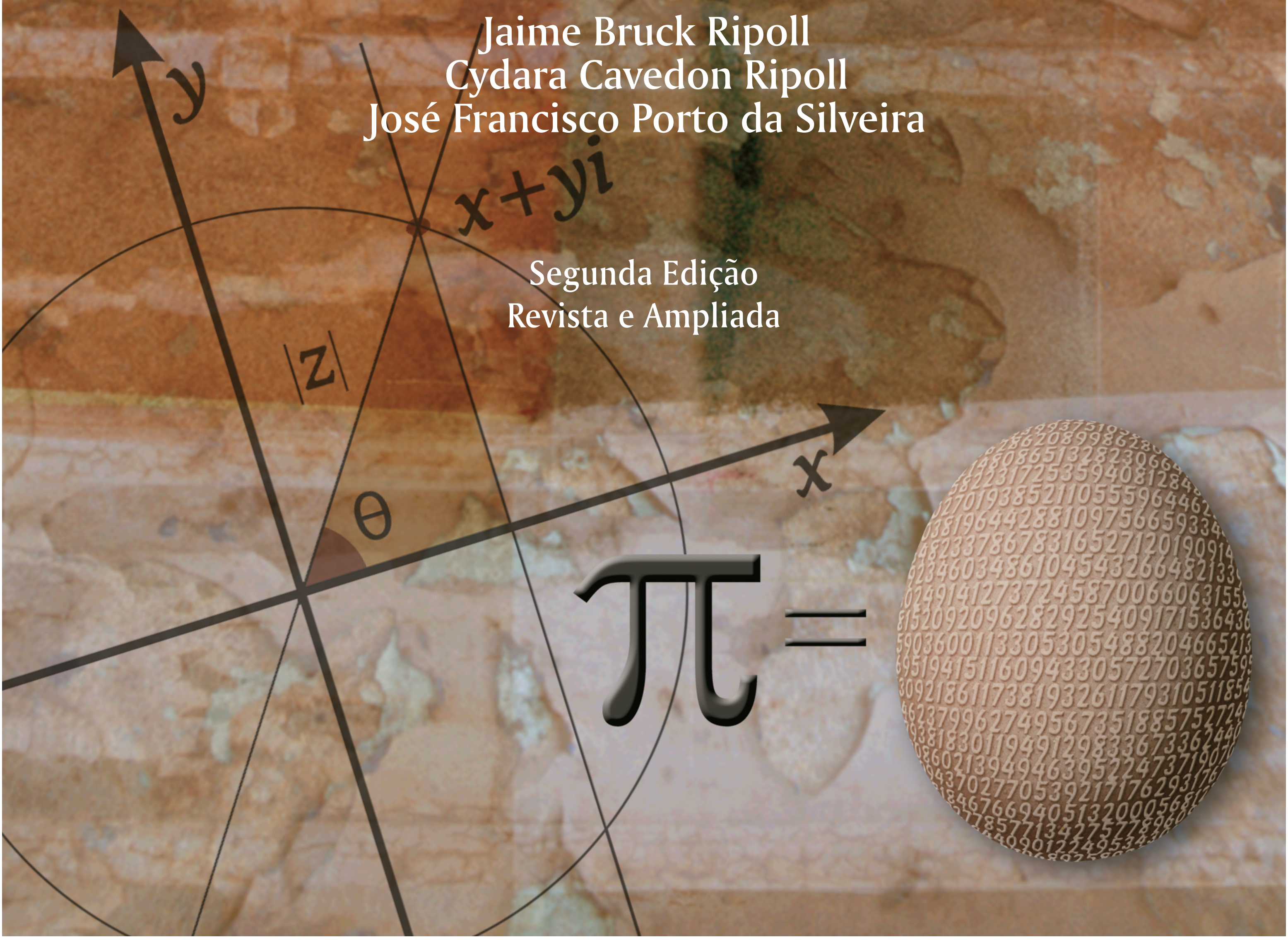
UFRGS
EDITORA

Números Racionais, Reais e Complexos

Jaime Bruck Ripoll
Cydara Cavedon Ripoll
José Francisco Porto da Silveira

Segunda Edição
Revista e Ampliada



Números Racionais, Reais e Complexos

Números Racionais, Reais e Complexos

Jaime Bruck Ripoll
Cydara Cavedon Ripoll
José Francisco Porto da Silveira

Segunda Edição
Revista e Ampliada

UFRGS
EDITORA

1ª edição: 2006

Capa: Vera Lucia Gliese, a partir de sugestão dos autores. Um dos destaques da capa é um ovo sobre o qual está escrita a parte inicial da expansão decimal de um dos mais notáveis números: o π. Esse número é uma fonte inesgotável de propriedades, algumas das quais são suficientemente elementares para serem abordadas num dos capítulos centrais deste livro.

Revisão: Ana Paula Anele Weber
Editoração eletrônica: Os autores e Observatório Gráfico

A grafia desta obra foi atualizada conforme o Acordo Ortográfico da Língua Portuguesa, de 1990, que entrou em vigor no Brasil em 1º de janeiro de 2009.

R592n Ripoll, Jaime Bruck
Números racionais, reais e complexos / Jaime Bruck Ripoll, Cydara Cavedon Ripoll e José Francisco Porto da Silveira. – 2. ed. rev. e ampl. – Porto Alegre: Editora da UFRGS, 2011.
528 p. : il. ; 21x25cm

Inclui figuras, gráficos, quadros e tabelas.

Inclui respostas e sugestões aos exercícios.

Inclui índice remissivo.

Inclui referências.

1. Matemática. 2. Campos numéricos – Números reais – Números complexos – Números hipercomplexos. 3. Matemática – Método dedutivo – Demonstrações matemáticas. 4. Reta euclidiana – Números racionais. 5. Método da régua decimal infinita – Número reais absolutos. 6. Teorema Fundamental da Geometria Analítica – Números reais – Operações aritméticas - Corpo algébrico. 7. Números reais – Natureza – Representações aritméticas e algébricas. 8. Números complexos – Representações geométricas e analíticas – Operações aritméticas e algébricas. 9. Primeiro Teorema Final da Aritmética. 10. Teoremas Fundamentais da Álgebra. 11. Números racionais – Expansão decimal. I. Ripoll, Cydara Cavedon, II. Silveira, José Francisco Porto da . III. Título.

CDU 511

CIP-Brasil. Dados Internacionais de Catalogação na Publicação.
(Jaqueline Trombin – Bibliotecária responsável CRB10/979)

ISBN 978-85-386-00128-9

Prefácio à primeira edição

Este livro trata de uma das mais básicas noções da Matemática: a noção de número. Os principais *campos numéricos*[1] que estudaremos neste livro são o dos *números reais* e o dos *números complexos*. O nível de nosso estudo não ultrapassa o do primeiro ano universitário e, mesmo assim, tivemos o especial cuidado de procurar torná-lo bastante autossuficiente no que toca a conhecimentos prévios.

O público-alvo deste livro são os alunos e professores de cursos de Licenciatura em Matemática. Ou seja, ele é mais voltado para a *formação de professores dos Ensinos Médio e Fundamental*. Contudo, ele também pode ser usado como fonte de consulta e subsídios por professores já lecionando nesses níveis de ensino.

Os conceitos, ideias e resultados associados aos campos dos números reais e complexos foram desenvolvidos ao longo de muitos séculos, durante os quais várias crises e controvérsias – conceituais e técnicas – precisaram ser enfrentadas pela comunidade matemática. Essas históricas dificuldades tinham uma força tão grande que muitas delas ainda sobrevivem sob a forma de vários tipos de erros e confusões, ainda bastante comuns nos livros de Matemática destinados ao Ensino Fundamental e Médio. O principal fator que motivou os autores a escreverem este livro foi exatamente o desejo de apontar e esclarecer essas dificuldades.

Este texto é fruto de longas discussões que os autores vêm tendo, já há três anos, sobre o ensino dos números reais e complexos ministrado aos alunos do Curso de Licenciatura em Matemática da Universidade Federal do Rio Grande do Sul (UFRGS). O mesmo foi testado e aperfeiçoado através de seu uso como livro-texto, durante cinco semestres, na disciplina Fundamentos da Matemática A, também na UFRGS.

Agradecemos aos colegas do Instituto de Matemática da UFRGS que nos últimos cinco semestres lecionaram as disciplinas de Matemática Elementar I e Fundamentos da Matemática A, bem como aos alunos do Curso de Licenciatura que estudaram versões preliminares deste texto e que contribuíram com sugestões.

Porto Alegre, outubro de 2005.
Os autores.

[1]Por “campo numérico” entendemos mais do que um conjunto de números. Entendemos um conjunto de números sobre os quais estão definidas operações e relações, tais como as operações aritméticas. Elas dão ao campo uma estrutura que pode ser algébrica, topológica ou de ordem. De um modo semelhante, um “espaço” é mais que um conjunto de pontos: tem de haver uma estrutura geométrica associada.

Prefácio à segunda edição

Além de ter sido feita uma revisão/correção da primeira edição deste livro, o mesmo também foi ampliado. Podemos resumir os principais pontos desta ampliação do seguinte modo:

- foi quase que dobrado o número de exercícios;
- no capítulo 2, sobre números inteiros, foram incluídas as demonstrações de todos os resultados mencionados, bem como ampliada a discussão sobre divisibilidade;
- foi feita uma discussão mais detalhada sobre a natureza dos números racionais, bem como sobre o significado intuitivo de suas operações aritméticas. De modo a tornar mais clara essa discussão, o capítulo 3 da primeira edição foi dividido em capítulos 3 e 4;
- o capítulo 7, sobre números reais, agora termina com uma demonstração completa e detalhada de que os mesmos formam um corpo ordenado arquimediano.

Como diz o título do livro, nosso grande objetivo é o estudo dos números racionais, reais e complexos, o que é feito a partir do capítulo 3. Assim, o capítulo 1 é uma introdução ao pensamento matemático, e o capítulo 2 deve ser visto mais como uma referência para resultados e conceitos de números inteiros que serão usados nos capítulos posteriores.

Porto Alegre, julho de 2010.
Os autores.

Uma panorâmica do conteúdo desta segunda edição.

Este livro pode ser dividido em três partes. De modo muito resumido, a primeira parte consiste de uma introdução ao pensamento matemático, a segunda tem como principal objetivo o estudo do campo dos números reais, e a terceira parte estuda o dos números complexos. Vejamos um pouco mais de detalhes.

Primeira parte

Consiste no Capítulo 1: Introdução ao Pensamento Matemático. Ela tem como grande objetivo dar ao aluno que está começando seus estudos universitários de Matemática uma iniciação sólida e concreta ao método de argumentação usado nesta disciplina: o método dedutivo. São explicados, comparados e exemplificados todos os tipos usuais de demonstrações matemáticas.

Segunda parte

É formada pelos Capítulos 2 a 8, ao longo dos quais são estudados, sucessivamente, os campos dos números inteiros, dos racionais, dos números reais absolutos e dos números reais.

O Capítulo 2 resume-se a uma breve revisão dos principais resultados, sobre números inteiros, que serão usados em demonstrações feitas nos capítulos seguintes.

O primeiro passo em direção aos números reais é dado no Capítulo 3, onde os números racionais são introduzidos e estudados sob um ponto de vista adequado para a construção dos números reais absolutos. Essa introdução é seguida pelo Capítulo 4, no qual é feito um estudo bastante detalhado e preciso da expansão decimal dos números racionais.

O Capítulo 5 tem um caráter intermediário. Com efeito, no mesmo, é feito um estudo da continuidade da reta euclidiana (Postulado do Contínuo e consequências). Isso nos permitirá entender a necessidade de ampliar o conjunto dos números racionais para, assim, ficarmos capazes de expressar a medida exata de qualquer segmento da reta euclidiana.

No Capítulo 6 aborda-se o problema da medição de um segmento qualquer da reta euclidiana. Usando-se uma idealização e generalização natural da familiar régua decimal utilizada no Ensino Elementar, introduzimos o que chamaremos de *método da régua decimal infinita,* método que nos permitirá introduzir os *números reais absolutos.*

No Capítulo 7, por meio do problema da determinação de coordenadas para pontos da reta euclidiana, realizamos o grande objetivo de introduzir os números reais. Demonstra-se aí o Teorema Fundamental da Geometria Analítica, o qual estabelece a existência de uma correspondência biunívoca entre os pontos da reta euclidiana e os números reais. Conclui-se este capítulo com as definições de operações aritméticas entre números reais, e mostra-se que este campo numérico fica assim munido de uma estrutura algébrica de *corpo.*

O Capítulo 8 procura fazer um estudo inicial da natureza dos números reais, investigando as relações entre a sua enorme quantidade e a complexidade de suas representações aritméticas e algébricas.

Terceira parte

É formada pelos Capítulos de 9 a 11, ao longo dos quais são construídos e estudados os números complexos e generalizações.

O Capítulo 9 generaliza os números reais introduzindo os *números complexos*, suas representações geométricas e analíticas (exceto as representações trigonométricas e exponencial, que necessitam do conhecimento das funções trigonométricas e exponencial), bem como suas operações aritméticas e algébricas. Em particular, mostra-se que, novamente, estamos diante de um campo numérico que tem a estrutura de corpo.

Um dos cuidados que tivemos na redação deste capítulo foi o de apontar os reais acontecimentos que motivaram a introdução dos números complexos, bem como os problemas que precisaram ser resolvidos até que eles passassem a ser aceitos sem reservas pela comunidade matemática.

O Capítulo 10 tem dois grandes objetivos. O primeiro é o de mostrar que, sob o ponto de vista aritmético, não é preciso ampliar o campo dos números complexos, pois ele é plenamente suficiente para dar sentido a todas as operações aritméticas racionais, algébricas irracionais e às operações transcendentais elementares. A precisa caracterização dessa suficiência constitui o chamado *Primeiro Teorema Final da Aritmética.*

O segundo grande objetivo deste capítulo é investigar as relações entre os campos numéricos, os polinômios e as raízes das equações polinomiais. Mostra-se que a plenitude da simplicidade e utilidade dessas relações realiza-se no campo dos números complexos. Essa descoberta é sintetizada através de um importantíssimo grupo de teoremas assemelhados e que são todos chamados de *Teorema Fundamental da Álgebra.*

O Capítulo 11, apesar do "freio" imposto pelo Primeiro Teorema Final da Aritmética, procura investigar a possibilidade de existirem campos numéricos ainda mais gerais do que o dos complexos, e ainda com propriedades úteis. A mais natural dessas generalizações é a dos *números hipercomplexos*, a qual é aqui introduzida e estudada. Apesar de esses campos numéricos não mais terem a estrutura de corpo, eles nos permitem entender melhor a importância dos números complexos, bem como identificar claramente as propriedades estruturais que viabilizam a existência dos teoremas fundamentais da Álgebra.

Encadeamento dos capítulos do livro

Como o Capítulo 1 é uma introdução geral ao pensamento matemático, a leitura do mesmo pode ser substituída por consultas oportunas enquanto estuda-se os outros. Os demais capítulos seguem uma ordenação linear: o estudo de um exige o estudo dos anteriores, com uma única exceção: o Capítulo 8 não é necessário para a compreensão dos Capítulos 9, 10 e 11.

Estrutura dos capítulos do livro

Os onze capítulos do livro têm uma estrutura semelhante. Cada um inicia com um índice do mesmo e continua com o texto propriamente dito: motivações, definições, teoremas, demonstrações, exemplos, etc. Em cada capítulo há uma profusão de exercícios propostos ao leitor, os quais são apresentados à medida que o texto vai sendo desenvolvido. Alguns capítulos trazem uma ou mais seções que chamamos de *Leitura complementar*, e que são textos de leitura não obrigatória que procuram aprofundar alguma ideia ou técnica abordada.

Sumário

CAPÍTULO 1

INTRODUÇÃO AO PENSAMENTO MATEMÁTICO

1.1 Em Matemática, não basta intuir, não basta testar: é preciso demonstrar

Nos tempos atuais, estima-se que mais de 100.000 novos resultados matemáticos são publicados anualmente. Esses resultados podem ser de vários tipos: propriedades e classificações de objetos matemáticos, novos métodos e algoritmos, etc. Cada um desses resultados é fruto de um trabalho que envolve duas etapas: a heurística e a demonstração.

A heurística consiste no trabalho de descoberta dos resultados matemáticos. Usando-se casos particulares, fazendo-se analogias, simulações, ou mesmo usando-se simplesmente nossa experiência e intuição, produzimos ou enunciamos (prefere-se usar a expressão "intuímos") o que chamamos usualmente de *conjectura*: a afirmação de um resultado matemático do qual temos alguma evidência da veracidade, mas não a certeza. Dizendo de um outro modo: embora estejamos até dispostos a apostar na veracidade da afirmação feita por uma conjectura, estamos bem cientes de que há um risco de que a mesma corresponda a um resultado falso.

Uma vez que intuímos uma conjectura, passa-se à sua *demonstração*. Essa objetiva dar condições para que tanto a pessoa que intuiu a conjectura, como a qualquer outra pessoa, convença-se de modo indubitável da sua veracidade ou, se for o caso, da sua falsidade.

O produto da demonstração é o que chamamos prova. Toda prova que demonstre a *veracidade* de uma dada conjectura consiste num *encadeamento de deduções* que mostram que o resultado afirmado pela conjectura é uma consequência lógica e irrefutável de resultados matemáticos já aceitos como verdadeiros. Por outro lado, uma prova que demonstre a *falsidade* de uma conjectura resume-se, em geral, na exibição de um *contraexemplo*, ou seja, na exibição de uma situação particular (exemplo) onde o que é afirmado pela conjectura não ocorre.

Uma conjectura que tenha sido demonstrada ser verdadeira passa a ter o status de teorema, de verdade matematicamente demonstrada. Por outro lado, chamamos de *conjectura falsa* a toda conjectura que tenha sido demonstrada não ser verdadeira.

Exemplo 1.1 *(uma conjectura que se revelou falsa)*

Procurando grandes números primos, o famoso matemático Pierre de Fermat, por volta de 1640, estudou os inteiros da forma:

$$P(n) = 1 + 2^{(2^n)}.$$

Com muito trabalho, pois naquela época os cálculos eram feitos na base de lápis e papel, ele verificou que

$$P(0) = 3,\ P(1) = 5,\ P(2) = 17,\ P(3) = 257,\ P(4) = 65\,537$$

são primos, o que lhe inspirou a conjecturar que $P(n)$ é um número primo para os infinitos casos $n \in \{0, 1, 2, \dots\}$.

Foram precisos mais de cem anos para que outro grande matemático, Leonhard Euler, mostrasse que, na verdade, $P(5)$ *não é primo, refutando, ou falsificando, assim, a Conjectura de Fermat:*

$$P(5) = 1 + 2^{32} = 4\,294\,967\,297 = 641 \times 6\,700\,417\,.$$

O leitor pode ter achado que a razão de a conjectura anterior ter levado cerca de 100 anos para ser resolvida tenha sido a pequena importância da mesma. Não necessariamente! O exemplo seguinte trata de uma conjectura que, apesar de ter se revelado muito importante para os rumos da Matemática, foi ainda mais resistente que a anterior:

Exemplo 1.2 *A Conjectura de Fermat (uma conjectura que virou teorema)*

O mesmo Pierre Fermat, em 1637, ao estudar as equações

$$x + y = z, \quad x^2 + y^2 = z^2, \quad x^3 + y^3 = z^3, \quad x^4 + y^4 = z^4, \ldots ,$$

onde as incógnitas x, y *e* z *podem assumir apenas valores inteiros positivos*[1]*, constatou que a primeira equação tem muitas soluções, que a segunda tem bem menos (apesar de ainda serem em número infinito) e que não há nenhuma solução no terceiro e quarto caso. Com isso, ele conjecturou que:*

não existem soluções inteiras positivas para $x^n + y^n = z^n$, se $n \geqslant 3$.

Mesmo após o esforço de muitos dos maiores matemáticos de todos os tempos, passaram-se 356 anos até que o inglês Andrew Wiles, em 1993, conseguiu demonstrar a veracidade dessa conjectura.

Tanto o tempo que se precisou para se chegar à demonstração da veracidade da Conjectura de Fermat, como as milhares de páginas ocupadas pela respectiva prova, servem magnificamente bem para mostrar o quão grande pode ser a distância entre a descoberta de um resultado e a demonstração de sua veracidade.

Também é importante observarmos que, na tentativa de demonstrar a Conjectura de Fermat, os matemáticos desenvolveram uma significativa quantidade de ideias e resultados que serviram não apenas para fertilizar muitos campos da Matemática,

[1] O "positivo" tem origem geométrica: dividir um quadrado na soma de dois quadrados, um cubo na soma de dois cubos, etc. Problema que foi originalmente estudado, caso dos quadrados, pelo matemático Diophantos de Alexandria, c. 300 dC.

como também foram aplicados na produção de tecnologias que o cidadão moderno utiliza no seu viver diário, como é o que ocorreu com alguns métodos de criptografia (codificação e decodificação de senhas, assinaturas e mensagens). O leitor interessado poderá ler mais sobre essa conjectura e sua prova no livro de Simon Singh, O último teorema de Fermat*, da Editora Record.*

Nos dois exemplos anteriores apresentamos conjecturas que finalmente foram resolvidas. No entanto, existem muitas conjecturas que há muito tempo continuam ainda não resolvidas, ou em aberto. Uma das mais famosas delas é a seguinte:

Exemplo 1.3 *A Conjectura de Goldbach (uma conjectura ainda em aberto).*

Christian Goldbach, em 1742, afirmou:

> Todo número inteiro par $\geqslant 4$ pode ser escrito como a soma de dois números primos, possivelmente iguais.

Usando-se computadores modernos, a veracidade dessa conjectura foi comprovada desde o inteiro 4 até 10^{18} (julho de 2 008). Contudo, ainda não existe uma prova que ateste de fato sua veracidade nos outros infinitos casos.

Recentemente, foi oferecido um prêmio de 1 milhão de dólares a quem for capaz de resolvê-la, demonstrando sua veracidade ou apresentando um contraexemplo que prove sua falsidade. O leitor interessado em saber mais detalhes sobre esta conjectura pode ler o fascinante livro Tio Petros e a conjectura de Goldbach*, de Apostolos Doxiadis.*

Embora transcendendo em muito os propósitos e nível deste texto, não podemos deixar de comentar que, em 1930, o matemático Kurt Gödel demonstrou um resultado tremendamente perturbador, no qual afirma que existem conjecturas matemáticas, perfeitamente legítimas e até naturais, para as quais é impossível se chegar a uma demonstração, seja de sua veracidade, seja de sua falsidade. Podemos dizer que Gödel provou que existem conjecturas que ficarão eternamente em aberto. Esse resultado é conhecido como *Teorema da Incompletude de Gödel* e é tido como uma das mais profundas e brilhantes conquistas intelectuais já feitas pela Humanidade. Felizmente, esses impasses são raros em Matemática e o leitor não deve se inquietar com eles, principalmente em assuntos elementares, como o do presente texto.

O principal objetivo dessa seção é insistir que, por maior que seja o talento e autoridade científica de quem intuiu uma conjectura, por maior que seja a quantidade de pessoas que pensem que a mesma é verdadeira, por maior que seja o trabalho gasto na heurística que a produziu, a mesma continuará incompleta – sem o direito de ser incorporada ao corpo dos conhecimentos matemáticos e de usufruir do status *teorema* – se não estiver acompanhada de uma prova que permita a qualquer pessoa "matematicamente alfabetizada" convencer-se de modo indubitável da sua veracidade. Dizendo de outro modo: *enquanto não nos for exibida uma prova para uma conjectura dada, devemos ter em mente que existem tanto chances de ela ser verdadeira como de ser falsa.* A exigência de demonstração é característica essencial, inegociável, da Matemática.

Nossa insistência em lembrar que faz parte do protocolo oficial da Matemática o hábito de demonstrar tudo o que se afirme tem cabimento na medida em que já são minoria os livros de Matemática Elementar que trazem demonstrações. Mais do que isso, o ensino voltado para o vestibular e suas questões de múltipla escolha estimula a heurística da esperteza, ao invés de desenvolver o pensamento científico.

Por outro lado, também queremos deixar claro que não nos incluímos entre os matemáticos que negam qualquer mérito à heurística, a ponto de dizerem que *um resultado matemático pertence a quem o demonstra e não a quem o descobre.* Estamos apenas insistindo que, frente à atual realidade educacional, não podemos deixar de ter em mente que, como diz o título desta seção, *em Matemática não basta intuir: é preciso demonstrar*!

Exercício 1 -

Intua um padrão geral sugerido pelas igualdades

$$5^2 - 5 = 4^2 + 4$$
$$7^2 - 7 = 6^2 + 6.$$

A seguir responda: o padrão que você intuiu é uma afirmação falsa ou verdadeira? Por quê?

Exercício 2 -

Idem exercício anterior, considerando as igualdades

$$(20 + 25)^2 = 2025$$
$$(30 + 25)^2 = 3025.$$

1.2 Em Matemática, demonstrar não é o mesmo que verificar muitos casos

A Matemática destaca-se entre as demais ciências por ter um alto padrão de rigor. Em particular, ao demonstrarmos a veracidade de uma conjectura matemática, esse padrão de rigor exige que sejam examinados todos os casos particulares envolvidos na mesma.

A experiência nos mostra que os vícios trazidos do Ensino Elementar fazem com que haja uma forte tendência de os alunos de graduação não obedecerem a esse padrão de rigor. Isso é especialmente verdadeiro no caso da demonstração de afirmações que podem ser vistas como uma lista de afirmações particulares, como é o que ocorre nos seguintes exemplos:

Exemplo 1.4 -

É par qualquer número do conjunto $\{10,\ -234,\ 4578,\ 1200\}$.

Exemplo 1.5 -

$n^2 - n + 41$ *é um número primo, para qualquer número natural* n.

Exemplo 1.6 -

n^2 *é um número par, para qualquer número inteiro par* n.

Exemplo 1.7 -

$n^2 - n + 10$ *é um número par, para qualquer número natural* n.

Podemos classificar esses exemplos em dois tipos: afirmações com quantidade finita de casos particulares e afirmações com quantidade infinita de casos. O primeiro exemplo encaixa-se no tipo finito (tem apenas quatro casos particulares), enquanto os demais correspondem a afirmações que valeriam uma infinidade de vezes (ou para todos os números naturais ou para todos os números pares) e que, portanto, são do segundo tipo.

Nas afirmações envolvendo um número finito de casos, a demonstração da veracidade pode ser feita demonstrando cada um deles em separado, ou em grupos. Exemplifiquemos.

– *Demonstração do valor lógico da afirmação do exemplo* 1.4.

Lembrando que número par é todo inteiro múltiplo de 2 e que

$$\begin{aligned} 10 &= 2 \times 5 \\ -234 &= 2 \times (-117) \\ 4578 &= 2 \times 2289 \\ 1200 &= 2 \times 600, \end{aligned}$$

podemos concluir que a afirmação do exemplo 1.4 é verdadeira. CQD.

A demonstração de afirmações envolvendo um número finito de possibilidades feita através da comprovação caso a caso é basicamente uma questão de paciência, embora matematicamente legítima. Por outro lado, essa estratégia é, obviamente, inviável quando procuramos atender à exigência de verificação de todos os casos das afirmações envolvendo um universo de infinitas possibilidades. Esses tipos de afirmações são comuns em Matemática e o encontramos nos três últimos exemplos. Vejamos a orientação geral para se proceder nesses casos.

– *Decisão do valor lógico da afirmação do Exemplo* 1.5.

Os vícios trazidos da escola tornam comuns pseudo demonstrações do tipo:

> *"A afirmação é válida, pois por exemplo,*
> $1^2-1+41=41$, $\quad 2^2-2+41=43$, $\quad 3^2-3+41=47$,
> $4^2-4+41=53$, $\quad 5^2-5+41=61$, $\quad 6^2-6+41=71$,
> $7^2-7+41=83$ $\quad$ *são todos números primos."*

Mesmo correndo o risco de esgotar a paciência do leitor, insistimos que um argumento desse tipo *não serve como demonstração* da veracidade desta afirmação, já que a comprova apenas para um número finito de valores de n, enquanto n varia no conjunto infinito de todos os números naturais.

Reiteramos que *argumentos experimentais sempre correm o risco de produzirem conclusões falsas.* É exatamente isso o que ocorre no presente exemplo pois, embora se possa mostrar que de $n = 1$ até $n = 40$, o número $n^2 - n + 41$ sempre é primo, tal primalidade é falsa para $n = 41$. Com efeito: $41^2 - 41 + 41 = 41 \cdot 41$. CQD.

> Ainda insistindo, chamamos a atenção do leitor para o fato de que a pseudo demonstração anteriormente citada *continuaria sendo não aceita mesmo que a afirmação da conjectura fosse verdadeira*, e não falsa como ocorreu. Faz parte dos valores da Matemática aceitar apenas demonstrações que examinam *todos* os casos particulares da afirmação envolvida.

No Exemplo 1.5 a demonstração foi de *falsidade* da conjectura e, assim, bastou dar um contraexemplo, o correspondente ao caso particular $n = 41$. Fica, então, a pergunta: como demonstrar a *veracidade* de uma conjectura envolvendo a afirmação de uma infinidade de casos? Resposta: ou descobrindo algum argumento genérico que seja aplicável a qualquer uma das infinitas possibilidades de n, ou achando algum artifício para reduzir o universo das infinitas possibilidades a um número finito de famílias de casos, cada uma das quais podendo ser examinada genericamente. Ilustramos isto a seguir, demonstrando a veracidade dos Exemplos 1.6 e 1.7.

– *Decisão do valor lógico da afirmação do Exemplo* 1.6.

Sendo n um inteiro par, podemos escrevê-lo na forma $n = 2k$, com k inteiro. Daí,

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)\,.$$

Como $2k^2$ é ainda um inteiro, a igualdade

$$n^2 = 2(2k^2)$$

nos permite concluir que n^2 é par. Logo, a afirmação do Exemplo 1.6 é verdadeira. CQD.

Exercício 3 -

Prove que se n é um inteiro ímpar, então n^2 também é ímpar.

– *Decisão do valor lógico da afirmação do Exemplo* 1.7.

Dividamos o problema em dois casos possíveis:

Caso 1: n é um natural par.
Pelo Exemplo 1.6 , sabemos que n^2 é par. Deixamos ao leitor o exercício de mostrar que, então, $n^2 - n$ é par.

Caso 2: n é ímpar.
Pelo Exercício 3, sabemos que n^2 é ímpar. Deixamos ao leitor o exercício de mostrar que também aqui $n^2 - n$ é par.

Provamos assim que, em qualquer caso, $n^2 - n$ é um número par, digamos,

$$n^2 - n = 2k\,,$$

com k inteiro. Daí:

$$n^2 - n + 10 = 2k + 10 = 2(k+5)\,,$$

e como $k+5$ é também inteiro, concluímos que, em qualquer caso, $n^2 - n + 10$ é par. Fica assim demonstrado que a afirmação do Exemplo 1.7 é verdadeira.

Antes de encerrarmos esta seção, precisamos chamar a atenção do leitor para o fato de que as ciências naturais (como é o caso da Física, Química e Biologia) aceitam como demonstração da veracidade de uma afirmação a comprovação de uma quantidade finita de casos particulares da mesma. Por isso, dizemos que essas ciências são *empíricas*. Diferentemente, a Matemática não é uma ciência empírica!

A Matemática tem um padrão de rigor muito superior ao das ciências empíricas. Em particular, ela não aceita demonstrações que se resumem à verificação de milhões de possibilidades, se ficar faltando a demonstração de um único caso que seja, pois este caso pode tornar a afirmação falsa. É essencial que o leitor entenda que em Matemática o exame de uma quantidade de casos, mesmo que enorme, tem no máximo um valor heurístico, se este exame não envolver todos os casos.

Resumindo:

- Em afirmações com um número *finito* de possibilidades, temos duas estratégias de demonstração: ou usamos um argumento genérico, ou testamos TODAS as possibilidades.
- Em afirmações com um número *infinito* de possibilidades, temos que recorrer a um raciocínio que não dependa de casos particulares, ou seja, somos obrigados a usar um raciocínio genérico.

TESTAR ALGUMAS *ou mesmo* MUITAS *possibilidades* de uma afirmação matemática *não é* DEMONSTRAR.

Exemplo 1.8 -

É verdade que $d(p) = 2^{p-1} - 1$ *nunca é divisível por* p^2*, se* p *for um número primo?*

Esta pergunta foi feita pelo russo D. A. Grave. Constata-se que a resposta é afirmativa até $p = 1091$*. Apesar disso,* $d(1093)$ *é divisível por* 1093^2.

Exemplo 1.9 -

É verdade que o valor

$$P(n) = 1 + 991n^2$$

nunca é um quadrado, qualquer que seja $n \in \{1, 2, \dots\}$*?*

A resposta é afirmativa para uma enormidade de casos: até

$$n_0 = 12\ 055\ 735\ 790\ 331\ 359\ 447\ 442\ 538\ 766 \cong 12 \times 10^{27}.$$

Contudo, o valor seguinte de n *já dá* $P(n)$ *um quadrado perfeito:*

$$\begin{aligned} &P(n_0 + 1) \\ &= 144\ 032\ 698\ 557\ 259\ 999\ 607\ 886\ 110\ 560\ 755\ 362\ 973\ 171\ 476\ 419 \\ &973\ 199\ 366\ 400 \\ &= (379\ 516\ 400\ 811\ 930\ 638\ 014\ 896\ 080)^2\,. \end{aligned}$$

1.3 Conceitos lógicos básicos e notações

Pode-se dizer que, até aqui, nos preocupamos mais em alertar o leitor acerca do que *não é permitido fazer* em Matemática, do que realmente ensinar a pensar matematicamente. O objetivo do restante deste capítulo é enfrentar parcialmente essa deficiência.

Antes de mais nada, é importante entender o porquê do *parcialmente* que foi usado no parágrafo anterior. Para isso, lembramos que já foi colocado que o trabalho da produção de resultados matemáticos envolve duas etapas: a heurística (que é uma etapa de descoberta) e a demonstração (que é uma etapa que comprova a veracidade ou a falsidade da conjectura descoberta na heurística). A experiência de milhares de anos de ensino da Matemática mostra que o aprendizado e desenvolvimento da heurística precisam ser feitos em campos específicos da Matemática (como Geometria, Álgebra etc.) e é difícil transportá-la de um campo para outro. Por isso, sendo este capítulo uma introdução geral ao pensamento matemático, aqui enfrentaremos apenas a segunda etapa: trataremos somente da demonstração.

Na verdade, este capítulo é ainda mais restritivo, pois tratará meramente de *parte* da etapa da demonstração. Com efeito, podemos dividir a tarefa de demonstração de uma conjectura em duas partes: a concepção da demonstração (um trabalho também de natureza heurística e que nos permite conceber uma seqüência de pequenos passos formando um caminho que nos leva até a verdade que se procura defender) e a redação da prova (que corresponde ao trabalho detalhado, cuidadoso e sistemático da escritura do encadeamento de argumentos cujas linhas mestras foram concebidas anteriormente).

A etapa da concepção da demonstração é uma arte de criar caminhos, sendo muito dependente de talento inato e da experiência que se acumula com o estudo a fundo de cada campo matemático. Em particular, é uma arte difícil de se ensinar. Por outro lado, a etapa da redação da prova tem uma natureza bem mais mecânica ou técnica, e é dela que nos limitaremos a tratar no que se segue.

É importante que o leitor entenda que é necessário dominar perfeitamente a etapa da redação de uma prova, pois é este domínio que lhe vai permitir tanto ler provas escritas por outras pessoas (como as que encontrará neste ou em outros livros que terá de estudar) como de iniciar a escrever suas próprias provas. Contudo, também é importante alertar que o domínio da técnica da redação, embora possibilite o leitor a desenvolver as provas matemáticas mais rotineiras, não é garantia de que possa vir a desenvolver uma prova matemática mais interessante ou inovadora. É algo semelhante ao que ocorre com qualquer linguagem humana: o conhecimento de vocabulário e gramática é uma necessidade, mas não é suficiente para garantir que, só com isso, alguém se torne capaz de escrever lindas poesias.

Passemos, enfim, ao estudo da mecânica da redação de provas matemáticas. Os aspectos básicos desse estudo formam o que se chama Lógica Matemática. Esta, corresponde ao que poderíamos chamar de *gramática da Matemática*. Como toda gramática, ela envolve conceitos formulados de uma maneira bastante precisa e abstrata, bem como uma notação especializada. Essas características costumam ser pontos dificultadores do aprendizado, a ponto de poderem ofuscar totalmente o verdadeiro significado do que se está estudando. Na verdade, esse é um fenômeno que ocorre no estudo de qualquer tipo de gramática. O que podemos fazer é minimizar o problema, usando, na medida do possível, uma abordagem menos abstrata.

– Proposições

Iniciamos introduzindo uma das noções mais básicas da Lógica, a de proposição. Essa noção nos permitirá conceituar mais rigorosamente as noções de conjectura e teorema.

Definição 1.10 -

Uma proposição, em Lógica e Matemática, é uma afirmação ou declaração que tem um valor lógico, i.e., é possível dizermos se ela é verdadeira *(V) ou* falsa *(F).*

Exemplo 1.11 -

São exemplos de proposições:

i). Pelé foi jogador profissional de basquete.
ii). 28 é número par.
iii). O triângulo é uma figura plana.
iv). Para todo $x \in \mathbb{N}$, o algarismo da unidade de x^2 é igual ao de x.

Não são proposições as seguintes afirmações:

v). 2^4. *(nada afirmo)*
vi). $x = 3$. *(não sei quem é x, logo não posso decidir)*
viii). $m < n$.
ix). $2 < \sqrt{3}$? *(pergunta não é afirmação)*

> Em Matemática, uma proposição nunca pode ser verdadeira e falsa ao mesmo tempo. Ou seja, tem exatamente um valor lógico. O que pode ocorrer é que seu valor lógico ainda não seja conhecido. Exemplo: "a maior raiz de $x^5 - x + 1 = 0$ é $x = 3$".

Notação:
Costumamos representar as proposições por letras latinas minúsculas:

p : Pelé foi jogador profissional de basquete
q : 28 é par
r : $2 > 3$

Em Matemática, as proposições verdadeiras podem receber o nome de postulados, axiomas, lemas, proposições, teoremas ou corolários.

Os axiomas ou postulados (atualmente, estas denominações são consideradas sinônimas) constituem os "alicerces" de cada teoria matemática, e, por serem seu ponto de partida, são indemonstráveis. São aceitos sem qualquer demonstração.

Exemplo 1.12 -

"Por dois pontos distintos passa uma e somente uma reta" é um famoso axioma (postulado) da Geometria Euclidiana.

Já os lemas, proposições, teoremas e corolários são afirmações verdadeiras que têm de ser acompanhadas de uma demonstração atestando sua veracidade. O raciocínio envolvido em tal demonstração tem de se apoiar exclusivamente em conceitos e resultados já aceitos como verdadeiros, incluindo possivelmente os axiomas (ou postulados).

– Sentenças abertas

Vamos agora nos concentrar em um outro tipo de afirmação que encontramos em Matemática. Para isso, iniciemos notando que sentenças da forma

$$\begin{array}{l} x = 3, \\ x + y \leq 5, \\ T \text{ é um triângulo equilátero,} \\ 2x + 1 = 3, \\ m < n \end{array}$$

não são proposições! Contudo, podemos observar que se dermos valores numéricos para x, y, m e n, ou se subtituirmos T por um triângulo específico, elas se tornam proposições. Os símbolos x, y, T, m e n são por isso chamados variáveis, e sentenças desse tipo são chamadas sentenças abertas.

Definição 1.13 -

Sentença aberta é toda afirmação contendo uma ou mais variáveis e que é tal que fica com veracidade determinável – se transforma em proposição – cada vez que dermos um "valor" à sua variável, ou às suas variáveis.

Notação:

. $p(x), q(T), p(y)$ são notações que indicam sentenças abertas envolvendo uma variável (respectivamente: x, T, y)

. $p(x, y), q(x, z)$ são notações indicando sentenças abertas com duas variáveis (respectivamente: x, y e x, z)

Exemplo 1.14 -

São exemplos de sentenças abertas:

$$\begin{array}{l} \textit{do tipo } p(x): \; x+1=2 \\ \textit{do tipo } p(x,y): \; x+y \leqslant 5 \end{array}$$

Todo valor da variável (ou das variáveis) de uma sentença aberta que a transforma numa proposição verdadeira é dito *satisfazer a sentença.*

Exemplo 1.15 -

Equações são um tipo importante de sentença aberta. Assim, a equação "$x^2-1=0$" é uma sentença aberta que é satisfeita apenas pelos valores $x=1$ e $x=-1$, os quais são chamados de suas raízes.

Exemplo 1.16 -

Com relação às sentenças abertas do Exemplo 1.14:

$$\begin{array}{l} 1 \textit{ satisfaz } p(x), \textit{ pois é verdade que } 1+1=2; \\ \textit{o par } (2,3) \textit{ satisfaz } p(x,y), \textit{ pois } p(2,3): \; 2+3=5 \leqslant 5 \textit{ é } V. \end{array}$$

– Proposições quantificadas:

Em Matemática, é muito comum precisarmos tratar de uma proposição sobre a veracidade de um bloco, ou conjunto, de proposições associadas a uma dada sentença aberta. Mais precisamente, tal proposição afirma a veracidade de uma certa quantidade de proposições do bloco. Por isso, este tipo de proposição é dito ser uma proposição quantificada. Vejamos um exemplo inicial.

Consideremos a sentença aberta $p(x): \; x-3>0$. Denotando por X o conjunto dos inteiros positivos, consideremos o bloco das proposições correspondentes a cada valor de $x \in X$, ou seja:

$$1 - 3 > 0, 2 - 3 > 0, 3 - 3 > 0, 4 - 3 > 0, \ldots$$

Para este bloco, podemos formar quatro proposições quantificadas:

- "para cada $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição falsa, pois $1 - 3 < 0$)
- "para ao menos um $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição verdadeira, pois $4 - 3 > 0$)
- "para exatamente um $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição falsa, pois $4 - 3 > 0$ e $5 - 3 > 0$)
- "para nenhum $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição falsa, pois, por exemplo, $4 - 3 > 0$)

Se escolhermos outro X (ou seja, outro bloco de proposições) teremos outras quatro proposições quantificadas, a partir da mesma sentença aberta. Por exemplo, se $X =$ conjunto dos inteiros pares e $\geqslant 4$, temos:

- "para cada $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição verdadeira, pois $4 - 3 = 1 > 0, 6 - 3 = 3 > 0, \ldots$)
- "para ao menos um $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição verdadeira, pois $4 - 3 = 1 > 0$)
- "para exatamente um $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição falsa, pois $4 - 3 > 0$ e $6 - 3 > 0$)
- "para nenhum $x \in X$, é verdade que vale $x - 3 > 0$"
  (a qual é uma proposição falsa, pois $4 - 3 > 0$)

Definição 1.17 -

Dada uma sentença aberta, selecionemos um conjunto de valores para sua variável (ou suas variáveis), o qual chamaremos de universo. *Com estes valores, formemos o bloco (ou conjunto) das proposições associadas pela sentença. Assim feito, chamamos de* **proposição quantificada** *qualquer proposição que afirme a veracidade de uma certa quantidade*[2] *de proposições do bloco.*

[2] Todos, alguns, exatamente um e nenhum são as escolhas usuais desta quantidade.

Dada sentença uma aberta, $p(x)$
$\downarrow$
escolho um universo X de valores para x
$\downarrow$
formo o bloco das proposições $p(x)$, $x \in X$
$\downarrow$
formulo uma PROPOSIÇÃO QUANTIFICADA para o bloco, ou seja: uma afirmação sobre a VERACIDADE de uma certa quantidade de proposições do bloco.

De modo que o bloco das proposições de uma proposição quantificada seja escrito mais rapidamente (ou seja, sem ter de listar individualmente suas proposições) e mais precisamente (ou seja, sem ter de usar recursos como "…"), usamos símbolos especiais chamados quantificadores. Os quatro quantificadores mais usados são:

$\forall$	quantificador universal (leia-se "para todo", "para qualquer", "dado qualquer")
$\exists$	quantificador existencial (leia-se "existe pelo menos um", "existe um (ao menos)")
$\exists!$	quantificador singular (leia-se "existe exatamente um")
$\nexists$	quantificador excludente (leia-se "não existe", "para nenhum")

Em textos de Lógica, principalmente nos mais antigos, e de Ciência da Computação, o leitor poderá encontrar outros símbolos para os quantificadores acima.
Também é de se observar que, além dos quatro quantificadores que mencionamos, existem outros. Um exemplo seria $\exists^m$, que é lido "existem muitos". Contudo, os mesmos são usados apenas em assuntos muito especializados e avançados.

– Estrutura simbólica de uma proposição quantificada, caso de uma variável:

$\boxed{\text{quantificador } x \in X : \ p(x)}$

Exemplo 1.18 -

Vejamos como reescrever as quatro proposições quantificadas de nosso exemplo inicial:

- $\forall x \in X : \ x - 3 > 0$
- $\exists x \in X : \ x - 3 > 0$
- $\exists! x \in X : \ x - 3 > 0$
- $\nexists x \in X : \ x - 3 > 0$

Exemplo 1.19 -

i). O Exemplo 1.1 poderia ter sido escrito simplesmente da seguinte forma:

$$\forall n \in \{0, 1, 2, 3, \dots\}, \ P(n) = 1 + 2^{(2^n)} \textit{ é um número primo.}$$

ii). O Exemplo 1.2 poderia ter sido escrito simplesmente da seguinte forma:

$$\forall n \in \{3, 4, 5, \dots\}, \textit{a equação } x^n + y^n = z^n \textit{ não tem soluções inteiras positivas.}$$

ou, então, como:

$$\nexists n \in \{3, 4, 5, \dots\}, \textit{a equação } x^n + y^n = z^n \textit{ tem soluções inteiras positivas.}$$

iii). O Exemplo 1.6 poderia ter sido escrito da seguinte forma:

$$\forall\, x \in \{10, \ -234, \ 4578, \ 1200\}, \ x \textit{ é par.}$$

iv). O Exemplo 1.7 poderia ter sido escrito da seguinte forma:

$$\forall\, n \in \mathbb{N}, \ n^2 - n + 41 \textit{ é primo.}$$

v). $\exists\, x \in \mathbb{N}, \ x = 3$
(leia-se: "existe, pelo menos, um número natural que é igual a 3").

vi). $\forall\, x \in \{2, 3, 4, 5\}, \ 1 < x \leq 3$
(leia-se: "todo elemento do conjunto $\{2, 3, 4, 5\}$ *é um número entre 1 e 3, podendo ser, inclusive, igual a 3").*

vii). $\forall\, T \in \{\textit{triângulos isósceles}\}, T$ *é um triângulo equilátero*
(leia-se: "todo triângulo isósceles é um triângulo equilátero").

Verifique que as expressões quantificadas acima são de fato proposições. Quais seus valores lógicos?
E quais são os valores lógicos das proposições a seguir?

viii). $\forall\, T \in \{$*triângulos equiláteros*$\}$, T *é um triângulo isósceles.*

ix). $\exists\, T \in \{$*triângulos isósceles*$\}$, T *é um triângulo equilátero.*

– Estrutura simbólica de uma proposição quantificada, caso de várias variáveis:

$\boxed{\text{quantificador } x \in X, \text{ quantificador } y \in Y, \ldots :\ p(x, y, \ldots)}$

Temos $4 \times 4 = 16$ possibilidades de combinar os quantificadores no caso de duas variáveis, $4 \times 4 \times 4 = 64$ no caso de três variáveis, etc.
Note, ademais, que todas as variáveis precisam estar quantificadas e que a ordem da quantificação é importante.

Exemplo 1.20 -

Denotando por X o conjunto dos números inteiros positivos, note a diferença entre as seguintes proposições quantificadas:

. $\forall x \in X, \exists y \in X :\ x = y^2$
a qual é lida como "para cada escolha de valor de x inteiro positivo, existe (ao menos um) y inteiro positivo cujo quadrado vale x."
(uma proposição falsa, pois $2 = y^2$ nunca vale se y for inteiro positivo)

. $\exists y \in X, \forall x \in X :\ x = y^2$
a qual pode ser lida como "existe y inteiro positivo cujo quadrado é igual a cada um dos inteiros positivos".
(uma proposição falsa, pois envolve igualar um valor de y a infinitos de x).

Estas duas proposições têm os mesmos quantificadores e são ambas falsas. Apesar disso, a troca da ordem dos quantificadores tornou-as logicamente distintas e mudou drasticamente seu significado matemático.

Na prática, usualmente, tornaremos a leitura mais clara e significativa com o uso de letras mais indicativas para os conjuntos e variáveis envolvidas. Por exemplo, a primeira proposição acima fica mais clara quando escrita como:

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} :\ n = x^2.$$

Com efeito, estamos acostumados a denotar incógnitas por x.

É comum que cada variável envolvida numa proposição quantificada tenha um universo distinto. Por exemplo, um dos objetivos deste livro é introduzir um campo numérico, dito campo dos números reais e denotado por $\mathbb{R}$, que torna verdadeira a seguinte variante da primeira proposição do exemplo anterior:

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{R} : \; n = x^2.$$

Definição 1.21 -

O conjunto de valores que a variável, ou que cada variável, de uma proposição quantificada é permitido assumir chama-se universo da variável.

Exemplo 1.22 -

No Exemplo 1.19 temos para universo das variáveis envolvidas:

i). *o conjunto* $\mathbb{N}$

ii). *o conjunto* $\{3, 4, 5, \dots\}$

iii). *o conjunto* $\{10, \; -234, \; 4578, \; 1200\}$

iv). *o conjunto* $\mathbb{N}$

v). *o conjunto* $\mathbb{N}$

vi). *o conjunto* $\{2, 3, 4, 5\}$

vii). *o conjunto* $\{$*triângulos isósceles*$\}$

viii). *o conjunto* $\{$*triângulos equiláteros*$\}$

ix). *o conjunto* $\{$*triângulos isósceles*$\}$

Salientamos ainda que as proposições

$$\forall x \in \mathbb{N}, \; 2x > x \qquad \text{e} \qquad \forall y \in \mathbb{N}, \; 2y > y$$

expressam o mesmo fato, a saber, "o dobro de um número natural é sempre maior do que este número". A diferença é que na primeira simbolizamos esse número natural genérico por x, enquanto na segunda o chamamos de y, assim como podíamos também ter usado "fulano".

1.4 O método dedutivo

No que toca à decisão do valor lógico de uma dada proposição (ou seja, provar que ela é verdadeira, ou provar que ela é falsa), já muito insistimos que o uso de exemplos (casos particulares) é matematicamente válido apenas para demonstrar a *falsidade* dessa proposição[3]. A demonstração de sua *veracidade* terá de ser feita pelo método dedutivo; ou seja, por meio de uma dedução.

Toda dedução é o resultado de uma implicação, ou do encadeamento de várias implicações. Assim, nossa abordagem do método dedutivo começará pelo estudo do conceito de implicação. Nas seções seguintes trataremos objetivamente das diversas maneiras básicas com que as implicações podem ser encadeadas numa dedução.

Definição 1.23 -

Dizemos que uma proposição p implica uma proposição q *se a* suposição *da veracidade de* p *nos leva a concluir (deduzir) a veracidade de* q.
Abreviaremos isso escrevendo $p \Rightarrow q$.

Exemplo 1.24 -

Supondo que $7 \times 123456 = 864192$, *podemos concluir que* $5 + 7 \times 123456 = 864197$.
Ou seja: $(7 \times 123456 = 864192) \Rightarrow (5 + 7 \times 123456 = 864197)$.

Exemplo 1.25 -

Do mesmo modo: $\big((123\,466)^2 = 234\,456\,256\big) \Rightarrow \big(\,1 + (123\,466)^2 = 234\,456\,257\big)$.

Terminologia: A notação $p \Rightarrow q$ pode ser lida de várias maneiras:

– q segue de p
– q é conseqüência de p
– para que ocorra q basta ocorrer p
– p é condição suficiente para q
– q é condição necessária para p
– se ocorre p então necessariamente ocorre q
– se p então q.

[3]Exceto nas situações excepcionais em que a proposição resume-se em um número finito de casos particulares.

Terminologia:
É tradicional dizermos que p é a hipótese ou premissa da implicação $p \Rightarrow q$, e que q é sua tese.

Cuidado!
Note que para decidirmos se uma implicação $p \Rightarrow q$ é verdadeira (ou seja, se foi feita corretamente), não precisamos saber se a hipótese p é *efetivamente* verdadeira. Tudo o que temos de fazer é mostrar que a veracidade da tese q é uma consequência (efeito) da *suposição* da veracidade de p.

Observemos que isso envolve uma sutileza. Assim, no Exemplo 1.25, da hipótese $(123\ 466)^2 = 234\ 456\ 256$ somos obrigados a concluir que $1 + (123\ 466)^2 = 234\ 456\ 257$. Apesar disso, atente que a hipótese envolvida é falsa! Com efeito: $(123\ 466)^2 = 15\ 243\ 853\ 156$!

Também podemos ter uma implicação verdadeira com hipótese falsa, mas tese verdadeira, como é o caso de

$$(2 \text{ e } 4 \text{ são ímpares}) \Rightarrow (6 \text{ é par}).$$

Essa proposição tem de ser entendida da seguinte maneira: "se for verdade que 2 e 4 são ímpares, então, como a soma de ímpares é par, temos de concluir que 6 é par." Talvez o leitor se sinta mais confortável lendo-a como: "se fosse verdade que 2 e 4 são ímpares, então, como a soma de ímpares é par, poderíamos concluir que 6 é par."

> *O leitor deve procurar se convencer de que a definição de implicação nunca nos pode levar a uma situação onde a hipótese é verdadeira e a tese é falsa.*

Como mostrar a veracidade de uma implicação matemática?

Resposta:
usando axiomas (proposições que se convenciona serem verdadeiras) e/ou em resultados já demonstrados. Assim, no Exemplo 1.24, o resultado usado foi o algoritmo da adição de inteiros, que nos permitiu afirmar que $5 + 864192 = 864197$. Por sua vez, no Exemplo 1.26, usamos apenas o resultado que diz "a soma de inteiros pares é um inteiro par". Em situações mais comuns em Matemática, podemos ter de fazer o uso de vários resultados; em estudos avançados pode-se ter de usar até centenas deles, ou mesmo mais.

A demonstração matemática típica consiste num encadeamento de implicações verdadeiras.

Como mostrar a efetiva veracidade de uma proposição matemática?

Resposta:
se a Matemática se resumisse tão somente em provar implicações, ela seria uma coleção de "supondo isso, então aquilo"; ela seria um mero jogo lógico, construindo sonhos. Bem entendido, as implicações são importantes, mas não suficientes para a plena Matemática. Ou seja: além de sabermos demonstrar implicações, precisamos saber decidir a veracidade, ou valor lógico, das proposições matemáticas.

Em essência, temos duas maneiras de mostrar que uma proposição matemática é efetivamente verdadeira:

– Ou esta proposição é um axioma da teoria em estudo.
– Ou esta proposição é a tese q de uma implicação verdadeira, $p \Rightarrow q$, cuja hipótese p também se sabe ser efetivamente verdadeira.
  Na prática, este raciocínio seria assim colocado: sabemos que p é verdadeira; ora, $p \Rightarrow q$, logo temos que q também é verdadeira.

Exemplo 1.26 -

Supondo que 2 *e* 4 *sejam pares, como a soma de pares é par, então* $6 = 2 + 4$ *teria de ser par. Ou seja:*

$$2 \ e \ 4 \ pares \overset{soma \ de \ pares \ é \ par}{\Rightarrow} 6 \ é \ par\,.$$

Ora, 2 *e* 4 *realmente são pares, logo* 6 *é efetivamente par.*

Complementando, observe que, enquanto uma conjectura p estiver em aberto (ou seja, ainda não se souber se é uma proposição verdadeira ou falsa, como é o caso da Conjectura de Goldbach), tudo o que os matemáticos podem fazer é deduzir cadeias de *implicações* verdadeiras

$$p \Rightarrow p' \Rightarrow p'' \Rightarrow p''' \Rightarrow \ldots$$

na qual ainda não se conhece o valor verdade de nenhuma das *proposições* envolvidas. Consequentemente:

- se algum dia se conseguir mostrar que a conjectura p é verdadeira, automaticamente ficará provado que também p', p'', p''', etc são verdadeiras;
- se algum dia se provar que alguma das proposições p', p'', p''', etc é falsa, pela definição de implicação, poderemos garantir que a conjectura p também é falsa.

Exemplo 1.27 -

No capítulo a seguir, quando estudarmos o Teorema Fundamental da Aritmética, teremos condições de facilmente provar a seguinte implicação $p \Rightarrow q$:

> *"se a conjectura de Goldbach for verdadeira, então todo múltiplo de 4 pode ser escrito como a soma de dois pares, não ambos múltiplos de 4."*

Temos duas maneiras de concluir que a tese $q =$ (*todo múltiplo de* 4 *pode ser ...*) *é efetivamente verdadeira: ou se prova que a Conjectura de Goldbach é verdadeira, ou se prova uma implicação $p' \Rightarrow q$ na qual se sabe que a proposição p' é efetivamente verdadeira.*
Ademais, estudando o valor lógico dessa tese, também temos chances de decidir a veracidade da hipótese $p =$ (*a Conjectura de Goldbach é verdadeira*)*. Por exemplo, se algum dia se achar um múltiplo de 4 que não pode ser escrito como soma de dois pares, não ambos múltiplos de 4 (ou seja, se for provado que a tese q é falsa), poderemos afirmar que a Conjectura de Goldbach é falsa. Vide maiores detalhes no Exercício 54 do Capítulo 2.*

Em Matemática, também utilizamos implicação entre sentenças abertas. As definições e notações são semelhantes às de implicação de proposições. Dizemos que uma sentença aberta $p(x)$ implica outra $q(x)$, e escrevemos $p(x) \Rightarrow q(x)$, quando:

i). o universo onde varia a variável de cada uma dessas sentenças é o mesmo conjunto;

ii). para cada valor $x = x_0$ desta variável em tal universo, temos que $p(x_0) \Rightarrow q(x_0)$, no sentido de implicação de proposições.

Exemplo 1.28 -

No universo dos números inteiros:

$$x^2 = 1234 \Rightarrow \left(5 + x^2 = 1239\right).$$

Exemplo 1.29 -

$$x \textit{ é inteiro par} \Rightarrow x + 10 \textit{ é par}$$

ou seja: supondo que x seja um número inteiro par, como a soma de pares é par, então $x + 10$ é par.

Importante!

Mais uma vez, enfatizamos que nunca precisamos saber se a *hipótese* é de fato verdadeira para decidirmos se uma *implicação* é verdadeira. Isto vale tanto para implicações entre proposições quanto para implicações entre sentenças abertas. Com efeito, no segundo exemplo acima, a sentença "x é inteiro par" torna-se verdadeira para alguns valores de x, e para outros torna-se falsa. Apesar disso, a implicação é verdadeira.

Note que o entendimento do significado da implicação "se x é tal que $p(x)$ é V, então $q(x)$ também o é", ou seja, o significado da *suposição* de $p(x)$ ser V implica $q(x)$ ser verdadeira, fica mais evidente no caso das proposições abertas.

Terminologia:
Analogamente ao caso das implicações entre proposições, uma implicação entre sentenças abertas $p(x) \Rightarrow q(x)$, $p(x)$ é chamada de hipótese , e $q(x)$ de tese da implicação.

Terminologia:
A notação $p(x) \Rightarrow q(x)$ pode ser lida de várias formas, todas semelhantes às usadas para $p \Rightarrow q$. Nos damos ao trabalho de explicitar as mais comuns:

– $q(x)$ segue de $p(x)$
– $q(x)$ é consequência de $p(x)$
– para que ocorra $q(x)$ basta ocorrer $p(x)$
– $p(x)$ é condição suficiente para $q(x)$
– $q(x)$ é condição necessária para $p(x)$
– se ocorre $p(x)$, então necessariamente ocorre $q(x)$
– se $p(x)$, então $q(x)$.

Definição 1.30 -

A recíproca *da implicação* $p \Rightarrow q$ *(ou* $p(x) \Rightarrow q(x)$*) é a implicação* $q \Rightarrow p$, *(ou, respectivamente,* $q(x) \Rightarrow p(x)$*).*

É fundamental que não confundamos uma sentença com sua recíproca, pois uma delas pode ser verdadeira e a outra não. Começamos ilustrando com um exemplo não matemático:

Exemplo 1.31 -

"o nome do presidente é João" $\Rightarrow$ *"o presidente é homem"*
é uma implicação verdadeira, mas não podemos afirmar que é verdadeira sua recíproca:
"o presidente é homem" $\Rightarrow$ *"o nome do presidente é João".*

Costumamos escrever "o presidente é homem" $\not\Rightarrow$ *"o nome do presidente é João".*

Exemplo 1.32 -

No universo dos números inteiros: "$x = 2 \Rightarrow x^2 = 4$*", mas "*$x^2 = 4 \not\Rightarrow x = 2$*".*

No entanto, eventualmente encontraremos implicações verdadeiras, cuja recíproca também é verdadeira:

Exemplo 1.33 -

Temos que $(2^3 = 8) \Rightarrow (2^3 + 1 = 9)$.
É igualmente imediato ver que $(2^3 + 1 = 9) \Rightarrow (2^3 = 8)$.

Exemplo 1.34 -

Sendo
$p : \big(123\ 466^2 = 234\ 456\ 256\big)$ *e* $q : \big(123\ 466^2 + 2 = 234\ 456\ 258\big)$,
então temos $p \Rightarrow q$*, mas também podemos afirmar que* $q \Rightarrow p$.

Definição 1.35 -

Quando duas proposições (ou duas sentenças abertas) são tais que a primeira implica a segunda e a segunda implica a primeira, dizemos que elas são equivalentes*.*

Denotamos a equivalência entre p e q por $p \Leftrightarrow q$, e a equivalência entre $p(x)$ e $q(x)$ por $p(x) \Leftrightarrow q(x)$.
Semelhantemente, se não ocorrer tal equivalência, escreveremos, respectivamente: $p \not\Leftrightarrow q$, e $p(x) \not\Leftrightarrow q(x)$.

Exemplo 1.36 -

$\left(123\,466^2 = 234\,456\,236\right) \iff \left(123\,466^2 + 2 = 234\,456\,238\right)$.

Terminologia:
Podemos expressar a idéia de equivalência de diferentes formas:

– q segue de p e p segue de q;
– p é uma condição necessária e suficiente para q;
- q é uma condição necessária e suficiente para p.

> Note que duas proposições equivalentes têm o mesmo valor verdade:
> *ou são ambas V, ou são ambas F.*
> Com efeito, se uma for V e a outra F, então teríamos uma verdadeira implicando numa falsa. Portanto, é muito comum expressarmos a equivalência de duas proposições p e q dizendo:
>
> p é verdadeiro se, e somente se, q o for.
>
> Analogamente, quando duas sentenças abertas são equivalentes, então cada vez que elas se tornarem proposições:
> *ou serão ambas V, ou serão ambas F.*

Exemplo 1.37 -

Para todo número natural n:

$$n^2 < 9 \Leftrightarrow n < 3.$$

Por exemplo, para $n = 2$ temos $2^2 < 9$ e $2 < 3$, ambas V; e para $n = 5$ temos $5^2 < 9$ e $5 < 3$, ambas F.

Exemplo 1.38 -

Para todo número inteiro r,

$$r^2 < 9 \not\Leftrightarrow r < 3,$$

pois é V a implicação $\Rightarrow$ mas não é verdadeira a implicação $\Leftarrow$. Por exemplo, $-20 < 3$ é V, mas $(-20)^2 < 9$ é F, o que produz $V \to F$.
Outra maneira de concluir é usar o critério da "mesma veracidade". No caso, a escolha $r = -20$ nos dá $r^2 < 9$: F e $r < 3$: V; logo, não existe a equivalência.

1.5 Demonstração de proposições enunciadas como implicações

Para demonstrar uma implicação do tipo

$$p(x) \Rightarrow q(x),$$

onde $p(x)$ e $q(x)$ denotam sentenças abertas na variável x, existem três métodos básicos: demonstração direta, contrapositiva e por absurdo, os quais passamos a descrever e exemplificar.

a). Demonstração direta:

> Consiste em supor que $p(x)$ *é* V e construir um encadeamento de inferências (igualdades, desigualdades e outras) que tenham como conclusão (ou que nos permitam deduzir) que $q(x)$ *é* V.

Exemplo 1.39 -

A soma de dois números inteiros de mesma paridade sempre é par. Ou seja:
– a soma de dois inteiros pares é par: $x, y \in \mathbb{Z}$ e pares $\Rightarrow$ $x + y$ par;
– a soma de dois inteiros ímpares é par: $x, y \in \mathbb{Z}$ e ímpares $\Rightarrow$ $x + y$ par.

Prova:

Sejam $x, y \in \mathbb{Z}$, ambos pares. Então, podemos escrever: $x = 2m$ e $y = 2n$, para apropriados $m, n \in \mathbb{Z}$. Daí $x + y = 2m + 2n = 2(m + n)$ = dobro de inteiro, logo, par.

Sejam $x, y \in \mathbb{Z}$, ambos ímpares. Então, podemos escrever: $x = 2m+1$ e $y = 2n+1$, para apropriados $m, n \in \mathbb{Z}$. Daí $x + y = (2m + 1) + (2n + 1) = 2m + 2n + 2 = 2(m + n + 1) =$ dobro de inteiro, logo, par.

CQD.

Exemplo 1.40 -

O produto de dois números inteiros pares é par, e o produto de dois inteiros ímpares é ímpar. Ou seja:
– $x, y \in \mathbb{Z}$ e pares $\Rightarrow$ xy par;
– $x, y \in \mathbb{Z}$ e ímpares $\Rightarrow$ xy ímpar.

Prova:

Sejam $x, y \in \mathbb{Z}$, ambos pares. Então, podemos escrever: $x = 2m$ e $y = 2n$, para apropriados $m, n \in \mathbb{Z}$. Daí $xy = 2m \cdot 2n = 2(2mn) =$ dobro de inteiro, logo, par.

Sejam $x, y \in \mathbb{Z}$, ambos ímpares. Então, podemos escrever: $x = 2m+1$ e $y = 2n+1$, para apropriados $m, n \in \mathbb{Z}$. Daí $xy = (2m + 1) \cdot (2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1 = 1+$ dobro de inteiro, logo, ímpar.

CQD.

Exercício 4 -

Use os dois exemplos anteriores para dar uma demonstração direta de que $n^2+n+500$ sempre é um número par, qualquer que seja o valor de n inteiro.

b). Demonstração por absurdo:

> *Provar por absurdo* que $p(x) \Rightarrow q(x)$ consiste em mostrar que a "mistura" da possibilidade de $p(x)$ ser verdadeira com a de $q(x)$ ser falsa produz um conflito; nos leva a algum resultado sabidamente falso ou absurdo.

Justifiquemos.
A suposição da veracidade de $p(x)$ nos dá apenas duas possibilidades exclusivas para a combinação $p(x), q(x)$:

– ou $p(x)$ é V e $q(x)$ é V ;
– ou $p(x)$ é V e $q(x)$ é F .

Daí, se provarmos que a segunda alternativa não pode ocorrer, seguirá que somos obrigados a ter que $p(x)$ é V e $q(x)$ é V. Ou seja, temos que a suposição $p(x)$ é V implica $q(x)$ é V.

Uma dificuldade associada a essa técnica de demonstração consiste no fato de que o absurdo a que chegaremos varia com a prova. Não podemos prever onde ele ocorrerá em nossa argumentação, e nem que forma ele terá (pode ser fatos como $1 = 0$, $2 > 3$ e outros).

Exemplo 1.41 -

Se n estiver no universo dos números naturais, então

$$n^2 + 2n + 3 \neq (n+1)^2 - 5,$$

ou, equivalentemente:

$$n \in \mathbb{N} \Rightarrow n^2 + 2n + 3 \neq (n+1)^2 - 5.$$

Prova:

Por absurdo, suponhamos que exista $n \in \mathbb{N}$, tal que $n^2 + 2n + 3 = (n+1)^2 - 5$. Então, pelas propriedades da adição e da multiplicação de números naturais, podemos escrever:

$$\begin{aligned}
n^2+2n+3 &= (n+1)^2-5 \Rightarrow \\
n^2+2n+3 &= n^2+2n+1-5 \Rightarrow \\
n^2+2n+3 &= n^2+2n-4 \Rightarrow \\
3 &= -4, \text{ absurdo!}
\end{aligned}$$

Concluímos que $n^2+2n+3 \neq (n+1)^2-5$, para todo $n \in \mathbb{N}$. CQD.

Notação:
Indicamos a negação de $p(x)$ por $\neg p(x)$.
(É conveniente ter em mente que $\neg\neg p(x) = p(x)$.)

Com esta notação, podemos afirmar:

> provar por absurdo que $p(x) \Rightarrow q(x)$ significa provar:
> supor que $p(x)$ e $\neg q(x)$ são V gera um conflito, ou um resultado absurdo.

Exercício 5 -

Reflita cuidadosamente sobre essa última afirmação.

c). Demonstração por contraposição

Esta técnica de demonstração de implicações é a menos natural de todas. Apesar disto, é muito útil, pois frequentemente é de fácil aplicação enquanto as outras são difíceis ou inviáveis. Para facilitar, introduzamos mais uma terminologia clássica.

Definição 1.42 -

$\neg q(x) \Rightarrow \neg p(x)$ *é chamada de* contrapositiva *da implicação* $p(x) \Rightarrow q(x)$.

Exemplo 1.43 -

Consideremos as seguintes proposições, no universo dos números inteiros:
$p(x): \ x < 0$
$q(x): \ x \neq 0$

Com isso, obtemos a seguinte combinatória de implicações:

[direta]	$p(x) \Rightarrow q(x)$,	ou seja: $x < 0 \Rightarrow x \neq 0$
[reciproca]	$q(x) \Rightarrow p(x)$,	ou seja: $x \neq 0 \Rightarrow x < 0$
[contrapositiva]	$\neg q(x) \Rightarrow \neg p(x)$,	ou seja: $x = 0 \Rightarrow x \geqslant 0$
[reciproca da contrapositiva]	$\neg p(x) \Rightarrow \neg q(x)$,	ou seja: $x \geqslant 0 \Rightarrow x = 0$.

No exemplo acima, a direta e a contrapositiva tiveram o mesmo valor de verdade. O método da demonstração por contrapositiva explora que essa concordância sempre ocorre. Ou seja:

> *Provar por contraposição* uma implicação $p(x) \Rightarrow q(x)$ consiste em provar de forma direta sua contrapositiva $\neg q(x) \Rightarrow \neg p(x)$.
> Equivalentemente:
> partindo da suposição que $\neg q(x)$ é verdadeira, deduzimos que $\neg p(x)$ também é verdadeira.

Justiquemos.
Seja dado que conseguimos provar diretamente que $\neg q(x) \Rightarrow \neg p(x)$. O que podemos concluir sobre $q(x)$ se $p(x)$ for V?
A suposição da veracidade de $p(x)$ nos dá apenas duas possibilidades exclusivas para a combinação $p(x), q(x)$:

– ou $p(x)$ é V e $q(x)$ é V
– ou $p(x)$ é V e $q(x)$ é F,

o que equivale dizer:

– ou $p(x)$ é V e $q(x)$ é V
– ou $p(x)$ é V e $\neg q(x)$ é V.

Ora, estamos supondo que conseguimos provar diretamente que a suposição de que $\neg q(x)$ é verdadeira implica $\neg p(x)$ também ser verdadeira, ou seja: $p(x)$ é F. Isto faz com que a segunda alternativa acima não possa ocorrer. Quem ocorre é a primeira alternativa!

Consequentemente, a prova da contrapositiva nos autoriza dizer que a suposição da veracidade de $p(x)$ implica na veracidade de $q(x)$. Ou seja, a prova da contrapositiva $\neg q(x) \Rightarrow \neg p(x)$ implica na prova de $p(x) \Rightarrow q(x)$.

Exemplo 1.44 (protótipo) -

Sempre que x^2 for ímpar, teremos que x é obrigatoriamente ímpar.

Prova:

Observemos que a implicação [x^2 ímpar] $\Rightarrow$ [x ímpar] tem uma contrapositiva muito mais fácil de provar: [x par] $\Rightarrow$ [x^2 par]. Com efeito:

x par $\Rightarrow x = 2n \Rightarrow x^2 = 4n^2 = 2 \cdot 2n^2 =$ par.

CQD.

Exercício 6 -

Para que o leitor se convença da vantagem, ao menos neste caso, de usarmos a contrapositiva, tente provar este último resultado diretamente.

Exemplo 1.45 -

Provemos a seguinte proposição: x tem a mesma paridade que seu quadrado, sempre que $x \in \mathbb{Z}$.

Prova:

Nossa proposição pode ser escrita como a equivalência

$$\forall x \in \mathbb{Z} : \ [x \text{ é par} \Leftrightarrow x^2 \text{ é par}].$$

Observemos, a seguir, que a implicação ($\Rightarrow$) já foi demonstrada (de forma direta); assim, resta provarmos a recíproca, o que faremos por contraposição. Ou seja, provemos:

$$\text{não é verdade que } x \text{ é par } \Rightarrow \text{ não é verdade que } x^2 \text{ é par},$$

ou seja (já que um inteiro que não é par é necessariamente ímpar), que

$$x \text{ é ímpar} \Rightarrow x^2 \text{ é ímpar}.$$

De fato:

$$\begin{aligned} x \text{ é ímpar} \Rightarrow x = 2k+1, \text{ para algum } k \in \mathbb{Z} \Rightarrow \\ x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1. \end{aligned}$$

Como $2k^2 + 2k$ é um inteiro, temos que x^2 é um inteiro ímpar.

CQD.

Exemplo 1.46 -

Afirmamos que, sendo x racional positivo:

$$x^2 = 2 \Rightarrow x > 1\,.$$

Prova:

Por contraposição, e trabalhando no universo dos números racionais positivos, provemos que

$$0 < x \leqslant 1 \Rightarrow x^2 \neq 2\,.$$

De fato,

$$0 < x \leqslant 1 \overset{\text{como } x>0}{\Longrightarrow} 0 = 0 \cdot x < x \cdot x \leqslant x \cdot 1 = x \leqslant 1 \Rightarrow x^2 \leqslant 1 < 2 \Rightarrow x^2 \neq 2\,.$$

CQD.

> Tornamos a enfatizar que a não existência de um número racional, cujo quadrado seja 2, não tem nada a ver com a legitimidade da demonstração dada. A demonstração tratou de provar a legitimidade da implicação, e não a veracidade da sua hipótese.

Exercício 7 -

Prove que se x é um racional positivo, tal que $x^2 = 2$, então $x < \frac{3}{2}$.

1.6 Demonstração de proposições não enunciadas como implicações

Trataremos aqui apenas dos tipos mais comuns de demonstrações de proposições matemáticas que não estão enunciadas sob a forma de implicação.

a). Demonstrações de afirmações existenciais

Para comprovar que uma proposição da forma

$$\exists a \in A \text{ tal que } p(a) \text{ é } V$$

ou

$$\exists a \in A \text{ tal que } a \text{ satisfaz } p(x),$$

basta *exibir* um elemento do conjunto A que satisfaça a condição $p(x)$.

Exemplo 1.47 -

$\exists a \in \mathbb{Z}$, a é multiplo de 2 e de 35 simultaneamente.

Prova:

De fato, basta tomar $a = 2 \times 35$.

CQD.

Cuide o leitor de não generalizar, achando que toda prova de afirmação de existência tenha de ser feita exibindo-se o elemento procurado. Isto, por exemplo, não ocorre com a afirmação de que toda equação polinomial, de coeficientes reais e grau ímpar, é obrigada a ter ao menos uma raiz real. Com efeito, em vez de procurarmos expressar tal raiz (o que é em geral impossível, se o grau for cinco ou um ímpar ainda maior), usa-se um argumento indireto que mostra que tal existência não pode deixar de ocorrer, embora o mesmo não possa dar o valor dessa raiz.

b). Demonstração de afirmações de impossibilidade

Para comprovar a validade de uma proposição da forma

$$\nexists a \in A \text{ tal que } p(a) \text{ é } V,$$

podemos, por exemplo, raciocinar por absurdo.

Exemplo 1.48 -

Não existe n inteiro positivo tal que $n^2 + 2n + 3 = n(n+1)$.

Prova:

Por absurdo, se existisse um inteiro positivo n_0 tal que $n_0^2 + 2n_0 + 3 = n_0(n_0+1)$, teríamos que este n_0 verificaria $n_0^2 + 2n_0 + 3 = n_0^2 + n_0$. Simplificando, obteríamos: $n_0+3 = 0$, o que é uma impossibilidade entre os inteiros positivos. Assim, concluímos que não existe n inteiro positivo tal que $n^2 + 2n + 3 = n(n+1)$.

CQD.

c). Demonstração de afirmações de universalidade

Para comprovar a validade de proposições da forma

$$\forall a \in A,\ p(a) \text{ é } V,$$

podemos raciocinar de forma direta, provando a implicação

$$a \in A \Rightarrow p(a) \text{ é } V,$$

como fizemos nos exemplos da seção anterior.

Um caso particular ocorre quando temos uma afirmação sobre todas as proposições de uma sequência: $p(1), p(2), \ldots$. Um exemplo sendo:

$$p(n): \quad \forall n \text{ inteiro positivo}, \ \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Esse tipo de proposição pode ser expresso de modo mais sintético e preciso usando-se quantificadores. Com efeito, sendo $A =$ conjunto dos inteiros positivos, elas têm a forma:

$$\forall n \in A,\ p(n) \ \text{ é } V.$$

A técnica de demonstração mais útil para esse caso particular é a baseada no *Princípio da Indução Matemática,* que estudaremos na próxima seção.

d). Demonstração da falsidade de afirmações de universalidade

Como comprovamos a *não validade* de uma proposição da forma

$$\forall a \in A,\ p(a) \text{ é } V$$

ou seja,

$$\forall a \in A, \ a \ \text{ satisfaz } p(x)?$$

Ora, uma proposição é falsa se e só se sua negação é V; portanto, mostrar que a afirmação citada é falsa, é o mesmo que mostrar que sua negação é verdadeira. No caso, então, quereríamos mostrar que

$$\exists a \in A, \ \text{ tal que } a \text{ não satisfaz } p(x).$$

Quando provamos esta afirmação exibindo um elemento (veja (a)), tal elemento é chamado um *contraexemplo* para a proposição original.

Exemplo 1.49 -

A afirmação

$$\text{“}\textit{para todo } x \textit{ inteiro positivo, } n^2 - n + 41 \textit{ é um número primo}\text{''}$$

é uma proposição quantificada falsa (F)*, pois* 41 *é um contraexemplo para a mesma (a decisão de sua veracidade já foi feita no Exemplo 1.5).*

Exemplo 1.50 -

A afirmação

$$\text{“}\textit{para todo } n \textit{ inteiro positivo: } 2^n > n^2\text{''}$$

é falsa (F)*, sendo que* 2 *serve como contraexemplo.*

Observação 1.51 -

Em ordem a não alongarmos demasiadamente este capítulo introdutório, não abordaremos a demonstração de proposições envolvendo dois ou mais quantificadores. Um exemplo seria que, dado um certo conjunto A *de números inteiros:*

$$(\forall x \in A)(\exists y \in A)(x + y = 5)\,.$$

Em relação a isso, uma das primeiras coisas a ser entendida é que, em geral, não podemos trocar a ordem das quantificações envolvidas. Assim, se tomarmos no exemplo anterior $A = \{0, 1, 2, 3, 4, 5\}$*, temos que a proposição envolvida é verdadeira, enquanto que:*

$$(\exists y \in A)(\forall x \in A)(x + y = 5)$$

é falsa (no exercício a seguir, o leitor é convidado a examinar essa e outras possibilidades).

Exercício 8 -

Sendo $A = \{0, 1, 2, 3, 4, 5\}$, *pede-se decidir o valor verdade de cada uma das proposições mencionadas acima:*

i).
$$(\forall x \in A)(\exists y \in A)(x + y = 5)\,.$$

ii).
$$(\exists y \in A)(\forall x \in A)(x + y = 5)\,.$$

Exercício 9 -

Sendo $A = \{0, 1, 2, 3, 4, 5\}$, *pede-se decidir o valor verdade de cada uma das proposições a seguir:*

i).
$$(\forall x \in A)(\forall y \in A)(x + y = 5)\,.$$

ii).
$$(\exists x \in A)(\exists y \in A)(x + y = 5)\,.$$

1.7 Demonstração por indução matemática

Iniciemos propondo uma brincadeira que nos servirá para tornar concretas as ideias básicas da técnica envolvida numa demonstração por indução. A brincadeira consiste no seguinte:

> enfileirar (e "em pé") as pedras de um jogo de dominó de modo tal que com um único toque sejamos capazes de derrubar todas elas.

Observemos que a "solução" da brincadeira repousa em duas condições:

1). garantir que o toque inicial realmente derruba a primeira pedra da fila;

2). garantir que as pedras estejam distanciadas de modo tal que cada uma que caia derrube a seguinte.

Note o rigorismo envolvido na condição (2). Assim, se a distância entre, digamos, a 12^{a} e a 13^{a} pedra não estiver conforme (no sentido de que a derrubada da 12^{a} pedra não cause ou implique a derrubada da 13ª), e se a 5^a pedra for derrubada, cairão, no máximo, a 5^a, a 6^a, a 7^a, a 8^a, a 9^a, a 10^a, a 11^a e a 12^a pedras da fileira.

Note, ademais, que o *efeito dominó* somente se realiza se as duas condições estiverem verificadas. Ou seja: sozinha, nenhuma delas é capaz de produzir o efeito desejado!

O interesse dessa brincadeira está no fato de que o raciocínio que ela envolve, uma vez abstraído, pode ser usado para provar a veracidade de uma sequência infinita de proposições matemáticas. Basta explorarmos as seguintes analogias:

"dominó" $\leftrightarrow$ "proposição",
"dominó derrubado" $\leftrightarrow$ "proposição verdadeira".

Coloquemos tudo isso sob forma de um teorema:

Teorema 1.52 (Princípio da Indução Matemática Simples) -

Consideremos uma sequência de proposições $p(n)$, indexadas por uma variável inteira $n \geqslant 1$. Supondo que:

i). a afirmação $p(1)$ seja verdadeira;
ii). a implicação "$p(k)$ é $V \Rightarrow p(k+1)$ é V" seja verdadeira, para cada $k \geqslant 1$,

então a proposição $p(n)$ é verdadeira, para todos os inteiros $n \geqslant 1$.

Observação 1.53 -

Certamente, o leitor terá observado que os itens (i) e (ii) do teorema correspondem às condições (1) e (2) da brincadeira dos dominós.

Definição 1.54 -

A condição (i) no Princípio da Indução é chamada de base de indução, enquanto que a premissa da implicação em (ii) é denominada hipótese de indução e a implicação envolvida em (ii) é dita ser a passagem de indução.

Na prática matemática, além de não trabalharmos com dominós, podemos encontrar sequências que, devido ao contexto em que estão inseridas, têm uma enumeração diferente da usada no enunciada do teorema. Ou seja, em vez de $p(1)$, $p(2)$, $p(3), \ldots$, podemos encontrar sequências da forma $p(0)$, $p(1)$, $p(2), \ldots$, ou $p(2)$, $p(3)$, $p(4), \ldots$; ou, em geral, iniciando com um $p(\alpha)$, onde α é um número inteiro qualquer.

É fácil vermos que esses casos se encaixam no teorema acima, bastando modificar a notação. Por exemplo, se a sequência do contexto matemático original é $p(2)$, $p(3)$, $p(4), \ldots$, caímos no enunciado do teorema trabalhando com $q(1) = p(2)$, $q(2) = p(3), \ldots$. Contudo, fica mais prático darmos um enunciado mais geral para o Príncipio da Indução Simples:

Teorema 1.55 -

Consideremos uma sequência de proposições $p(n)$, indexadas por uma variável inteira n. Seja α um valor particular inicial de n. Supondo que:

i). a afirmação $p(\alpha)$ seja verdadeira;

ii). a implicação "$p(k)$ é $V \Rightarrow p(k+1)$ é V" seja verdadeira, para cada $k \geqslant \alpha$,

então a proposição $p(n)$ é verdadeira para todos os inteiros $n \geqslant \alpha$.

Observação 1.56 -

Na prática, os valores mais usuais para a constante α são: $\alpha = 0$ (quando tivermos de provar a veracidade de uma sequência $p(0), p(1), p(2), \ldots$ de proposições) ou $\alpha = 1$ (quando estivermos estudando uma sequência de proposições $p(1), p(2), \ldots$). Mas, é perfeitamente possível encontrarmos um problema no qual a sequência de proposições da qual queremos provar a veracidade inicie com uma $p(\alpha)$ onde $\alpha \neq 0, 1$.

Também pode ocorrer que queiramos demonstrar a veracidade de uma sequência $p(0), p(1), p(2), \ldots$ de proposições tais que a passagem de indução ocorra somente, digamos, para $n \geqslant 2$. Num caso como este, a base de indução seria com $\alpha = 2$, e as proposições $p(0)$ e $p(1)$ seriam provadas "por fora" do raciocínio indutivo.

Se o leitor sempre estiver fazendo a analogia dos dominós, dificilmente cometerá erros.

Damos a seguir vários exemplos de demonstrações utilizando o Princípio da Indução. Costumamos dizer então que "a demonstração foi feita por indução". Note que sua aplicação consiste em verificar a veracidade da base de indução (item (i)) e, o que tipicamente será a parte que pode provocar dificuldades, provar a ocorrência da "engrenagem" associada à passagem de indução (item (ii) do Princípio).

Exemplo 1.57 (protótipo) -

Demonstrar que:

$$1 + 7 + 13 + \cdots + (6n - 5) = n(3n - 2), \quad \forall n \geqslant 1.$$

Prova:

Temos de provar a veracidade da sequência de afirmações $p(1), p(2), p(3) \cdots$, onde

$$(\forall n \geqslant 1)\ p(n):\ 1 + 7 + 13 + \cdots + (6n - 5) = n(3n - 2).$$

Tentaremos fazer a demonstração por indução, tomando como base de indução o caso $p(1)$, ou seja $\alpha = 1$.

etapa (i):
meramente verificamos que $1 = 1(3 - 2)$.

etapa (ii):
sendo $k \geqslant 1$ e valendo $1 + 7 + 13 + \cdots + (6k - 5) = k(3k - 2)$ (hipótese de indução), provemos que terá de valer:

$$1 + 7 + 13 + \cdots + (6k - 5) + \big((6(k + 1) - 5\big) = (k + 1)(3k + 1).$$

Ora, somando $(6k + 1)$ a ambos os membros da hipótese de indução, temos:

$$1+7+13+\cdots+(6k-5)+(6k+1) = k(3k-2)+(6k+1) = 3k^2+4k+1 = (k+1)(3k+1),$$

o que confirma a validade do passo de indução.

Juntando as etapas (i) e (ii), pelo Princípio da Indução, podemos dar por concluída a demonstração.

CQD.

Exemplo 1.58 (Indução no contexto da Teoria de Números) -

Demonstrar que

$$\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n + 1)} = \frac{n}{n + 1},$$

para todo n inteiro positivo.

Prova:

Seja $p(n)$ a afirmação dada pela equação anterior, isto é,

$$p(n): \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Notemos então que

$$\frac{1}{1.2} = \frac{1}{2} = \frac{1}{1+1},$$

de modo que $p(1)$ é verdadeira.

Seja $k \geq 1$ e suponhamos que $p(k)$ é verdadeira, ou seja,

$$\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}.$$

Verifiquemos se isto implica que a afirmação é verdadeira para o inteiro $k+1$, ou seja, que $p(k+1)$ é verdadeira. Temos:

$$\begin{aligned}
&\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{(k+1)[(k+1)+1]} \\
&= \left(\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{k(k+1)}\right) + \frac{1}{(k+1)(k+2)} \overset{\textit{hipótese de indução}}{=} \\
&= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} = \frac{k(k+2)+1}{(k+1)(k+2)} \\
&= \frac{k^2+2k+1}{(k+1)(k+2)} = \frac{(k+1)^2}{(k+1)(k+2)} \\
&= \frac{k+1}{k+2} = \frac{k+1}{(k+1)+1},
\end{aligned}$$

e, portanto, $p(k+1)$ é também verdadeira.

Assim, pelo Princípio da Indução, concluímos que

$$\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1},$$

para todo n inteiro maior ou igual a 1.

CQD.

Exercício 10 -

Provar que a soma dos quadrados dos n primeiros inteiros positivos é igual a

$$\frac{n(n+1)(2n+1)}{6}.$$

Exercício 11 -

Provar que, para todo n inteiro positivo:

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

Exemplo 1.59 (Indução no contexto de polinômios) -

Provemos que

$$(X^m - 1) = (X-1)(1 + X + X^2 + \cdots + X^{m-1}),$$

para todos os inteiros $m \geqslant 2$.

Ou, equivalentemente:

$$1 + X + X^2 + \cdots + X^{m-1} = \frac{X^m - 1}{X - 1},$$

para todo $m \geqslant 2$.

Prova:

Note que

$$(X-1)(1+X) = (X-1)(X+1) = (X^2 - 1)$$

mostra que a afirmação é verdadeira para $m = 2$:

$$1 + X = \frac{X^2 - 1}{X - 1}.$$

Suponhamos que a afirmação é verdadeira para $k \geqslant 2$, ou seja,

$$1 + X + X^2 + \cdots + X^{k-1} = \frac{X^k - 1}{X - 1}. \tag{1.1}$$

Verifiquemos, então, se a afirmação também é verdadeira para o inteiro $k+1$. Ora:

$$\begin{aligned} 1 + X + X^2 + \cdots + X^{(k+1)-1} &= \Big(1 + X + X^2 + \cdots + X^{k-1}\Big) + X^k \\ &\overset{(1.1)}{=} \frac{X^k - 1}{X - 1} + X^k = \frac{X^k - 1 + X^k(X-1)}{X-1} \\ &= \frac{X^{k+1} - 1}{X - 1} \end{aligned}$$

e, portanto, a afirmação é efetivamente verdadeira para o inteiro $k+1$. CQD.

Exercício 12

Aplique o resultado enunciado no exemplo anterior para deduzir a fórmula da soma dos m primeiros termos de uma progressão geométrica.

Exemplo 1.60 (Indução no contexto da Geometria) -

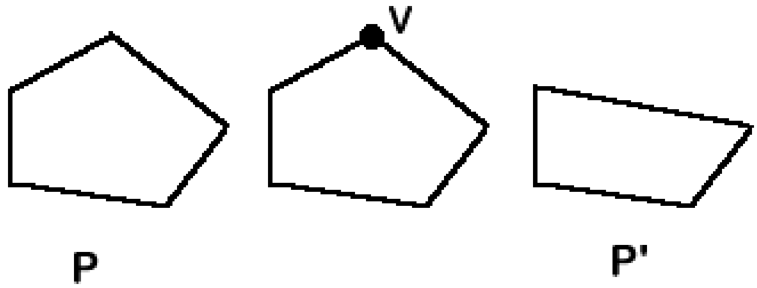
Provemos a seguinte afirmação: a soma das medidas dos ângulos internos de qualquer polígono convexo de n lados vale $(n-2)\cdot 180°$.

Prova:

Neste caso, $p(n) =$ todo polígono convexo de n lados tem para soma das medidas de seus ângulos internos $(n-2)\cdot 180°$.

Como o triângulo é o polígono com o menor número possível de lados, temos que a base de indução é a afirmação $p(3)$. Ora, $p(3)$ é uma afirmação verdadeira bem conhecida na Geometria; consequentemente, resta-nos provar a passagem de indução. Para tal, dado $k \geqslant 3$, supondo que todo polígono convexo com k lados tenha como soma de seus ângulos internos o valor $(k-2)\cdot 180°$, precisamos provar que todo polígono convexo de $(k+1)$ lados tem para soma de seus ângulos internos o valor $(k+1-2)\cdot 180° = (k-1)\cdot 180°$.

Seja P um polígono convexo de $k+1$ lados, e fixemos um vértice V deste polígono. Como P é convexo, eliminando V e emendando os dois vértices adjacentes a V, vamos formar um polígono P' de k lados e ainda convexo (veja figura).



Daí, como $p(k)$ é por hipótese verdadeira, temos que P' tem para soma de seus ângulos internos o número $(k-2)\cdot 180°$. Ora, P pode ser visto como a "emenda" de P' com o triângulo cujos vértices são V e seus adjacentes. Portanto, a soma dos ângulos internos de P é igual à soma dos ângulos internos de P' (que, por hipótese, vale $(k-2)\cdot 180°$) com os ângulos internos de tal triângulo (que, pela base de indução, sabemos ser igual a $180°$). Ou seja:

$$(k-2)\cdot 180° + 180° = (k-1)\cdot 180°,$$

o que mostra que a afirmação $p(k+1)$ é também verdadeira. Pelo Princípio da Indução, conclui-se que, para todo inteiro $n \geqslant 3$, a soma das medidas dos ângulos internos de qualquer polígono convexo de n lados é igual a $(n-2)\cdot 180°$.

CQD.

Exemplo 1.61 (Indução no contexto da Trigonometria) -

Provemos que, para todo inteiro $n \geqslant 2$ e todo ângulo a, vale:

$$\operatorname{sen}(2^n a) = 2^n \operatorname{sen} a \cdot \cos a \cdot \cos(2a) \ldots \cos(2^{n-1}a)\,.$$

Prova:

Seja $p(n)$ a afirmação

$$\operatorname{sen}(2^n a) = 2^n \operatorname{sen} a \cdot \cos a \cdot \cos(2a) \ldots \cos(2^{n-1}a)\,.$$

Temos, então, que $p(2)$ corresponde a $\operatorname{sen}(2a) = 2 \operatorname{sen} a \cdot \cos a$. Que essa identidade é verdadeira segue da lei dos senos, para dois ângulos quaisquer a e b:

$$\operatorname{sen}(a+b) = \operatorname{sen} a \cdot \cos b + \cos a \cdot \operatorname{sen} b\,. \qquad (*)$$

Com efeito, basta tomarmos $a = b$. Suponhamos, agora, que k é um inteiro maior ou igual a 2 e que $p(k)$ é verdadeira. Ou seja, supondo que vale

$$\operatorname{sen}(2^k a) = 2^k \operatorname{sen} a \cdot \cos a \cdot \cos(2a) \ldots \cos(2^{k-1} a), \quad (**)$$

provemos que $p(k+1)$ é também verdadeira. Ora, podemos escrever

$$\begin{aligned}
\operatorname{sen}(2^{k+1} a) &= \operatorname{sen}(2^k a + 2^k a) \stackrel{(*)}{=} \\
&= 2 \operatorname{sen}(2^k a) \cdot \cos(2^k a) \stackrel{(**)}{=} \\
&= 2 \left(2^k \operatorname{sen} a \cdot \cos a \cdot \cos(2a) \ldots \cos(2^{k-1} a) \right) \cdot \cos(2^k a) \\
&= 2^{k+1} \operatorname{sen} a \cdot \cos a \cdot \cos(2a) \ldots \cos(2^{k-1} a) \cdot \cos(2^k a),
\end{aligned}$$

e, portanto, $p(k+1)$ é também verdadeira.

Pelo Princípio da Indução, podemos concluir que, para todo todo ângulo a e todo inteiro $n \geq 2$, vale a fórmula

$$\operatorname{sen}(2^n a) = 2^n \operatorname{sen} a \cdot \cos a \cdot \cos(2a) \ldots \cos(2^{n-1} a).$$

CQD.

Os exemplos anteriores servem para mostrar a utilidade da indução matemática. Note que, em geral, precisa-se ter bastante cuidado na sua aplicação. Os exercícios que seguem apresentam *erros de raciocínio* na aplicação do Princípio da Indução Matemática, e o leitor é convidado a descobrir a falha de cada um deles.

Exercício 13 -

Seja a afirmação:
"Em qualquer grupo de pessoas, todas têm o cabelo da mesma cor".
Obviamente, ela é falsa. Assim, pede-se mostrar onde está o erro de raciocínio na seguinte pretensa prova de sua veracidade:

Prova por indução no número n de pessoas do grupo. Para $n = 1$, a afirmação é trivialmente verdadeira. Supondo válida para um grupo de k pessoas, mostremos que vale para grupos de $k+1$ pessoas. Dado um grupo de $k+1$ pessoas, pela hipótese de indução, no subgrupo das suas k primeiras pessoas, todas elas têm o cabelo da mesma cor, e isto também ocorre no subgrupo das k últimas pessoas do grupo dado. Ora, esses dois subgrupos têm uma pessoa em comum, e então todas as $k+1$ pessoas dadas têm o cabelo da mesma cor.

Exercício 14 -

Seja a afirmação:
"todos os números inteiros positivos são ímpares".
Obviamente, ela é falsa. Assim, pede-se mostrar onde está o erro de raciocínio na seguinte pretensa prova de sua veracidade:

Prova por indução. O primeiro inteiro positivo, 1, é ímpar. Além disso, se os k primeiros inteiros positivos forem ímpares, então $k+1=(k-1)+2=$ *ímpar + par = ímpar. Logo, pelo Princípio da Indução, concluímos a veracidade do que foi afirmado.*

Exercício 15 -

Seja a afirmação:

$$1+2+3+\cdots+n=\frac{(2n+1)^2}{8},\quad \forall n\geqslant 1.$$

Obviamente, ela é falsa. Assim, pede-se mostrar onde está o erro de raciocínio na seguinte pretensa prova de sua veracidade.

Prova:
Escrevamos $S_n=1+2+\cdots+n$*, para cada* $n\geqslant 1$*. Suponhamos que a fórmula*

$$S_n=\frac{(2n+1)^2}{8}$$

seja válida para um certo natural n*, e mostremos que ela também é válida para* $n+1$ *:*

$$\begin{aligned} S_{n+1} &= S_n+(n+1)=\frac{(2n+1)^2}{8}+(n+1)\\ &= \frac{4n^2+4n+1}{8}+(n+1)=\frac{4n^2+4n+1+8n+8}{8}\\ &= \frac{4n^2+12n+9}{8}=\frac{(2n+3)^2}{8}=\frac{[2(n+1)+1]^2}{8}. \end{aligned}$$

Logo, pelo Princípio da Indução,

$$S_n=\frac{(2n+1)^2}{8},$$

para cada $n\geq 1$.

Exercício 16 -

Prove que $3^{3n+3} - 26n - 27$ *sempre é um múltiplo de* 169, *qualquer que seja* n *inteiro positivo.*

Teorema 1.62 (Princípio da Indução Matemática Completa) -

Consideremos uma sequência de proposições $p(n)$, *indexadas por uma variável inteira* n. *Seja* α *um valor particular, tipicamente inicial, de* n. *Supondo que:*

i). a afirmação $p(\alpha)$ *seja verdadeira;*

ii). a implicação "$p(\alpha), p(\alpha+1), \ldots, p(k)$ *todas* $V \Rightarrow p(k+1)$ *é* V*" seja verdadeira, para cada* $k \geqslant \alpha$,

então, a proposição $p(n)$ *é verdadeira para todos os inteiros* $n \geqslant \alpha$.

Usando a analogia dos dominós, o leitor pode facilmente se aperceber da utilidade desta variante do Princípio da Indução Simples. Esta ocorre quando uma pedra do dominó não tem "força" suficiente para derrubar a seguinte da fileira. A queda só será garantida quando todos os anteriores "juntarem-se" para derrubar a seguinte.

Uma aplicação clássica ocorre no estudo da sequência de Fibonacci: $F_1, F_2, F_3, \ldots$, onde se tem que $F_1 = 1, F_2 = 1$ e a partir daí: $F_n = F_{n-1} + F_{n-2}$, $\forall n \geqslant 3$. Assim, por exemplo: $F_3 = F_2 + F_1 = 1 + 1 = 2$, $F_4 = F_3 + F_2 = 2 + 1 = 3$ etc. Não é trivial induzirmos a lei de formação dos termos desta sequência, mas podemos provar muitas de suas propriedades por indução. Só que é fácil ver que isso não poderá ocorrer com Indução Simples, uma vez que o valor da "pedra" F_{k+1} depende do valor tanto de F_k, como de F_{k-1}. A saída é usarmos Indução Completa.

Infelizmente, não temos aqui espaço e utilidade para esta variante do Princípio da Indução, e não voltaremos mais a falar sobre ela.

Terminando, alertemos o leitor que o uso de indução, para mostrar que uma afirmação vale para todo número natural, não é uma obrigatoriedade. Por exemplo, a fórmula da soma dos n primeiros termos de uma progressão aritmética pode ser demonstrada tanto por indução, como sem indução.

CAPÍTULO 2

NÚMEROS INTEIROS

Neste livro, consideramos como conhecidas do leitor as quatro operações aritméticas com inteiros, suas propriedades, e a representação decimal posicional destes números. Também assumimos como familiares ao leitor os conceitos de divisibilidade e fatoração de números naturais, incluindo a noção de mdc, bem como seus resultados básicos. Tudo isso, em nível de Ensino Fundamental.

De modo que possamos fazer referências precisas ao que precisaremos desses resultados, faremos, neste capítulo, uma rápida abordagem dos mesmos, insistindo mais nos teoremas básicos da divisibilidade e fatoração. Dependendo de seu preparo, o leitor pode usar este capítulo ou para uma revisão objetiva, ou como mera fonte para as referências que serão feitas nos próximos capítulos.

2.1 Notações, conceitos e resultados preliminares

Será cômodo termos uma notação para denotarmos, de modo rápido e preciso, o conjunto dos números inteiros e alguns de seus subconjuntos importantes:

$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$
conjunto dos números inteiros, ou inteiros relativos
(a letra Z vem do alemão: Zahl = número)

$\mathbb{N} = \{0, 1, 2, 3, \cdots\}$
conjunto dos números naturais ou inteiros absolutos

$\mathbb{Z}^*$ e $\mathbb{N}^*$
conjuntos que resultam ao tirarmos o número zero de $\mathbb{Z}$ e $\mathbb{N}$, respectivamente.
(Atente o leitor que muitos autores denotam por $\mathbb{N}$ o que denotamos por $\mathbb{N}^*$).

Exercício 17 -

Considere uma proposição quantificada da forma:

$$\text{quant } x \in A : \; x > 0,$$

onde quant *representa algum dos quantificadores* $= \forall, \exists, \exists!, \nexists$. *Pede-se decidir, para possibilidade de valor para* quant *e cada caso* $A = \mathbb{Z}, \mathbb{N}, \mathbb{N}^*$, *se a proposição resultante é verdadeira ou falsa.*

– adição e multiplicação de inteiros

Do Ensino Fundamental, nosso leitor já deve ter bastante familiaridade com as propriedades dessas operações aritméticas. Contudo, provavelmente não deve saber que há um conjunto básico delas, do qual saem todas as demais. Este conjunto expressa a natureza da estrutura algébrica do campo dos inteiros, $[\mathbb{Z}, +, \cdot]$. Confira no seguinte teorema:

Teorema 2.1 -

O campo dos inteiros, $[\mathbb{Z}, +, \cdot]$, *tem o seguinte conjunto de propriedades básicas: Para todos os* a, b, $c \in \mathbb{Z}$*:*

i). fechamento das operações $+$ *(adição) e* $\cdot$ *(multiplicação):*
$a + b \in \mathbb{Z}$ [*a operação* $+$ *é fechada*]
$a \cdot b \in \mathbb{Z}$ [*a operação* $\cdot$ *é fechada*]

ii). *associatividade das operações:*
$a + (b + c) = (a + b) + c$ [*associatividade da* $+$]
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ [*associatividade da* $\cdot$]

iii). *existência de elemento neutro para as operações:*
$a + 0 = a$ [0 *é elemento neutro da* $+$]
$a \cdot 1 = a$ [1 *é elemento neutro da* $\cdot$]

iv). *existência de inverso na adição:*
$\exists a' \in \mathbb{Z}$ *tal que* $a + a' = 0.$ [a' *é o simétrico de* a]
(a' *é único e costumamos indicá-lo por* $-a$)

v). *comutatividade das operações:*
$a + b = b + a$ [*comutatividade da* $+$]
$a \cdot b = b \cdot a$ [*comutatividade da* $\cdot$]

vi). *distributividade da multiplicação:*
$a \cdot (b + c) = a \cdot b + a \cdot c$ [*distributividade da* $\cdot$]

vii). *integridade da multiplicação:* $a \cdot b = 0 \Rightarrow a = 0$ *ou* $b = 0$ [*integridade da* $\cdot$]

Observação 2.2 -

Em sua formação matemática, o leitor encontrará outros campos numéricos verificando as propriedades acima. Dizemos que todos eles tem uma mesma estrutura algébrica, a qual é chamada de anel de integridade. *Assim, o campo dos inteiros,* $[\mathbb{Z}, +, \cdot]$, *é o mais simples e conhecido dos anéis de integridade.*

Exemplo 2.3 -

Como uma amostra bem pequena, mas crucial, da capacidade de geração de resultados desse conjunto básico de propriedades, provemos que o simétrico de cada número inteiro é único.

Para isso, usaremos que a existência de elemento neutro (o zero) e a comutatividade da adição nos permitem afirmar: $0 = b + b' = b' + b$, *bem como* $0 + b = b + 0 = b$, *qualquer que seja o inteiro* b.

Passando à prova da unicidade alegada, raciocinemos por absurdo. Se a' *e* a'' *fossem simétricos de* a, *poderíamos escrever:*

$$a' = 0+a' = (a+a'')+a' = a+(a''+a') = a+(a'+a'') = (a+a')+a'' = 0+a'' = a''.$$

(*Fica para o leitor apontar, em cada passagem acima, qual das propriedades do anel de integridade foi usada.*)

Essa unicidade é importante, pois é exatamente ela que nos permite definir a operação de subtração *de inteiros, e usar a notação* $-a$ *sem ambiguidade. Com efeito, fazemos isso por meio de*

$$a - b \stackrel{\text{def.}}{=} a + b' = a + (-b),\ \forall a, b \in \mathbb{Z}\,.$$

Como uma amostra mais significativa da capacidade de geração de resultados das propriedades caracterizando o anel de integridade, provemos formalmente as muito importantes leis do cancelamento na adição e multiplicação de inteiros:

Proposição 2.4 (leis do cancelamento) -

Sendo a, b *números inteiros:*

i). $a + c = b + c \Rightarrow a = b, \quad \forall\, c \in \mathbb{Z}$

ii). $a \cdot c = b \cdot c \Rightarrow a = b, \quad \forall\, 0 \neq c \in \mathbb{Z}$

Prova:

– Para (i)
Temos que, sendo $x, y, z \in \mathbb{Z}$, de $x = y$, segue: $x + z = y + z$. Daí, de $a + c = b + c$ sai $(a+c) - c = (b+c) - c$, e, pela associatividade, $a + (c - c) = b + (c - c)$, ou seja: $a + 0 = b + 0$. Assim, pelo fato de 0 ser elemento neutro da adição, $a = b$.

– Para (ii)
De $ac = bc$ tiramos $ac - bc = bc - bc = 0$. Usando a comutatividade e distributividade da multiplicação, podemos escrever $0 = ac - bc = ca - cb = c \cdot (a - b) = 0$. Mas o produto de dois inteiros só pode dar zero quando ao menos um deles for zero (pela integridade da multiplicação), daí, como $c \neq 0$, segue: $a - b = 0$. CQD.

Exercício 18 -

No raciocínio acima, a passagem $ca - cb = c \cdot (a - b)$ *está, a rigor, usando a distributividade da multiplicação na subtração. Prove detalhadamente que isso realmente é verdade.*

Exercício 19 -

Raciocinando estritamente a partir das propriedades de anel de integridade, mostre que:

i). $0 \cdot a = 0, \quad \forall a \in \mathbb{Z}$
(*Dica:* $aa = (a+0)a = \cdots$);

ii). $(-1)a = -a, \quad \forall a \in \mathbb{Z}$
(*Dica:* $0 = 0a = (1+1')a = \cdots$).

– relação de ordem nos inteiros

Iremos supor conhecido do leitor que em $\mathbb{Z}$ está definida uma relação de ordem, denotada por $a > b$ ou $b < a$ e que significa que $a - b \in \{1, 2, 3, \dots\}$.

Em particular, como $a - 0 = a$, temos que $a > 0$ quando, e só quando, tivermos $a \in \{1, 2, 3, \dots\}$. Assim, escrever $a > b$, é o mesmo que escrever $a - b > 0$.

Com isso, o conjunto $\mathbb{Z}$ dos números inteiros fica dividido em três partes disjuntas:

- $\mathbb{Z}^+ = \{1, 2, 3, \dots\} = \mathbb{N}^*$
  que fica "rebatizado" como conjunto dos *inteiros positivos*, pois pode ser dito que é o conjunto dos inteiros x, tais que $x > 0$
- $\mathbb{Z}^- = \{\dots, -3, -2, -1\}$
  conjunto dos *inteiros negativos*, ou conjunto dos inteiros x com $x < 0$
- $\{0\}$
  o conjunto formado pelo número zero.

Supomos que o leitor também conheça as notações $a \geqslant b$ (que significa que ou $a > b$ ou $a = b$) e $a \leqslant b$ (que significa que ou $a < b$ ou $a = b$).

Ademais, supomos sabido que as relações de ordem $<$ e $\leqslant$ são compatíveis com a adição e a multiplicação, conforme é especificado nos seguintes resultados:

Proposição 2.5 -

Sendo $a, b, c \in \mathbb{Z}$:

i). a relação de ordem é preservada *na adição:*
$a < b \iff a + c < b + c, \quad \forall c \in \mathbb{Z},$
$a \leqslant b \iff a + c \leqslant b + c, \quad \forall c \in \mathbb{Z}.$

ii). a relação de ordem é preservada *na multiplicação por inteiros positivos:*
$a < b \iff a \cdot c < b \cdot c, \quad \forall c > 0,$
$a \leqslant b \iff a \cdot c \leqslant b \cdot c, \quad \forall c > 0.$

iii). a relação de ordem é invertida *na multiplicação por inteiros negativos:*
$a < b \Longleftrightarrow a \cdot c > b \cdot c, \quad \forall c < 0,$
$a \leqslant b \Longleftrightarrow a \cdot c \geqslant b \cdot c, \quad \forall c < 0.$

(Costuma-se dizer que as propriedades (i) e (ii) atestam que, no campo dos números inteiros, a relação de ordem é compatível com a adição e a multiplicação.)

Observação 2.6 -

Como a relação entre a ordem e a multiplicação é fonte de frequentes confusões entre alunos, reescrevamos as propriedades (ii) e (iii) da proposição anterior de um modo mais concreto:

$$\begin{aligned} a < b &\Rightarrow\ 2a < 2b,\ 3a < 3b, \cdots \\ &\Rightarrow\ -a > -b,\ -2a > -2b,\ -3a > -3b, \cdots \end{aligned}$$

Resultados semelhantes para o caso $a \leqslant b$. Escreva-os!

Prova:

Demonstraremos explicitamente os casos $<$, sendo que os casos $\leqslant$ constituem imediata adaptação, que fica para o leitor. Também fica como exercício para o leitor apontar em cada etapa da demonstração abaixo qual propriedade do Teorema 2.2 está sendo usada.

– Para (i)
$a < b$ é o mesmo que $b - a > 0$. Somando e subtraindo c, obtemos $(b+c)-(a+c) > 0$, ou seja, $a + c < b + c$.

– Para (ii)
Para qualquer inteiro $x > 0$, é imediato que $2x,\ 3x \cdots > 0$, ou seja: $x > 0 \Rightarrow cx > 0$, para todo c inteiro positivo.
Supondo, então, que $a < b$, temos $b - a > 0$ e, então, $c \cdot (b - a) > 0$, para todo c inteiro positivo. Resta observar que $c \cdot (b - a) = bc - ac$ e que $bc - ac > 0$ significa $ac < bc$.

– Para (iii)
Para qualquer inteiro $x > 0$, é imediato que $-x,\ -2x,\ -3x \cdots < 0$, ou seja: $x > 0 \Rightarrow cx < 0$, para todo c inteiro negativo.
Supondo, então, que $a < b$, temos $b - a > 0$ e, então, $c \cdot (b - a) < 0$, para todo c inteiro negativo. Resta observar que $c \cdot (b - a) = bc - ac$, e que $bc - ac < 0$ significa $ac > bc$. CQD.

Exercício 20 -

Conclua a demonstração da proposição anterior, provando os casos envolvendo $\leqslant$.

Exercício 21 -

Mostre que as propriedades abaixo são consequências da última proposição:

i). $a < b$ *e* $c < d \;\Rightarrow\; a + c < b + d$ *;*

ii). $0 < a < b$ *e* $0 < c < d \;\Rightarrow\; a \cdot c < b \cdot d$
(Cuidado! Note que neste item exige-se $a, b, c, d > 0$*. Com efeito, prove que esta exigência é essencial).*

Exercício 22 -

Mostre que no item (ii) do exercício anterior é imprescindível termos $a, b, c, d > 0$.

– propriedade arquimediana[1] dos inteiros

Proposição 2.7 -

A relação de ordem do campo dos números inteiros tem a propriedade arquimediana: *dado um número inteiro* $\delta > 0$*, para cada escolha de* $k \in \mathbb{Z}$*, sempre é possível encontrar* $n \in \mathbb{N}$ *tal que* $k < n\delta$.

O leitor deve ver δ como sendo um módulo com o qual procuramos fazer uma estimativa da magnitude de k.

Prova:

Os casos $k \leqslant 0$ são triviais, pois verificam que $k \leqslant 0 < \delta$. Nos casos em que $k > 0$, temos que $\delta \geqslant 1$ implica $2k\delta \geqslant 2k > k$.

CQD.

Exemplo 2.8 -

Observe que a verificação da propriedade $k < n\delta$ *é imediata nos casos em que o módulo* $\delta \geqslant k$*. Com efeito,* $n = 1$ *já serve nos casos* $k < \delta$*, e no caso* $k = \delta$*, o menor* n *que serve é* $n = 2$.

[1] De Archimedes, matemático que viveu no mundo grego, lá por cerca de 200 AC.

Por exemplo, sendo $\delta = 2$, temos que $n = 1$ serve para $k < 2$. Enquanto que $k = 2$ nos força tomar $n = 2$. Tomando $k = 100$, como $100 = 2 \times 50$, o menor n que serve é 51.

Observação 2.9 -

Podemos ver a propriedade arquimediana do campo dos números inteiros como dizendo que, para cada inteiro $\delta > 0$, temos que a sequência de seus múltiplos naturais não apenas cresce incessantemente:

$$\delta < 2\delta < 3\delta < \cdots ,$$

como cresce infinitamente, na medida que, cedo ou tarde, ultrapassa toda e qualquer cota inteira k.

– valor absoluto de um número inteiro

Definição 2.10 -

O valor absoluto $|a|$ de un número inteiro $|a|$ é definido como:

$$|a| = \begin{cases} a \text{ se } a \geqslant 0 \\ -a \text{ se } a < 0 \end{cases}$$

Exemplo 2.11 -

$|-2| = 2 = |2|$,
$|0| = 0$.

Intuitivamente falando, tomar o valor absoluto de um número inteiro consiste em deixá-lo inalterado se o número for positivo ou nulo; e apagar seu sinal, caso ele seja negativo.

Usaremos o valor absoluto mais como uma notação. Não necessitaremos conhecer suas inúmeras propriedades.

– conceitos básicos de divisibilidade

Um defeito do campo dos números inteiros é que nem sempre conseguimos achar soluções x inteiras para equações do primeiro grau: $\alpha x = \beta$, com $\alpha \neq 0$, $\beta \in \mathbb{Z}$. Por exemplo, é impossível achar alguma solução $x \in \mathbb{Z}$ verificando a equação $2x = 3$. Contudo, existe solução inteira para a equação $2x = 4$, ela é $x = 2$.

Uma ideia que nos permite caracterizar as equações de primeiro grau que têm solução (tudo isso em $\mathbb{Z}$) é a de divisor, a qual passaremos a recordar.

Definição 2.12 -

Divisor de um dado número inteiro a é todo inteiro b capaz de transformar o inteiro dado num produto de inteiros: $a = b \cdot c$, para algum número inteiro c.
Sempre que b for divisor de a, também costuma-se empregar as seguintes terminologias alternativas, sinônimas:

- *"o inteiro b divide a", o que abreviamos com a notação: $b|a$;*
- *"o inteiro a é um múltiplo de b".*

Exemplo 2.13 -

- *os divisores de $a = 4$ são $b = -2, -1, 1, 2$.*
  Com efeito: todos eles são não nulos e temos, respectivamente:
  $4 = (-2) \cdot (-2)$, $4 = (-1) \cdot 1$, $4 = 1 \cdot 4$, $4 = 2 \cdot 2$.
- *$b = -3$ é um dos divisores de $a = -15$, pois $-15 = (-3) \cdot 5$*
- *os divisores de $a = 0$ são todos os inteiros b.*

Cuidado:
– zero só é divisor dele mesmo;
– todos os inteiros são divisores do zero.

Exemplo 2.14 -

Sendo α e β números inteiros, a equação $\alpha x = \beta$ tem solução x inteira $\iff$ α é divisor de β. Mais detalhadamente:

- *se $\alpha \neq 0$ e é divisor de β, então a lei do cancelamento nos mostra que há exatamente uma solução;*
- *se $\alpha = 0$ e é divisor de β, então necessariamente $\beta = 0$ e todos os x inteiros são solução da equação.*

Observação 2.15 -

Note que no Ensino Fundamental o conceito de divisor é apresentado tão somente no contexto dos números naturais. Aqui e em Teoria dos Números, consideramos divisor para números inteiros quaisquer, mesmo os negativos. Como consequência, todo número inteiro tem tanto divisores positivos como negativos. Mais precisamente, o leitor certamente não terá nenhuma dificuldade de provar que

se b for divisor de a, então $-b$ também é, e reciprocamente.

Exercício 23 -

i). Prove a última afirmação acima;
ii). Prove que se a é divisor de b e b é divisor de a, então ou $a = b$, ou $a = -b$.

Exercício 24 -

Sendo a, b, c números inteiros, prove que:

i). $c|a \Rightarrow c|ab$;
ii). $b|a \Rightarrow b|a^2$.

Exercício 25 -

Sendo a, b, c números inteiros: $[\ c|ab \Rightarrow c|a$ ou $c|b\ ]$. Verdade, ou falso?

– combinação linear inteira de números inteiros

Esta é a primeira noção da Teoria dos Números que o leitor encontra neste texto e que não foi estudada no Ensino Fundamental. Trata-se de uma noção pouco natural para o contexto, tanto é que surgiu bem tardiamente, com os estudos do francês E. Bézout, um escritor de vários livros-texto muito populares, por volta de 1 770.

Definição 2.16 -

Chamamos de combinação linear inteira de dois números inteiros, a e b, toda expressão da forma:

$$ma + nb, \quad onde \;\; m, n \in \mathbb{Z}.$$

Exemplo 2.17 -

O inteiro 6 *pode ser escrito como uma combinação linear inteira de* 4 *e* 5*. Com efeito,* $6 = 4 \cdot 4 + (-2) \cdot 5$*.*
A soma e a diferença de a *e* b *podem ser vistas como combinações lineares inteiras dos mesmos:* $a + b = 1 \cdot a + 1 \cdot b$*, e* $a - b = 1 \cdot a + (-1) \cdot b$*.*

Proposição 2.18 -

Se um número inteiro c *divide outros dois inteiros,* a *e* b*, então* c *divide qualquer combinação linear inteira de* a *e* b*.*
Simbolicamente: $c|a$ *e* $c|b \ \Rightarrow\ c|(ma + nb),\ \forall m, n \in \mathbb{Z}$*.*

Prova:

Pela hipótese: $a = Mc$ e $b = Nc$, para inteiros M, N adequados. Daí: $ma + nb = mMc + nNc = (mM + nN)c$. CQD.

Adiante, veremos que a noção de combinação linear nos permite provar facilmente vários resultados da Teoria dos Números.

– número primo e números relativamente primos

Definição 2.19 -

Como 1, -1, a, $-a$ *sempre são divisores de cada número inteiro* $a \neq 0$*, dizemos que eles são os* divisores triviais*, ou os* divisores impróprios*, de* a*.*

> Nos casos $a = 1$ e $a = -1$, obviamente, temos exatamente dois divisores triviais. Contudo, em todos os demais casos de $a \neq 0$, temos exatamente quatro divisores triviais. Não levar em conta esta diferença entre os casos $a = \pm 1$ e $a \neq 0, \pm 1$, por mais óbvia que seja, é "meio caminho andado" para se chegar a erros graves.

Exercício 26 -

Mostre que dizer que um inteiro não nulo tem quatro, ou mais divisores equivale a dizer que ele é distinto de 0, ± 1*.*

Definição 2.20 -

Número primo é todo inteiro $p \neq 0, \pm 1$ *cujos divisores são todos triviais. Isto equivale a dizer que um número primo é todo inteiro* p *com exatamente quatro divisores:* $p, -p, 1, -1$.

Exemplo 2.21 -

Os menores primos positivos são:

$$2, 3, 5, 7, 11, \ldots\ .$$

Obviamente, o único inteiro positivo par primo é 2. *Ademais, note que um inteiro positivo ímpar pode ser primo* ($como\ é\ o\ caso\ de$ $3, 5, 7$) *ou não primo* ($o\ primeiro\ exemplo\ sendo$: 9).

Observação 2.22 -

É imediato se ver que a *é primo se, e somente se,* $-a$ *for primo. Consequentemente, basta estudarmos os primos positivos.*

Ademais, para verificar que um número inteiro positivo a *é primo, basta mostrarmos que seus únicos divisores positivos são* 1 *e* a.

> *Para isto, basta mostrarmos que não existe nenhum inteiro* b *estritamente entre* 1 *e* a *e que seja divisor de* a.

Convenção

Tanto pela observação anterior como pelo fato de que, neste livro, não teremos nenhum uso para primos negativos, de agora em diante, *sempre que nos referirmos a "número primo" estaremos querendo dizer "número primo positivo".* Este expediente tornará a leitura de nosso texto mais "leve".

Outro cuidado que o leitor deve ter é que alguns autores incluem o número 1 entre os primos. Adiante, quando tratarmos do Teorema Fundamental da Aritmética, teremos uma melhor oportunidade de dar uma boa razão para não considerarmos 1 como primo.

Exercício 27 -

Prove as afirmações feitas na última observação.

Exercício 28 -

Tome vários livros-texto do Ensino Fundamental e observe as definições lá dadas para número primo. Compare seu teor matemático com o da definição acima.

Nota histórica:
O mais antigo texto conhecido tratando dos números primos é o livro *Elementos* de Euclides, escrito c. 300 AC. Em certa parte do mesmo, Euclides trata da medida de segmentos de reta. Tendo escolhido um segmento padrão, ou unitário, ele constrói segmentos inteiros por sucessivas justaposições do padrão. Numericamente, isto corresponde a escrever:

$$1 = 1,\ 2 = 1 + 1,\ 3 = 1 + 1 + 1,\ 4 = 1 + 1 + 1 + 1, \cdots$$

A seguir, Euclides observa que muitos segmentos inteiros também podem ser medidos tomando como padrão de medida segmentos inteiros não unitários. Numericamente, isso equivale a observar igualdades como:

$$4 = 2 + 2,\ 6 = 2 + 2 + 2 = 3 + 3,\ 9 = 3 + 3 + 3, \cdots$$

Esse tipo de segmentos inteiros Euclides denominou de *compostos* e aos demais (ou seja, os que só podem ser medidos por meio do segmento unitário) ele chamou de *incompostos*. As primeiras medidas incompostas, segundo Euclides, são:

$$1 = 1,\ 2 = 1 + 1,\ 3 = 1 + 1 + 1,\ 5 = 1 + 1 + 1 + 1 + 1, \text{ etc.}$$

Assim, as medidas incompostas correspondem ao número 1 e mais os números primos. Logo, podemos dizer que, para Euclides, 1 era primo. Mais tarde, se viu que existem vários inconvenientes em se considerar 1 como primo, daí a definição que demos anteriormente e que é a usada pela grande maioria dos textos atuais.

Complementando, o matemático Fibonacci, em seu famoso livro *Liber Abacci*, escrito por volta do ano 1 200, popularizou a denominação *primos* para os incompostos. Isso porque considerava-se os primos como de origem primária e os não-primos como de secundária, pois podem ser escritos como produto dos primários. (Vide Teorema Fundamental da Aritmética, que recordaremos adiante.)

Definição 2.23 -

Número composto é todo inteiro $k \neq 0$ que tem ao menos um divisor não trivial. Isto equivale a dizer que um número composto é todo inteiro $k \neq 0$ com cinco ou mais divisores.

Observação 2.24 -

Cuidado!
Dizer que não é primo não é o mesmo que dizer que é composto. Devido a isto, neste livro, procuraremos evitar a terminologia "composto".

Ademais, observe que, ao contrário de Euclides, tratamos tanto de inteiros positivos como dos negativos e do zero, sendo assim, nossa terminologia não corresponde exatamente à dele.

Definição 2.25 -

Chamamos de divisor comum *de dois, ou mais números inteiros dados a todo inteiro que seja divisor de cada um desses inteiros.*

Exemplo 2.26 -

Os divisores de 8 *são* $\pm1, \pm2, \pm4, \pm8$, *enquanto que os divisores de* 12 *são* $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$. *Assim, os divisores comuns de* 8 *e* 12 *são* $\pm1, \pm2, \pm4$.

Definição 2.27 -

Dizemos que dois números inteiros são relativamente primos *se tiverem como divisores comuns apenas os divisores triviais* $+1$ *e* -1.

Exemplo 2.28 -

Vejamos a relação entre paridade e relativamente primos.

- *Dois inteiros pares nunca são relativamente primos.*
  Com efeito: 2 *sempre é divisor comum de duplas de pares.*
- *Dois inteiros ímpares podem ser, ou não, relativamente primos.*
  Com efeito: 3 *e* 5 *tem apenas* 1 *como divisor comum, enquanto que* 3 *e* 9 *tem* 1 *e* 3 *como divisores comuns.*
- *Um inteiro par e um ímpar também podem ser, ou não, relativamente primos.*
  Com efeito: verifique que 6 *e* 3 *não são relativamente primos, mas* 2 *e* 3 *são.*

Exemplo 2.29 -

Quaisquer dois inteiros primos (distintos) são relativamente primos. Com efeito, indicando-os por p *e* q, *os divisores de* p *são* ±1, $\pm p$ *e os de* q *são* ±1, $\pm q$.

A recíproca é falsa. Por exemplo, 4 e 9 são relativamente primos, mas nenhum deles é primo.

Exemplo 2.30 -

Para qualquer número inteiro a, temos que a e $a+1$ são relativamente primos.
Com efeito: é imediato vermos que todo divisor comum de dois inteiros tem de ser também divisor da sua diferença; em particular, todo divisor de a e $a+1$ também é divisor de $(a+1)-a=1$; logo, tem de ser igual a ± 1.

Proposição 2.31 -

Todo número primo que não dividir um inteiro dado, é relativamente primo com o mesmo.

Prova:

Sendo p o número primo e a um número inteiro, como os únicos divisores de p são ± 1 e $\pm p$, e como p não divide a, segue que os únicos divisores comuns entre p e a são ± 1. CQD.

Exercício 29 -

- *i). Por que dois ímpares consecutivos sempre são relativamente primos?*
- *ii). Achar condição garantindo que dois inteiros que diferem por três unidades sejam relativamente primos.*
- *iii). Se um inteiro é divisível por dois inteiros consecutivos, ele também será divisível pelo produto deles?*

– máximo divisor comum

Definição 2.32 -

Chamamos de máximo divisor comum *de dois ou mais números inteiros dados ao maior dos divisores comuns desses inteiros.*
A notação $\mathrm{mdc}\,(a,b)$ indicará o máximo divisor comum dos inteiros a,b.

Exemplo 2.33 -

Temos $\mathrm{mdc}\,(6,9)=3$, pois os divisores comuns de 6 e 9 são ± 1 e ± 3.

Exemplo 2.34 -

Sendo b um número inteiro:

$$\operatorname{mdc}(0,b) = \begin{cases} |b| & \textit{se } b \neq 0 \\ \textit{não existe, se } b = 0\,. \end{cases}$$

Esses casos são considerados excepcionais. Na prática, estaremos interessados nos casos onde ambos, a e b, são não nulos.

Observação 2.35 -

Note que:

- *o* $\operatorname{mdc}(a,b)$ *sempre existe, a menos que $a = b = 0$.*
  Com efeito, o conjunto dos divisores comuns de qualquer conjunto de dois, ou mais números inteiros nunca é vazio (pois ± 1 sempre são divisores comuns deles) e é finito (pois os divisores de $c \neq 0$ estão entre c e $-c$).
- *o* $\operatorname{mdc}(a,b) \geqslant 1$*, em particular, sempre é positivo.*
  Novamente usamos que 1 sempre é divisor comum de qualquer par de inteiros.
- $\operatorname{mdc}(a,b) = \operatorname{mdc}(-a,b) = \operatorname{mdc}(a,-b) = \operatorname{mdc}(-a,-b)$.

Dizer que "a e b são relativamente primos" é o mesmo que escrever abreviadamente $\operatorname{mdc}(a,b) = 1$.

– conceitos básicos de fatoração

Há um ponto de vista dual ao da divisibilidade, que é o da fatoração, o qual passamos a recordar.

Definição 2.36 -

Sendo $a = b_1 \cdot b_2 \cdots b_n$, com $a, b_1, b_2, \ldots, b_n$ inteiros, dizemos que $b_1, b_2, \ldots, b_n$ são fatores *de a e que $b_1 \cdot b_2 \cdots b_n$ é uma* fatoração *deste a.*

O leitor deve ter cuidado, pois todo fator de um inteiro (não nulo) é divisor do mesmo, mas nem todo divisor pode estar sendo usado numa dada fatoração de tal inteiro.

Exemplo 2.37 -

Existem inteiros que têm várias fatorações (mesmo que consideremos como iguais as que têm os mesmos fatores só que escritos em ordem diferente):

$$12 = 2 \times 6 = 3 \times 4 = 2 \times 2 \times 3.$$

Essa variedade de fatorações fica ainda maior se considerarmos o fator 1*, que nos daria mais:*

$$12 = 1 \times 12 = 1 \times 2 \times 6 = etc.$$

Adiante, veremos que é perfeitamente possível eliminarmos essa variedade: basta aceitarmos apenas fatores primos e ordená-los em ordem não-decrescente ($\leqslant$)*. Este resultado será tornado preciso com o Teorema Fundamental da Aritmética, o último grande assunto deste capítulo. Antes, porém, precisamos discutir a chamada "divisão euclidiana".*

2.2 Teorema da divisão euclidiana

– A idéia de divisão:
consiste em "quebrar" um todo em partes iguais. Isto pode ser levado a cabo de modo *exato* (a união das partes dá exatamente o todo) ou de modo *inexato* (se ocorre o contrário); neste segundo caso estamos fazendo a chamada *divisão inexata.*

No contexto dos números inteiros, indicaremos por a o número que corresponde ao todo, e por b o número inteiro que corresponde ao valor de cada uma das partes iguais. Então:

- Dizer que podemos fazer a *divisão exata* de a por b equivale a dizer que existe um q inteiro tal que: $a = b \cdot q$.
- Dizer que podemos fazer a *divisão inexata* de a por b equivale a dizer que existe um q inteiro tal que: $a = b \cdot q + r$, onde o erro r tem magnitude menor do que a de b, ou seja: $|r| < |b|$.
  Na Teoria da Divisão, o erro r é chamado de *resto* da divisão.

Enquanto existe apenas uma maneira de fazermos uma divisão exata, há várias maneiras de fazermos uma divisão inexata. Numa primeira abordagem, podemos dividí-las em: inexatas por falta (como $20 = 7 \cdot 2 + 6$) e inexatas por excesso (como $20 = 7 \cdot 3 + (-1)$).

A divisão inexata mais utilizada em Matemática, e a única que usaremos neste texto, é uma divisão por falta chamada *divisão euclidiana*, que logo definiremos precisamente, e que é exemplificada pela divisão $20 = 7 \cdot 2 + 6$.

Um outro tipo clássico de divisão inexata é a *divisão com resto mínimo*, a qual, dependendo dos valores de a e b, pode corresponder a uma divisão por excesso, como em $20 = 7 \cdot 3 + (-1)$; ou a uma divisão por falta, como em $15 = 7 \cdot 2 + 1$.

Dados números inteiros a e b, o estudo de sua divisão inicia pelas questões de existência e unicidade da mesma. Inicialmente, vejamos como fica isso no caso da divisão exata.

– Existência e unicidade na divisão exata:

Dados a e b números inteiros, temos de considerar dois casos:

- $\mathbf{a \neq 0}$
  Como uma divisão de a por b significa achar q inteiro tal que $a = bq$, vemos que é impossível fazer divisão de $a \neq 0$ por $b = 0$. Resta examinarmos o que ocorre nos casos em que $b \neq 0$.
  Quando temos $a \neq 0$ e $b \neq 0$, toda divisão $a = bq$ tem de ter $q \neq 0$. Disso decorre facilmente que, ou ela é impossível (ou seja, nenhum q inteiro verifica $a = bq$), ou ela é possível com exatamente um q (basta aplicarmos a Lei do Cancelamento).

  Resumindo: sendo $a \neq 0$, é impossível fazer a divisão exata de a por $b = 0$; enquanto que a divisão exata por um inteiro $b \neq 0$ pode ser tanto impossível (como em $20 = 7q$) como possível, mas de uma única maneira, ou seja, com um único q. Este q, estando assim univocamente determinado, é chamado de quociente exato de a por b, ou simplesmente de quociente de a por b.

- $\mathbf{a = 0}$
  Para valer $0 = bq$: se $b = 0$, qualquer q inteiro serve; e se $b \neq 0$, somente $q = 0$ serve.

Podemos resumir esses resultados dizendo que:

Sendo a e b números inteiros, para falarmos num quociente univocamente determinado de a por b, é necessário termos $b \neq 0$. Mais precisamente:

- Se $a = 0$ e $b \neq 0$, a divisão exata de a por b sempre é possível e é única; o quociente é $q = 0$.
- Se $a \neq 0$ e $b \neq 0$, a divisão exata de a por b pode ser possível ou não; se possível, determina univocamente um quociente.
- Se $a = 0$ e $b = 0$, qualquer inteiro q verifica $a = bq$; de modo que, como não há unicidade da divisão, não tem sentido empregarmos a palavra quociente neste caso.
- Se $a \neq 0$ e $b = 0$, é impossível fazer a divisão exata de a por b; em particular, não há quociente.

Quando existe o quociente de a por b, da Definição 2.12, segue que b divide (exatamente) a. Em particular:

- se $b \neq 0$ for um divisor de a, então b divide a;
- se $b = 0$ for um divisor de a, então necessariamente $a = 0$; além disso, $b = 0$ não divide $a = 0$.

Assim que 0 é o único divisor que não divide nenhum inteiro.

– A divisão inexata chamada divisão euclidiana [2]

Como veremos em teorema logo a seguir, a divisão euclidiana permite estender o conceito de quociente de a por b aos casos em que b não é necessariamente um divisor de a, e isso sem ter de apelar para números não inteiros.

Definição 2.38 -

Fazer a divisão euclidiana *de um número inteiro a por um inteiro $b \neq 0$, consiste em achar uma decomposição da forma:*

$$a = b \cdot q + r, \text{ onde } q, r \text{ são inteiros, e com } 0 \leqslant r < |b|\,.$$

Denominações: q = quociente (euclidiano)*, r =* resto (euclidiano) *da divisão (euclidiana) de a por b.*

Exemplo 2.39 -

A divisão euclidiana de 20 por 7 é: $20 = 7 \cdot 2 + 6$ (de modo que $q = 2$, $r = 6$), enquanto que a de 2 por 11 é: $2 = 11 \cdot 0 + 2$ (logo, $q = 0$, $r = 2$).
A divisão euclidiana de -26 por 10 corresponde à decomposição: $-26 = (-3) \cdot 10 + 4$.
Confira isto e compare com a divisão euclidiana de $+26$ por 10 !
(Numa divisão euclidiana, o resto nunca é negativo.)

Observação 2.40 -

Evidentemente, quando $r = 0$, a divisão euclidiana coincide com a divisão exata. Por isso, dizemos que a divisão euclidiana generaliza a divisão exata entre números inteiros.

Teorema 2.41 (teorema da divisão euclidiana) -

Sendo a um número inteiro, e $b \neq 0$, também inteiro:

- *sempre é possível fazer a divisão euclidiana de a por $b \neq 0$;*
- *fixados a e $b \neq 0$, a partir deles, sempre obtemos o mesmo quociente euclidiano e o mesmo resto, não importando o procedimento usado para fazer sua divisão euclidiana.*

[2] No Ensino Fundamental, esta divisão é usualmente chamada de “a divisão com resto”; pelo que já vimos, isto não é uma caracterização exclusiva.

Prova:

• Existência
Os casos $a = 0$ tem divisão trivial: $a = 0 = 0 \cdot b + 0$. Por sua vez, os casos $b < 0$ saem dos de $b > 0$. Com efeito, dado um $b < 0$, como $-b > 0$, podemos escrever $a = (-b)q + r = b(-q) + r$, onde r verifica $0 \leqslant r < |-b| = |b|$.
Vejamos então o que ocorre nos casos em que $a \neq 0$, $b > 0$. Temos quatro possibilidades:

– Quando tivermos $0 < a < b$, é só colocar: $a = 0 \cdot b + a$.
– Quando tivermos $0 < a = b$, é só colocar: $a = 1 \cdot b + 0$.
– Quando tivermos $0 < b < a$, consideremos dois casos:

◇ a é um múltiplo de b
neste caso, temos: $a = q \cdot b + 0$, para algum inteiro positivo q.

◇ a não é um múltiplo de b
pela propriedade arquimediana (vide Observação 2.9), o valor de a terá de ficar "imprensado" entre dois valores sucessivos da sequência dos múltiplos de b. Ou seja, tem de existir um inteiro $q \geqslant 1$ tal que tenhamos:
$$0 < b < 2b < \cdots < qb < a < (q+1)b < \cdots .$$
De modo que $qb < a < qb + b$. Fica então fácil ver que a decomposição $a = qb + (a - qb)$ é euclidiana. Com efeito, resta só observar que $r = a - qb$ verifica a propriedade $0 \leqslant r < b$, pois temos: $qb - qb < a - qb < qb + b - qb$, ou seja, $0 < a - qb < b$.

– Quando tivermos $a < 0 < b$, um artifício nos remete ao caso anterior. Com efeito, como $-a > 0$, pelo caso anterior, achamos uma decomposição $-a = bq + r$, com $0 \leqslant r < b$. De modo que se $r = 0$, achamos nossa divisão euclidiana para (a, b), qual seja, $a = (-q)b + 0$. Se $0 < b < r$, precisamos ir mais longe. Mostremos que a seguinte decomposição é euclidiana para (a, b):

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

Com efeito, $(-q-1)$ é inteiro, e como $r < b$, segue que $(b - r) > 0$, e como $r > 0$ segue que $(b - r) < b$, ou seja, $0 < (b - r) < b$.

• Unicidade
Suponhamos que foram obtidas as divisões euclidianas: $a = bq + r$ e $a = bq' + r'$. Então:

– se $q = q'$, ficamos com $bq + r = bq + r'$, logo $r = r'$.
– se $q \neq q'$ teríamos um absurdo, pois sendo, por exemplo, $0 \leqslant q < q'$, ficaríamos com $r - r' = b \cdot (q' - q)$; ora, como $q' - q \geqslant 1$, disso seguiria que o valor de

$r - r'$ tem de estar na lista $b, 2b, 3b, \cdots$, o que é uma impossibilidade frente ao fato de que $0 \leqslant r, r' < |b|$, do qual sai que $|r - r'| < |b|$.

CQD.

Exemplo 2.42 -

Seja fazer a divisão euclidiana de 13 *por* 3.
Temos que

$$3 < 2 \cdot 3 < 3 \cdot 3 < 4 \cdot 3 < 13 < 5 \cdot 3 < \cdots$$

ou seja: $4 \cdot 3 = 12 < 13 = 12 + 1$. *Conclusão:* $13 = 4 \cdot 3 + 1$.

Exercício 30 -

Partindo da divisão euclidiana de 10 *por* 6*, mostre que* $10,\ 100,\ 1\,000, \ldots$ *são múltiplos de* 6 *aumentados de* 4.

Teorema 2.43 -

Um número inteiro que divide dois inteiros não nulos também divide o resto da divisão euclidiana deles.
Podemos melhorar isso dizendo que:
"os divisores comuns de dois inteiros $a \neq 0$ *e* $b \neq 0$*"*
são
"os divisores comuns de b *e* r*", onde* $a = qb + r$ *é a divisão euclidiana de* a *por* b.

Em particular:

$$\boxed{\mathrm{mdc}\,(a, b) = \mathrm{mdc}\,(b, r).}$$

Prova:

Sejam a, b, c inteiros e todos não nulos.
Supondo que c seja divisor de a e b, certamente ele terá de ser divisor do resto r da divisão euclidiana de a por b, pois r é uma combinação linear inteira de a e b. Com efeito: $r = a - qb$.
Reciprocamente, se c é divisor de b e de r, ele terá de ser divisor de a, pois a é uma combinação linear de b e r, a saber: $a = qb + r$.

CQD.

Exemplo 2.44 -

Como a divisão euclidiana de 84 *por* 35 *é* $84 = 35 \times 2 + 14$*, segue que*

$$\text{mdc}\,(84, 35) = \text{mdc}\,(35, 14) = 7.$$

Exercício 31 -

Qual o mdc *de dois inteiros cuja divisão euclidiana dá* 1 *como resto? Estes dois números podem ser consecutivos? Quando?*

Exercício 32 -

Seja $a = bq + r$*, a divisão euclidiana de* a *por* b*.*

i). Achar número que tenha como divisores todos os divisores comuns a a *e* b*.*

ii). Achar os pares de números que tenham como divisores comuns os mesmos divisores comuns de a *e* b*.*

Vejamos algumas aplicações da divisão euclidiana.

Teorema 2.45 (algoritmo de Euclides para o mdc) -

Para calcularmos o mdc de dois inteiros não nulos, a *e* b*, fazemos sucessivas divisões euclidianas, até obtermos um primeiro resto nulo. Chamando este resto de* $r_{n+1} = 0$*, e reescrevendo* b *como* $b = r_0$*, estas divisões se escrevem:*

$$\begin{aligned}
&a \;=\; b\,q_1 + r_1 = r_0 q_1 + r_1 \\
&r_0 = r_1 q_2 + r_2 \\
&r_1 = r_2 q_3 + r_3 \\
&r_2 = r_3 q_4 + r_4 \\
&\cdots \\
&r_{n-1} = r_n q_{n+1} + r_{n+1} = r_n q_{n+1}.
\end{aligned} \qquad (\,*\,)$$

Teremos, então, que

$$\text{mdc}\,(a, b) = r_n\,.$$

Ademais:

$$\text{mdc}\,(a, b) = \text{mdc}\,(b, r_1) = \text{mdc}\,(r_0, r_1) = \text{mdc}\,(r_1, r_2) = \cdots = \text{mdc}\,(r_{n-1}, r_n) = r_n.$$

Prova:

Como $0 \leqslant \cdots r_2 < r_1 < |b|$, e todos estes valores são inteiros, segue que, cedo ou tarde, acharemos um último resto não nulo. Indicando-o por r_n, temos:

$$r_{n-1} = r_n q_n + r_{n+1} = r_n q_n.$$

Pelo Teorema 2.43, essa igualdade implica que $\operatorname{mdc}(r_{n-1}, r_n) = \operatorname{mdc}(r_n, 0) = r_n$. Resta aplicarmos repetidamente aquele teorema para obtermos:

$$\operatorname{mdc}(a,b) = \operatorname{mdc}(b, r_1) = \operatorname{mdc}(r_0, r_1) = \operatorname{mdc}(r_1, r_2) = \cdots = \operatorname{mdc}(r_{n-1}, r_n).$$

De modo que $r_n = \operatorname{mdc}(r_{n-1}, r_n) = \operatorname{mdc}(a,b)$.

CQD.

Exemplo 2.46 -

Usando o algoritmo de Euclides, achar o mdc de 33 910 *e* 4 116.
Resolução:

x	y	q_k	r_k
33 810	4 116	8	882
4 116	882	4	588
882	588	1	294
588	294	2	0

Concluímos, então, que $\operatorname{mdc}(33\,810, 4\,116) = 294$.

Exercício 33 -

O Algoritmo de Euclides para o mdc *costuma ser apresentado no Ensino Fundamental sob a denominação de* Algoritmo da Grade. *Assim sendo, pede-se "remontar" a tabela acima no tal formato de grade.*

Teorema 2.47 (teorema de Bézout) -

O mdc *de dois números inteiros (não nulos) sempre pode ser escrito como uma combinação linear inteira dos mesmos.*
Simbolicamente: dados $a, b \in \mathbb{Z}^*$, existem $m, n \in \mathbb{Z}$ tais que

$$\boxed{\operatorname{mdc}(a,b) = ma + nb.}$$

Prova:

Do Algoritmo de Euclides para o mdc, é imediato que cada um dos restos envolvidos, do primeiro ao último, seja uma combinação linear de a e b. Vejamos:

$$\begin{aligned}
&a = bq_1 + r_1 = r_0q_1 + r_1 \;\rightarrow\; r_1 = a - bq_1 = M_1a + N_1b\\
&r_0 = r_1q_2 + r_2 \;\rightarrow\; r_2 = r_0 - r_1q_2 = b - (M_1a + N_1b)q_2 = M_2a + N_2b\\
&r_1 = r_2q_3 + r_3 \;\rightarrow\; r_3 = r_1 - r_2q_3 = M_1a + N_1b - (M_2a + N_2b)q_3 = M_3a + N_3b\\
&\ldots\\
&r_{n-2} = r_{n-1}q_n + r_n \;\rightarrow\; r_n = r_{n-2} - r_{n-1}q_n\\
&\qquad\qquad\qquad\qquad\qquad = M_{n-2}a + N_{n-2} - (M_{n-1}a + N_{n-1}b)q_n = M_na + N_nb.
\end{aligned}$$

CQD.

Exercício 34 -

Pede-se escrever o mdc $(389, 167)$ *como uma combinação linear inteira de* 389 *e* 167, *e isso de dois modos:*

i). Refazendo o raciocínio do Teorema 2.47.
*ii). Resolvendo as equações (*) daquele teorema na ordem inversa.*
iii). Compare as duas resoluções.

Resposta: $1 = 89 \times 389 + (-191) \times 167$.

Observação 2.48 -

O exercício anterior mostra que a expressão do mdc (a, b) , *em termos de uma combinação linear inteira de a e b , pode exigir trabalharmos com inteiros negativos. Ou seja, esse é um resultado que não pode ser formulado na Aritmética sobre o conjunto* $\mathbb{N}$ *dos números naturais, que é a estudada no Ensino Fundamental.*

Exercício 35 -

Prove que, se um inteiro positivo divide cada um de dois outros, então ele também divide o mdc *deles.*
Simbolicamente: sendo a, b, c inteiros positivos, $c|a$ e $c|b \Rightarrow c|$ mdc (a, b).

Observação 2.49 -

Na expressão mdc $(a, b) = ma + nb$ *os coeficientes inteiros, m e n, não são únicos.*

Com efeito, existem infinitas possibilidades para eles:

$$ma + nb = (m+b)a + (n-a)b = (m+2b)a + (n-2a)b = \cdots$$

Teorema 2.50 -

Para quaisquer números inteiros não nulos, a, b, c, temos:

$$\operatorname{mdc}(ac, bc) = |c| \cdot \operatorname{mdc}(a, b).$$

Prova:

Pela Observação 2.35, ou por prova direta: $\operatorname{mdc}(ac, bc) = \operatorname{mdc}(-ac, -bc)$; logo, $\operatorname{mdc}(ac, bc) = \operatorname{mdc}(a|c|, b|c|)$. Resulta disso que basta provarmos $\operatorname{mdc}(a|c|, b|c|) = |c| \operatorname{mdc}(a, b)$, que é o que passaremos a fazer.

Já sabemos que as seguintes igualdades produzidas na aplicação do algoritmo de Euclides para a, b:

$$\begin{aligned}
&a \;=\; b\,q_1 + r_1 = r_0 q_1 + r_1\\
&r_0 = r_1 q_2 + r_2\\
&r_1 = r_2 q_3 + r_3\\
&r_2 = r_3 q_4 + r_4\\
&\cdots\\
&r_{n-1} = r_n q_{n+1} + r_{n+1} = r_n q_{n+1}\,,
\end{aligned}$$

nos permitem afirmar que $r_n = \operatorname{mdc}(a, b)$.
Se multiplicarmos cada uma delas por $|c|$, ficamos com:

$$\begin{aligned}
&a|c| \;=\; b|c|\,q_1 + r_1|c| = r_0|c| \cdot q_1 + r_1|c|\\
&r_0|c| = r_1|c| \cdot q_2 + r_2|c|\\
&r_1|c| = r_2|c| \cdot q_3 + r_3|c|\\
&r_2|c| = r_3|c| \cdot q_4 + r_4|c|\\
&\cdots\\
&r_{n-1}|c| = r_n|c| \cdot q_{n+1}\,.
\end{aligned}$$

Ora, cada igualdade acima é uma divisão euclidiana que tem os mesmos quocientes que a correspondente na aplicação do algoritmo a a e b. Com efeito, resta observar que, como $|c| > 0$, os restos verificam: $0 \leqslant \ldots r_2|c| < r_1|c| < r_0|c| = b|c|$, e todos

estes valores são inteiros.
Consequentemente:

$$\mathrm{mdc}\,(a|c|, b|c|) = r_n|c| = |c| \cdot \mathrm{mdc}\,(a, b).$$

CQD.

Exercício 36 -

Para a, b, c inteiros não nulos e com a e b relativamente primos, calcule $\mathrm{mdc}\,(ac, bc)$*.*

2.3 Teoremas Básicos da Divisibilidade

Lembrete:
Daqui para a frente, será crucial que o leitor recorde que já "combinamos" que, para tornar mais leve a leitura do texto, e como não teremos nenhum uso para primos negativos, *sempre que nos referirmos a "número primo" estaremos querendo dizer "número primo positivo".*

Teorema 2.51 -

Todo número inteiro $\geqslant 2$ tem, ao menos, um divisor primo.
(Este divisor será o próprio número, caso ele seja primo).

Prova:

Basta provar o caso de $a \geqslant 2$ não primo. Ora, por definição, tal a tem um divisor positivo diferente de 1 e dele mesmo. Seja b_1 o menor dos seus divisores positivos. Afirmamos que b_1 é o primo anunciado. Com efeito, se b_1 não fosse primo, ele teria de ter um divisor não trivial e este último seria um divisor positivo de a menor do que b_1, o qual é o menor dos divisores positivos de a. Absurdo! CQD.

Proposição 2.52 -

Sempre que um número primo não dividir um dado inteiro, ele será relativamente primo com o mesmo.

Prova:

Sendo p primo, os divisores comuns dele, e um outro inteiro a qualquer, têm de estar na lista ± 1 e $\pm p$. Ora, se p não dividir tal a, esta lista se reduz a ± 1. Ou seja, teremos $\operatorname{mdc}(p,a) = 1$.

CQD.

Proposição 2.53 -

Todo par de inteiros não nulos e não *relativamente primos tem obrigatoriamente, ao menos, um divisor comum que é primo.*
Equivalentemente: se dois inteiros não nulos não *forem relativamente primos, então eles são múltiplos de um mesmo número primo.*
Simbolicamente: $mdc(a,b) \neq 1 \Rightarrow \exists\, p$ *primo tal que* $a = mp,\ b = np$, *para adequados* $m, n \in \mathbb{Z}$.

Prova:

Como os dois números dados não são relativamente primos, eles têm, ao menos, um divisor $d \geqslant 2$. Se d for primo o resultado está provado. Se d não for primo, pela Proposição 2.51, ele tem, ao menos, um divisor d' que é primo, e este, obrigatoriamente, tem de dividir cada um dos inteiros dados. CQD.

Para que o leitor possa bem apreciar o significado e valor dos dois teoremas que se seguirão, recomenda-se que recorde os Exercícios 25 e 24.

Teorema 2.54 (Teorema Básico I) -

Todo número inteiro que divide o produto de dois inteiros e que, ademais, é relativamente primo com um deles divide o outro.
Simbolicamente: $[\, c|ab$ *e* $\operatorname{mdc}(a,c) = 1\,] \Rightarrow c|b$.

Prova:

Como $\text{mdc}\,(a, c) = 1$, pelo Teorema 2.47 temos que $1 = ma + nc$, para m e n inteiros. Isso implica que $b = mab + ncb$ e daí, como c divide ab, por hipótese, e como obviamente também divide cb, segue que ele divide a combinação linear $b = mab + ncb$. CQD.

Teorema 2.55 (Teorema Básico II) -

Se um número primo *divide o produto de dois inteiros, então este primo divide, ao menos, um desses dois inteiros.*
Simbolicamente: $[\,p \text{ primo e } p|ab\,] \;\Rightarrow p|a \text{ ou } p|b.$

Exemplo 2.56 -

Como o primo 5 *divide* $120 = 8 \times 15$ *e não divide* 8*, segue que* 5 *tem de ser relativamente primo com* 8 *(pelo Teorema 2.52). Ora, daí, pelo Teorema 2.54, segue que* 5 *tem de dividir* 15*.*

Exercício 37 -

Abstraia e generalize o raciocínio do exemplo anterior para dar uma prova geral do Teorema 2.55.

Exercício 38 -

Generalize o enunciado do Teorema 2.55, de modo a que trate do caso onde um número primo divide um produto de vários fatores. Prove que sua generalização é verdadeira.

> Note que o primeiro teorema não exige que o divisor do produto seja primo, enquanto que o segundo faz esta exigência. Por outro lado, o segundo teorema não exige que o divisor seja relativamente primo com nenhum dos fatores. Por isso, é útil conhecermos os dois teoremas.

Corolário 2.57 -

Todo primo positivo que divide um produto de primos positivos é igual a um deles.

Prova:

Observando que a única maneira de um primo positivo dividir outro primo positivo é os dois serem iguais, o resultado deste corolário é uma imediata aplicação do Exercício 38, o qual é uma imediata aplicação do Teorema 2.55. CQD.

Exercício 39 -

Mostre que o resultado anterior fica falso se não exigirmos que os primos envolvidos sejam positivos.

Corolário 2.58 -

Sendo a um número inteiro, todo primo positivo que divide a^2, também dividirá a.

Prova:

Imediata pelo Teorema 2.55, uma vez que $a^2 = a \cdot a$. CQD.

Exercício 40 -

Mostre que a implicação: "$\forall a, b \in \mathbb{Z} : b|a^2 \Rightarrow b|a$" é falsa.

Exercício 41 -

Prove que todo inteiro, que é relativamente primo com cada fator de um produto de inteiros, tem de ser relativamente primo com esse produto.
DICA: inicie estudando o caso de 15 *versus* $4 \times 7 \times 11 = 308$.

Exercício 42 -

Sendo $\mathrm{mdc}\,(a,b) = 1$, *mostre que* $\mathrm{mdc}\,(a+b, ab) = \mathrm{mdc}\,(a-b, ab) = 1$.
Dica: raciocine por absurdo.

2.4 Teorema Básico da Fatoração

O teorema que estamos por abordar afirma que os números primos funcionam como "tijolos" com os quais podemos construir todo e qualquer número inteiro (exceto 0 e ± 1) fazendo apenas multiplicações. Sua importância é tão grande, que é chamado de Teorema Fundamental da Aritmética:

Teorema 2.59 (Teorema Fundamental da Aritmética) -

Todo número inteiro (exceto 0 e ± 1), ou é primo, ou é $\pm$ o produto de primos (positivos). Ademais, este produto pode ser escrito de uma só maneira, a menos da troca de posição dos fatores.

Em capítulos adiante e em outros livros, o leitor encontrará a fatoração em primos de um inteiro $a \neq 0, \pm 1$ escrita algebricamente, e isso de várias maneiras. Vejamos algumas delas.

- Existem primos $p_1, p_2, p_3, \ldots$, possivelmente repetidos, tais que

$$a = \pm\, p_1 \cdot p_2 \cdot p_3 \cdots .$$

- Existem primos $p_1 \leqslant p_2 \leqslant p_3 \leqslant \cdots \leqslant p_n$ tais que

$$a = \pm\, p_1 \cdot p_2 \cdot p_3 \cdots p_n .$$

- Existem primos distintos $p_1 < p_2 < p_3, \cdots < p_n$, e respectivos inteiros positivos $j_1, j_2, j_3, \cdots, j_n$, tais que:

$$a = \pm\, p_1^{j_1} \cdot p_2^{j_2} \cdot p_3^{j_3} \cdots p_n^{j_n} .$$

Assim, por exemplo,

$$\begin{aligned} -40 &= -2 \times 2 \times 2 \times 5 \\ &= -2^3 \times 5. \\ 63 &= 3 \times 3 \times 7 \\ &= 3^2 \times 7. \end{aligned}$$

Prova:

É óbvio que basta provarmos o resultado nos casos $a \geqslant 2$, o que passamos a fazer.

Existência da fatoração
Seja a um inteiro $\geqslant 2$. Supondo que a não seja primo, ele tem um divisor primo, que indicaremos por p_1 (cf. Teorema 2.51). Temos, então: $a = p_1 \cdot q_1$, para algum inteiro $q_1 \geqslant 2$. Se q_1 for primo, achamos uma fatoração de a.

Se q_1 não for primo, um novo uso do Teorema 2.51 nos dá: $q_1 = p_2 \cdot q_2$, para algum primo p_2 e algum inteiro $q_2 \geqslant 2$, o qual tem de verificar: $2 \leqslant q_2 < q_1$. Se q_2 for primo, achamos uma fatoração, qual seja: $a = p_1 \cdot q_1 = p_1 \cdot p_2 \cdot q_2$.

Se q_2 não for primo, repetimos o raciocínio até chegarmos a uma fatoração de a envolvendo apenas primos, pois as possibilidades de valor para $q_1, q_2, \ldots$ são em número finito, e vão diminuindo.

Unicidade da fatoração
Temos de provar que se um certo inteiro, $\geqslant 2$ e não primo, tiver duas fatorações em primos, elas têm de envolver a mesma quantidade de fatores, e diferir apenas pela ordem com que os fatores são escritos.

Nesse sentido, iniciamos lembrando que a única maneira de um número primo (positivo) dividir outro primo (positivo) é os dois serem iguais. A unicidade é uma consequência deste fato, e do Teorema Básico II (a rigor de sua imediata generalização, feita no Exercício 37). Vejamos.

Seja $p_1p_2 = q_1q_2 \ldots q_n$, com $n \geqslant 2$ e com todos esses fatores primos.
Como p_1 divide p_1p_2, pelo Teorema Básico II, ele tem de dividir um dos q's, digamos, o q_1. Daí, pela nossa observação inicial, $p_1 = q_1$ e, após cancelamento, ficamos com $p_2 = q_2 \ldots q_n$. Isto só é possível se $n = 2$ e $p_2 = q_2$. Assim, nossa fatoração era a mesma, exceto talvez pela ordem: ou $p_1p_2 = p_1p_2$ ou $p_1p_2 = p_2p_1$.

Seja $p_1p_2p_3 = q_1q_2q_3 \ldots q_n$, com $n \geqslant 3$ e com todos esses fatores primos.
O mesmo argumento nos dá, talvez após reordenarmos os q's, que $p_1 = q_1$. Cancelando, caímos no caso anterior: $p_2p_3 = q_2q_3 \ldots q_n$. Assim, nossa fatoração era a mesma, exceto talvez pela ordem: ou $p_1p_2p_3 = p_1p_2p_3$, ou $p_1p_2p_3 = p_2p_1p_3$, ou $p_1p_2p_3 = p_1p_3p_2$, ou $p_1p_2p_3 = p_2p_3p_1$, ou $p_1p_2p_3 = p_3p_1p_2$, ou $p_1p_2p_3 = p_3p_2p_1$.

Fica agora fácil o leitor ver que o caso $p_1p_2p_3p_4 = q_1q_2q_3q_4 \ldots q_n$, com $n \geqslant 4$ e com todos esses fatores primos, se reduz ao caso anterior e que, em geral, a unicidade do caso $p_1p_2 \ldots p_m = q_1q_2 \ldots q_n$, com $n \geqslant m \geqslant 2$ (e com todos esses fatores primos) implica a do caso seguinte: $p_1p_2 \ldots p_mp_{m+1} = q_1q_2 \ldots q_n$, com $n \geqslant m \geqslant 2$. Ou seja, por indução matemática (sobre m), está provada a unicidade.

CQD.

Observação 2.60 -

Alguns autores, e principalmente os antigos, incluem o número um entre os primos. Isto faz com que tenham de falar em "fatoração em primos $\geqslant 2$", para garantir a unicidade da fatoração. A prática moderna de excluir o número um entre os primos evita termos de acrescentar o "$\geqslant 2$".

Exercício 43 -

Aplique o raciocínio da prova do Teorema Fundamental da Aritmética para achar uma fatoração em primos positivos de 63*.*

Exercício 44 -

Aplique o raciocínio usado na prova da unicidade no Teorema Fundamental da Aritmética para provar diretamente que se for afirmado que $130 = 2 \times 5 \times 13$ *tem uma fatoração em primos positivos da forma* $130 = q_1 q_2 q_3$ *. Então temos de ter, ou* $q_1 q_2 q_3 = 2 \times 5 \times 13$*, ou* $= 2 \times 13 \times 5$*, ou* $= 5 \times 2 \times 13$*, ou* $= 2 \times 13 \times 2$*, ou* $= 13 \times 2 \times 5$*, ou* $= 13 \times 5 \times 2$*.*

Exercício 45 -

Mostre que a menor potência de 60*, que é divisível por* 36^4 *, é* 8*.*

Exercício 46 -

Escreva os elementos de um conjunto

i). de inteiros positivos que não têm fatores positivos menores;

ii). de inteiros positivos que não têm fatores positivos não unitários menores.

Exercício 47 -

Sejam dados dois inteiros $(a, b \geqslant 2)$*. Pede-se mostrar que*

(uma fatoração em primos positivos de ab*)* $=$
(uma fatoração em primos positivos de a*)* $\times$ *(uma fatoração em primos positivos de* b*).*

Em linguagem abreviada, escreveremos isso como:

$$\boxed{\text{fat}\,(ab) = \text{fat}\,(a) \cdot \text{fat}\,(b).}$$

Para entender a idéia envolvida neste exercício, observe que

$$200 = 2^3 \times 5^2$$
$$126 = 2 \times 3^2 \times 7.$$

Daí tem-se

$$25\,200 = 200 \times 126 = (2^3 \times 5^2) \times (2 \times 3^2 \times 7) = 2^4 \times 3^2 \times 5^2 \times 7.$$

Exercício 48 -

Um aluno do Ensino Fundamental apresentou a seguinte resolução para o problema "determine uma fatoração em números primos para 78".

$$\begin{array}{r|l} 78 & 3 \\ 26 & 2 \\ 13 & 13 \\ 1 & \end{array} \qquad \Rightarrow \qquad 78 = 3 \times 2 \times 13.$$

Discuta tanto a correção do raciocínio como a da resposta.

Do Exercício 47 tiramos como consequências:

Corolário 2.61 -

Sejam a e p inteiros positivos, com p primo. Temos que:

- *se p divide a, então p aparece em toda fatoração em primos de a;*
- *se p aparece numa fatoração em primos de a, então p divide a.*

Equivalentemente:
p primo é divisor de um inteiro a quando, e somente quando, p aparece na fatoração em primos de a.

Prova:

Deixemos de lado, pois que é trivial, o caso em que $p = a$.
• Suponhamos que p divida a. Temos que $a = p \cdot b$, para algum inteiro $\geqslant 2$ (lembre que, agora, $p \neq a$). Como p dividir a implica $a \geqslant 2$, podemos, então, escrever:

$$\text{fat}\,(a) = \text{fat}\,(pb) = \text{fat}\,(p) \cdot \text{fat}\,(b) = p\,\text{fat}\,(b)\,,$$

e o resultado segue pela unicidade, a menos de ordem, da fatoração em primos de a. Ou seja, p está em toda fatoração em primos de a.

• Suponhamos que p apareça numa fatoração em primos de a. Ora, reescrevendo essa fatoração de modo que p apareça como primeiro fator, teremos algo do tipo: $a = p \cdot p_1 p_2 \cdots p_n$ e, assim, percebemos que p tem de ser divisor de a. CQD.

Exercício 49 -

A partir da fatoração em primos de 210, *escreva todos os seus divisores.*

Exercício 50 -

A partir da fatoração em primos de 54 *e* 72, *mostre que* $\operatorname{mdc}(54, 72) = 18$.

Exercício 51 -

Usando fatoração em primos, dê condição suficiente para que um inteiro seja múltiplo de dois outros inteiros. Justifique.

Exercício 52 -

Generalize o resultado do Corolário 2.57, provando que todo primo que divide uma potência positiva de um inteiro, também divide este inteiro.

Exercício 53 -

O mais famoso teorema de Euclides afirma que existem infinitos números primos. Mostre que ele é uma consequência do Teorema Fundamental da Aritmética. Para isto, raciocine por absurdo: supondo que a lista dos primos seja finita, $p_1, p_2, \dots, p_n$, *considere o inteiro* $1 + p_1 p_2 \cdots p_n$ *e estude sua fatorabilidade em primos.*

Exercício 54 -

Este exercício é uma elaboração do Exemplo 1.27.

i). Prove que "se a Conjectura de Goldbach for verdadeira, então todo múltiplo de 4 *pode ser escrito como a soma de dois pares, não ambos múltiplos de* 4*".*

ii). Prove a veracidade da tese de (i).

iii). A partir de (i) e (ii), poderíamos concluir algo sobre a veracidade da Conjectura de Goldbach? Justifique-se.

CAPÍTULO 3

NÚMEROS RACIONAIS

Partimos da suposição de que o leitor traga do Ensino Fundamental a ideia de fração. Isto não é pouca coisa. Segundo o matemático Hassler Whitney, do Institute for Advanced Study (Princeton, USA): "*A primeira crise na matemática ensinada na escola ocorre com o estudo das frações. O stress é causado particularmente pela tremenda confusão das ideias associadas.*"[1]

O capítulo inicia recordando brevemente os significados intuitivos de fração e de número racional, bem como sua relação. A seguir, formalizaremos matematicamente[2] a ideia de número racional e passamos a recordar brevemente as propriedades básicas

[1] In Proceedings of the Second International Congress on Mathematical Education. Cambridge Univ. Press, 1973.

[2] Usa-se esta expressão para dizer que iremos dar uma definição ou caracterização estritamente

das operações aritméticas e da relação de ordem entre números racionais. Tudo isso sob um ponto de vista mais teórico do que o da abordagem do Ensino Fundamental, pois queremos aqui enfatizar as caracteristicas estruturais deste campo, e não os procedimentos de cálculo com frações.

3.1 Conceito de fração e número racional

– a ideia de fração

Como já foi dito, supomos que o leitor traga do Ensino Fundamental o conceito de fração. Em particular, que tenha perfeitamente clara a distinção entre, por exemplo, a fração $2/3$ e a $4/6$. Esta diferença costuma ser ilustrada com o tradicional bolo, com o qual se vê que pegar dois pedaços de um bolo que foi dividido em três partes iguais não é o mesmo que pegar quatro pedaços do mesmo bolo que foi dividido em seis partes iguais.

– a ideia de frações equivalentes

Retomemos o nosso "amigo" bolo. Usamos a ideia de fração para explicitar a *maneira* como foi feito um particionamento do bolo, enquanto que usa-se a ideia de número racional para expressar a *quantidade* de bolo separada.

Assim, embora servir dois pedaços de um bolo que foi dividido em três partes iguais não seja o mesmo que servir quatro pedaços do mesmo bolo que foi dividido em seis partes iguais, a *quantidade* de bolo servida é a mesma. Essas duas frações são ditas equivalentes, na medida que expressam uma mesma quantidade:

$$\text{quant}\,(\frac{2}{3}) = \text{quant}\,(\frac{4}{6}).$$

> *Em geral, como podemos decidir, a partir dos valores de a, b, A e B, se as quantidades representadas por a/b e A/B são as mesmas?*

Para decidir, levaremos em conta dois fatos:

- ninguém tem dúvidas quanto a comparar duas frações de mesmo denominador;
- ao tomarmos a pedaços de um bolo, que foi dividido em b partes, a quantidade separada é igual a que obteremos quando tomamos na partes do bolo se ele

matemática de uma ideia ou objeto, a/o qual pode então ser estudado em termos estritamente lógicos, independentemente da intuição.

for dividido em nb partes (n aqui é um número natural não-nulo), ou seja:

$$\text{quant}\,(\frac{a}{b}) = \text{quant}\,(\frac{na}{nb})\,.$$

Com efeito, esses dois fatos nos permitem escrever:

$$\text{quant}\,(\frac{a}{b}) = \text{quant}\,(\frac{aB}{bB}) \quad \text{e} \quad \text{quant}\,(\frac{A}{B}) = \text{quant}\,(\frac{Ab}{Bb}),$$

e concluir que:

$$\text{quant}\,(\frac{a}{b}) = \text{quant}\,(\frac{A}{B}) \Longleftrightarrow \text{quant}\,(\frac{aB}{bB}) = \text{quant}\,(\frac{Ab}{bB}) \Longleftrightarrow aB = Ab.$$

Embora o raciocínio acima tenha uma base intuitiva, o que é até bom, prosseguiremos de um modo plenamente rigoroso, por meio da seguinte definição formal:

Definição 3.1 -

Sendo $a, b \neq 0, A, B \neq 0$ números inteiros (possivelmente negativos), dizemos que as frações a/b e A/B são frações equivalentes, *o que denotaremos por*

$$\text{quant}\,(\frac{a}{b}) = \text{quant}\,(\frac{A}{B})\,,$$

quando, e só quando, tivermos $aB = Ab$. Ou seja:

$$\text{quant}\,(\frac{a}{b}) = \text{quant}\,(\frac{A}{B}) \Longleftrightarrow aB = Ab\,.$$

Por razões que já justificaremos, costuma-se abreviar a notação acima, denotando-se que "as frações a/b e A/B são equivalentes" por:

$$\frac{a}{b} = \frac{A}{B}\,.$$

Resumindo:

$$\boxed{\text{quant}\,(\frac{a}{b}) = \text{quant}\,(\frac{A}{B}) \Longleftrightarrow \frac{a}{b} = \frac{A}{B} \Longleftrightarrow aB = Ab\,.}$$

Exemplo 3.2 -

Temos a seguinte equivalência de frações:

$$\text{quant}\,(\frac{2}{3}) = \text{quant}\,(\frac{4}{6}) = \text{quant}\,(\frac{8}{12}) = \text{quant}\,(\frac{16}{24}) = \cdots\,,$$

a qual é tradicionalmente escrita de modo abreviado como:

$$\frac{2}{3} = \frac{4}{6} = \frac{8}{12} = \frac{16}{24} = \cdots\,,$$

Observação 3.3 (*importante*) -

A Definição 3.1 foi formulada a partir de observações gerais sobre frações do tradicional bolo, bem como a partir da observação de que a relação $aB = Ab$ tem sentido mesmo que um ou mais dos fatores envolvidos sejam inteiros negativos, ou nulos.

Por isso, essa definição implica estarmos considerando como fração objetos como $5/3$, ou seja: frações cujo numerador é maior do que o denominador. Bem mais do que isso, a tal definição também está considerando frações cujo numerador e/ou denominador tenha sinal negativo, como $(-3)/5$, $3/(-5)$ e $(-3)/(-5)$, bem como frações cujo numerador seja nulo.

Em vez de procurarmos dar um significado – por exemplo, em termos do tradicional bolo – para frações como $5/3$, $0/3$, $(-3)/5$ etc., vamos observar que a generalização envolvida na Definição 3.1 deve ser vista como uma conveniência justificada pelo cálculo, conforme ficará gradativamente claro. Trata-se de um passo que precisa ser dado para que consigamos formalizar a ideia de número racional.

Em verdade, o que estamos fazendo é algo comum em Matemática. Normalmente, as formalizações matemáticas nascem de algo concreto, mas se preocupam mais com as relações lógicas envolvidas do que com a possibilidade de uma interpretação concreta para todas as possibilidades contempladas nas mesmas. Isto é um ponto de vista básico da matemática contemporânea - o qual o leitor encontrará outras vezes, aqui neste livro e em muitos outros assuntos matemáticos que estudar -.

Exemplo 3.4 -

$$\frac{-2}{3} = \frac{-4}{6} = \frac{-6}{9} = \cdots = \frac{2}{-3} = \frac{4}{-6} = \cdots$$

$$\frac{3}{5} = \frac{6}{10} = \frac{9}{15} = \cdots = \frac{-3}{-5} = \frac{-6}{-10} = \cdots$$

$$\frac{0}{1} = \frac{0}{2} = \frac{0}{3} = \cdots = \frac{0}{-1} = \frac{0}{-2} = \cdots .$$

Observação 3.5 -

Voltemos à questão notacional. Como já dissemos, em vez de se usar a notação $\text{quant}\,(a/b) = \text{quant}\,(c/d)$, *preferimos* $a/b = c/d$. *Isto se faz não apenas por razões de simplicidade, mas também pelo fato que a equivalência de frações é uma* relação de equivalência, *conforme atestam as propriedades i), ii) e iii) da proposição seguinte.*

Em Matemática, sempre que tivermos uma relação com tais propriedades, podemos usá-la como se fosse uma igualdade; por isso costuma-se usar o símbolo $=$, *ou parecido, para denotá-la. A seguir, teremos muitas oportunidades de exemplificar este ponto de vista.*

Proposição 3.6 -

A equivalência de frações é uma relação de equivalência, pois tem as seguintes propriedades:

i). reflexiva: $\text{quant}\,(a/b) = \text{quant}\,(a/b)$;

ii). simétrica: $\text{quant}\,(a/b) = \text{quant}\,(c/d) \;\Rightarrow\; \text{quant}\,(c/d) = \text{quant}\,(a/b)$;

iii). transitiva: $\text{quant}\,(a/b) = \text{quant}\,(c/d),\; \text{quant}\,(c/d) = \text{quant}\,(e/f) \;\Rightarrow$ $\text{quant}\,(a/b) = \text{quant}\,(e/f)$.

Ou seja, usando a notação $=$:

i). reflexiva: $a/b = a/b$;

ii). simétrica: $a/b = c/d \;\Rightarrow\; c/d = a/b$;

iii). transitiva: $a/b = c/d,\; c/d = e/f \;\Rightarrow\; a/b = e/f$.

Prova:

Como as propriedades reflexiva e simétrica são óbvias, concentremo-nos na transitiva. Ora, de $a/b = c/d$ tiramos $ad = bc$, e de $c/d = e/f$ sai $cf = de$. Multiplicando a primeira igualdade de inteiros por f, obtemos: $adf = bcf$. Multiplicando a segunda por b, ficamos com $bcf = bde$. Daí, temos: $adf = bcf = bde$. Mas, como $d \neq 0$, a igualdade $adf = bde$ dá $af = be$, ou seja, $a/b = e/f$. CQD.

– definição formal de número racional

Um número racional será um novo tipo de objeto matemático que introduziremos para formalizar matematicamente a ideia intuitiva de quantidade associada a frações que apresentamos acima. Cada número racional será visto como uma classe[3] de frações equivalentes. Mais precisamente:

Definição 3.7 -

*Chamamos de **número racional** a classe de todas as frações equivalentes a uma dada fração. Dois números racionais serão ditos iguais se, e só se, suas classes são iguais como conjuntos.*
O conjunto de todos os números racionais é simbolizado por $\mathbb{Q}$.

Na prática:

- determinamos um número racional r explicitando uma fração a/b que é tal que r é a classe de todas as frações equivalentes a a/b;
- reciprocamente, dada uma fração a/b, a mesma determina exatamente um número racional, o qual é o conjunto (classe) de todas as frações equivalentes a a/b.

Definição 3.8 -

*Toda fração da classe de frações que consiste em um dado número racional é dita ser uma **representação fracionária** deste número.*
Usaremos a notacão $r = a/b$ para indicar que a fração a/b é uma representação do número racional r.

[3] A palavra *classe* significa o mesmo que conjunto, e é usada quando trabalhamos com um conjunto de objetos matemáticos que, de alguma maneira, são todos equivalentes entre sí.

Exemplo 3.9 -

A fração $2/3$ *determina o número racional* $\{2/3, 4/6, 8/12, \ldots\}$*, sendo que* $2/3$ *e* $4/6$ *são duas das infinitas representações fracionárias do mesmo. Denotando este número racional por* r*, podemos escrever* $r = 2/3$ *e* $r = 4/6$*.*

O número zero racional consiste na classe $\{0/1, 0/2, 0/3, \ldots, 0/-1, 0/-2, \ldots\}$*. Ele é o único número racional que tem representações fracionárias, tanto com numerador e denominador de sinais iguais, como de sinais opostos.*

Teorema 3.10 -

Um número racional r *, dado por uma fração* a/b *, é igual a um racional* s *dado por uma fração* c/d *se, e só se, tivermos que essas duas frações são equivalentes:*

$$r = s \Longleftrightarrow \frac{a}{b} = \frac{c}{d}.$$

Prova:

A condição é necessária:
sendo $r = a/b$ e $s = c/d$, como $r = s$, segue que $r = c/d$ e, então, que $a/b = c/d$, ou seja, a/b é equivalente a c/d.

A condição é suficiente:
temos de provar que se $r = a/b$, $s = c/d$ e a/b é equivalente a c/d, então $r = s$; ou seja, toda fração e/f de r está em s, e vice-versa; ou ainda, toda fração e/f representando r também representa s, e vice-versa. Vejamos.
Se $r = e/f$, temos $e/f = a/b$, e como $a/b = c/d$, segue pela transitividade da relação de equivalência que $e/f = c/d$. Ou seja, $s = e/f$.
Reciprocamente, se $s = e/f$, temos $e/f = c/d$, e como $a/b = c/d$, novamente a propriedade da associatividade nos dá $e/f = a/b$. Ou seja, $r = e/f$.

CQD.

Os resultados que estudaremos a seguir ficarão mais fáceis e mais úteis se considerarmos representações fracionárias de tipo especial. Vejamos dois deles.

Proposição 3.11 -

Todo número racional pode ser representado por uma fração de denominador positivo.

Prova:

Dado um número racional, seja a/b uma fração que o representa. Então, se $b > 0$ não precisamos fazer nada; se $b < 0$, como vale $a \cdot (-b) = (-a) \cdot b$, temos:

$$r = \frac{a}{b} = \frac{-a}{-b}.$$

e assim vemos que $-a/-b$ tem denominador positivo e representa r.

CQD.

Definição 3.12 -

Uma fração a/b é dita ser irredutível *quando a e b forem relativamente primos.*

Lema 3.13 -

A única maneira de duas frações irredutíveis e de denominador positivo serem equivalentes é serem idênticas: elas têm de ter o mesmo numerador e o mesmo denominador.

Prova:

Sendo $c/d = c'/d'$, com ambas irredutíveis e de denominador positivo, a equivalência nos dá $cd' = c'd$, e como c é relativamente primo com d, o Teorema Básico I da divisibilidade nos dá que c divide c'. Analogamente, como c' é relativamente primo com d', o mesmo teorema nos dá que c' divide c. Como ambos d e d' são positivos, segue então que $c = c'$, e isso implica que $d = d'$.

CQD.

Teorema 3.14 -

Todo número racional é representado por uma, e só uma, fração irredutível de denominador positivo.

Prova:

Seja a/b uma fração representando o racional dado. Já sabemos que podemos supor que $b > 0$. O teorema ficará demonstrado se provarmos que existe exatamente uma fração irredutível e de denominador positivo que seja equivalente a a/b.

Existe uma
Seja a/b com $b > 0$. Se tivermos $b = 1$, a fração dada já é irredutível. Resta examinarmos os casos $b \geqslant 2$. Os subcasos triviais $a = 0$, e $a = \pm 1$, são imediatos ($0/b = 0/1$ e $\pm 1/b$ já é irredutível). Tratemos dos subcasos $a \neq 0, \pm 1$.

Pelo Teorema Fundamental da Aritmética, podemos escrever $a = \pm mc' = mc$ e $b = md$, onde m é o produto de todos os divisores primos comuns a a e b, e c' e d é o que resta das respectivas fatorações. Ora, é imediato que $a/b = c/d$ (pois, como $m \neq 0$, provar $ad = bc$ é o mesmo que provar $mad = mbc$; ou seja $amd = bmc$, ou ainda, $ab = ba$), e c/d é facilmente visto ser irredutível e de denominador positivo.

Existe somente uma
se tivermos $a/b = c/d$ e $a/b = c'/d'$, com ambas c/d e c'/d' irredutíveis, e de denominador positivo, pela transitividade da relação de equivalência entre frações, tiramos que $c/d = c'/d'$. Mas pela irredutibilidade dessas duas frações, o lema anterior dá $c = c'$ e $d = d'$.

CQD.

Exercício 55 -

Encontrar uma representação em fração irredutível para cada um dos racionais dados pelas seguintes frações:

$$\frac{177}{18}, \quad \frac{25}{120}, \quad \frac{-12}{13}.$$

Exercício 56 -

Seja r um número racional representado pela fração $13/24$. Pergunta-se:

i). Podemos representar r por fração da forma $a/560$? Explique.

ii). E por fração da forma $a/168$? Explique.

Exercício 57 -

Seja r um número racional dado por $15/35$. Pede-se mostrar que ele também tem uma representação da forma a/b, onde $\mathrm{mdc}(a, b) = 18$.

Exercício 58 -

i). Encontre infinitas representações para o número racional r, se $r = 2/3$.

ii). Idem, para o número racional $14/49$.

iii). Encontre infinitas representações fracionárias para um racional qualquer a/b.

iv). A lista que você obteve em (ii) inclui todas as possíveis representações para o caso de $r = 14/49$ *? E na lista que você obteve em (i), para* $r = 2/3$ *?*

v). Tente intuir e demonstrar sua conjectura: em que casos as representações indicadas em (iii) constituem todas as representações possíveis para o racional dado?

Cuidados

• O conjunto $\mathbb{Q}$ dos números racionais *não* é o conjunto das frações de números inteiros, mas sim o conjunto das *quantidades numéricas* que elas representam. Mais precisamente: um número racional não é uma fração, mas sim um conjunto de frações equivalentes. Este "equivalentes" traduz rigorosamente o fato intuitivo de que a cada uma dessas frações está associada uma mesma quantidade.

• Usamos, e usaremos, alguns abusos de notação que são tradicionais e que exploram o fato de estarmos trabalhando com relações de equivalência. Assim, quando escrevermos

$$r = \frac{2}{3} = \frac{4}{6},$$

é importante que o leitor esteja bem consciente de que os iguais utilizados têm um significado diferente. Com efeito, o primeiro está indicando que a fração $2/3$ representa o número racional r, enquanto que o segundo igual está dizendo que as frações $2/3$ e $4/6$ são equivalentes.

• Outras convenções

Quando escrevermos: "seja um número racional r dado por $r = a/b$", ou mesmo "seja o número racional $r = a/b$", com a e $b \neq 0$ inteiros, estaremos dizendo abreviadamente que "r é um número racional que é representado pela fração a/b".

O desejo de abreviarmos também nos leva ao abuso de dizer "seja o número racional a/b", quando deveríamos dizer "seja o número racional representado pela fração a/b".

– Os números racionais realmente são números ?

É da tradição matemática considerar como números objetos matemáticos que, de algum modo, expressem quantidade (já vimos que os números racionais fazem isso) e para os quais seja possível definir operações aritméticas que têm propriedades, no mínimo, semelhantes às das operações aritméticas entre os números inteiros (isso passaremos a examinar na próxima seção.)

Convenção:

a partir deste ponto, tendo em vista a Proposição 3.11, ao escrevermos um racional por meio de uma fração a/b, estaremos subentendendo que tenhamos tomado $b > 0$.

3.2 O corpo dos números racionais

São dois os principais objetivos desta seção:

- dar um carácter plenamente numérico aos racionais, definindo as correspondentes operações aritméticas e mostrando que as mesmas têm propriedades bastante próximas dos números inteiros; isso será feito chamando a atenção para alguns aspectos matemáticos da teoria que não são discutidos, ou mesmo mencionados, no Ensino Fundamental e no Ensino Médio;
- mostrar que os números inteiros podem ser "imersos" de um modo bastante natural no campo dos números racionais, o que nos permitirá interpretar os números racionais como quocientes de inteiros.

Além disso, esta seção também servirá de base para, uma vez introduzido o conceito de número real (vide Capítulo 7), estendermos as operações aritméticas dos racionais aos números reais.

– operação adição em $\mathbb{Q}$

Para conceituarmos a adição de números racionais, retomemos nosso "amigo" bolo. A soma da quantidade de bolo (número racional) representada pela fração $1/5$ com a quantidade representada por $3/5$, certamente é a quantidade de bolo (número racional) representada pela fração $4/5$. De um modo abreviado, escrevemos isso com:

$$\frac{1}{5} + \frac{3}{5} = \frac{4}{5}\,.$$

É imediato generalizarmos para a soma dos racionais r e s, os quais são representados por frações de mesmo denominador. Por exemplo, sendo $r = a/b$ e $s = c/b$, temos:

$$r + s = \frac{a}{b} + \frac{c}{b} = \frac{a+c}{b}\,.$$

Para tratar da soma de números racionais representados por frações de denominador distinto, é só procurarmos representações equivalentes de mesmo denominador. Iniciemos com um exemplo numérico, no caso de $r = 2/3$ e $s = 1/5$:

$$r = \frac{2}{3} = \frac{10}{15}, \quad s = \frac{1}{5} = \frac{3}{15} \Rightarrow r + s = \frac{10}{15} + \frac{3}{10} = \frac{13}{15}.$$

No caso geral, sendo $r = a/b$ e $s = c/d$, teremos:

$$r = \frac{a}{b} = \frac{ad}{bd}, \quad s = \frac{c}{d} = \frac{bc}{bd} \quad \Rightarrow r + s = \frac{ad+bc}{bd}\,.$$

Resumamos esses significados intuitivos por meio de uma definição formal:

Definição 3.15 -

A adição das frações *a/b e c/d produz um resultado chamado* soma*, o qual é a fração denotada e definida por:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}\,.$$

A adição dos racionais *r e s, dados por $r = a/b$ e $s = c/d$, produz um resultado chamado* soma*, a qual é o número racional denotado por $r + s$ e representado pela soma das frações a/b e c/d. Ou seja:*

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}\,. \tag{3.1}$$

Observação 3.16 -

Pela definição,

$$\frac{2}{10} + \frac{9}{5} = \frac{10}{50} + \frac{90}{50} = \frac{100}{50}\,.$$

Por outro lado, podemos modificar ligeiramente o raciocínio intuitivo acima e escrever, apelando para o mínimo múltiplo comum dos denominadores:

$$\frac{2}{10} + \frac{9}{5} = \frac{2}{10} + \frac{18}{10} = \frac{20}{10}\,.$$

No caso, as duas frações soma, $100/50$ e $20/10$, são equivalentes; ou seja, definem um mesmo número racional.

Isso nos leva à seguinte questão crucial: a soma de dois números racionais fixos pode variar com as frações usadas para efetuar a soma?

Proposição 3.17 -

A adição de números racionais está bem definida, ou seja, o valor da soma independe das frações escolhidas para representar os racionais dados.
Mais precisamente: sendo a/b e A/B representações fracionárias de um número racional r, e c/d e C/D representações de um outro racional s, então as frações

$$\frac{ad+bc}{bd} \quad e \quad \frac{AD+BC}{BD}$$

representam um mesmo número racional. Simbolicamente:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=r+s=\frac{AD+BC}{BD}=\frac{A}{B}+\frac{C}{D}\,. \tag{3.2}$$

Prova:

Temos que mostrar que as frações $(ad+bc)/(bd)$ e $(AD+BC)/(BD)$ são equivalentes, o que é o mesmo que provar que $(ad+bc)(BD)=(AD+BC)(bd)$. Ora, pela equivalência das representações fracionárias dadas para r e s, temos que $aB=Ab$ e $cD=Cd$, e daí:

$$(ad+bc)(BD)=aBdD+bBcD=AbdD+bBCd=(AD+BC)(bd).$$

CQD.

Exercício 59 -

Para o problema "calcule a soma $\frac{9}{5}+\frac{7}{20}$", um aluno do Ensino Fundamental apresentou a seguinte resolução:

$$\frac{9}{5}+\frac{7}{20}=\frac{180+35}{100}=\frac{215}{100}\overset{\div 5}{=}\frac{43}{20}\,.$$

Pede-se uma resolução mais rápida.

Exercício 60 -

Sendo a/b uma fração irredutível com $a \neq 0$, prove que a soma $1/a+1/b$ também é uma fração irredutível.

Exercício 61 -

Sendo a/b uma fração irredutível, com $a \neq 0$, prove que a soma $a/b + b/a$ também é uma fração irredutível.

Exercício 62 -

Mostre que se a soma de duas frações irredutíveis é uma fração tipo $a/1$ (com a inteiro), então essas duas frações têm o mesmo denominador.

Exercício 63 -

A fração, que é preciso adicionar a uma fração irredutível para resultar um como soma, também é irredutível. Demonstre.

– operação multiplicação em $\mathbb{Q}$

Novamente, para conceituarmos multiplicação de números racionais, retomaremos nosso "amigo" bolo. Suponhamos que nos seja dada uma quantidade (número racional) de bolo, que corresponde a $1/5$ do mesmo. É claro que $2 \cdot 1/5$ e $2/5$ representam uma mesma quantidade de bolo, equivalente a dois pedaços de $1/5$ dele. Em geral:

$$n \cdot \frac{c}{d} = \frac{nc}{d}\,, \quad \text{onde, aqui e no que segue, } n = \text{ inteiro } \geqslant 1\,.$$

Como $1/5$ de bolo equivale a $2/10$ de bolo, pegar a metade de um pedaço de $1/5$ de bolo equivale a pegar a metade de um pedaço de $2/10$ de bolo; ou seja: pegar $1/10$ de bolo. É natural escrevermos isso como:

$$\frac{1}{2} \cdot \frac{1}{5} = \frac{1}{2} \cdot \frac{2}{10} = \frac{1}{10}\,.$$

Semelhantemente, pegar a terça parte daquele pedaço de $1/5$ equivale a escrever:

$$\frac{1}{3} \cdot \frac{1}{5} = \frac{1}{3} \cdot \frac{3}{15} = \frac{1}{15}\,.$$

Em geral:

$$\frac{1}{n} \cdot \frac{c}{d} = \frac{1}{n} \cdot \frac{nc}{nd} = \frac{c}{nd}\,.$$

Em termos ainda mais gerais: como interpretar tomar $2/3$ de $5/7$ do bolo? Já sabemos que tomar 2 vezes um pedaço de $5/7$ do bolo equivale a tomar:

$$2 \cdot \frac{5}{7} = \frac{2 \cdot 5}{7} = \frac{10}{7}\,,$$

o que consiste em tomar 3 vezes mais do que os 2/3 que precisamos tomar; logo, tomar 2/3 de 5/7 equivale a tomar 1/3 de 10/7, ou seja, 10/21. Resumimos isso, escrevendo:

$$\frac{2}{3}\cdot\frac{5}{7}=\frac{1}{3}\cdot\left(2\cdot\frac{5}{7}\right)=\frac{1}{3}\cdot\frac{2\cdot 5}{7}=\frac{2\cdot 5}{3\cdot 7}\,.$$

Generalizando:

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{1}{b}\cdot\left(a\cdot\frac{c}{d}\right)=\frac{1}{b}\cdot\frac{a\cdot c}{d}=\frac{a\cdot c}{b\cdot d}\,.$$

Resumamos esses significados intuitivos por meio de uma definição formal e geral:

Definição 3.18 -

A multiplicação das frações a/b e c/d produz um resultado chamado produto, o qual é a fração denotada e definida por:

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

A multiplicação dos racionais r e s, dados por $r=a/b$ e $s=c/d$, produz um resultado chamado produto, o qual é o número racional denotado por $r\cdot s$ e representado pelo produto das frações a/b e c/d. Ou seja:

$$r\cdot s=\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}. \tag{3.3}$$

Proposição 3.19 -

A multiplicação de números racionais está bem definida, ou seja, o valor do produto independe das frações escolhidas para representar os racionais dados.
Mais precisamente: sendo a/b e A/B representações fracionárias de um número racional r, e sendo c/d e C/D representações de um outro racional s, então as frações

$$\frac{ac}{bd} \quad e \quad \frac{AC}{BD}$$

representam um mesmo número racional. Simbolicamente:

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=r\cdot s=\frac{AC}{BD}=\frac{A}{B}\cdot\frac{C}{D}. \tag{3.4}$$

Prova: Temos que mostrar que as frações $(ac)/(bd)$ e $(AC)/(BD)$ são equivalentes, o que é o mesmo que provar que $ad\cdot BD=AC\cdot bd$. Ora, pela equivalência das representações fracionárias dadas para r e s, temos que $aB=Ab$ e $cD=Cd$, e daí:

$$ac\cdot BD=aBcD=AbCd=AC\cdot bd\,.$$

CQD.

Exercício 64 -

Demonstrar que o produto de duas frações irredutíveis também é irredutível, desde que o numerador de cada uma delas seja relativamente primo com o denominador da outra.

Exercício 65 -

Usando o Teorema Fundamental da Aritmética, caracterize os casos em que o produto das frações a/b e c/d é da forma $n/1$. Justifique.

– operação subtração em $\mathbb{Q}$

No campo dos números inteiros, temos que $10-2=8$, pois que $2+8=10$, e temos que $3-10=-7$, pois que $10+(-7)=10-7=3$. Estendendo esta ideia para as frações e racionais, deveremos escrever

$$\frac{a}{b}-\frac{c}{d}=\frac{\alpha}{\beta} \quad \text{quando} \quad \frac{c}{d}+\frac{\alpha}{\beta}=\frac{a}{b}.$$

Afirmamos que isso é possível sempre, desde que tomemos

$$\frac{\alpha}{\beta}=\frac{ad-bc}{bd}.$$

Com efeito:

$$\frac{c}{d}+\frac{ad-bc}{bd}=\frac{bc+ad-bc}{bd}=\frac{ad}{bd}=\frac{a}{b}.$$

Coloquemos tudo isso numa definição formal:

Definição 3.20 -

A subtração das frações *a/b e c/d produz um resultado chamado* diferença, *o qual é a fração denotada e definida por:*

$$\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}.$$

A subtração dos racionais *r e s, dados por $r=a/b$ e $s=c/d$, produz um resultado chamado* diferença, *a qual é o número racional denotado por $r-s$ e representado pela diferença das frações a/b e c/d. Ou seja:*

$$r-s=\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}. \tag{3.5}$$

Proposição 3.21 -

A subtração dos números racionais r e s está bem definida, no sentido de que o valor da diferença $r - s$ independe das frações escolhidas para representar os racionais dados e, ademais, realmente $s + (r - s) = r$.

Prova:

Sendo a/b e A/B representações fracionárias do número racional r, e c/d e C/D representações do racional s, então temos de mostrar a equivalência das frações

$$\frac{ad - bc}{bd} \text{ e } \frac{AD - BC}{BD}$$

o que é o mesmo que provar que $(ad + bc)(BD) = (AD + BC)(bd)$. Ora, pela equivalência das representações fracionárias dadas para r e s, temos que $aB = Ab$ e $cD = Cd$, e daí:

$$(ad - bc)(BD) = aBdD - bBcD = AbdD - bBCd = (AD - BC)(bd).$$

Resta observar que a validade de $s + (r - s) = r$ é imediata das considerações preliminares que fizemos.

CQD.

Observação 3.22 -

No contexto dos números inteiros, temos que $bc + b(-c) = b\big(c + (-c)\big) = b \cdot 0 = 0$, o que mostra que $b(-c) = -bc$. Este resultado e mais a definição de soma e de diferença de frações nos permitem afirmar que:

$$\frac{a}{b} + \frac{-c}{d} \overset{(\text{def.}+)}{=} \frac{ad + b(-c)}{bd} = \frac{ad - bc}{bd} \overset{(\text{def.}-)}{=} \frac{a}{b} - \frac{c}{d};$$

em particular: $c/d + (-c)/d = 0$. Por isso, convenciona-se escrever:

$$\boxed{-\frac{c}{d} = \frac{-c}{d} = \frac{c}{-d}.}$$

Exercício 66 -

Sendo a/b uma fração irredutível, com $a \neq 0$ e $b \neq 0$, mostre que $1/a - 1/b$ também é irredutível.

Exercício 67 -

Sendo a/b e c/d irredutíveis, com b e d relativamente primos, então $a/b + c/d$ e $a/b - c/d$ são ambas irredutíveis. Falso ou verdadeiro? Justifique.

– operação divisão em $\mathbb{Q}$

No campo dos números inteiros, temos que $20 \div 5 = 4$, pois $5 \cdot 4 = 20$. Analogamente, por $a/b \div c/d$ devemos entender uma fração e/f, tal que $c/d \ \cdot \ e/f \ = \ a/b$.

Desde que tenhamos $c \neq 0$, e pensemos em frações equivalentes, é fácil vermos que a escolha $e/f = ad/bc$ funciona:

$$\frac{c}{d} \cdot \frac{ad}{bc} = \frac{cad}{dbc} = \frac{a}{b}.$$

Coloquemos tudo isso numa definição formal:

Definição 3.23 -

A divisão das frações a/b e c/d (onde $c \neq 0$) produz um resultado chamado quociente, o qual é a fração denotada e definida por:

$$\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}.$$

A divisão dos racionais r e $s \neq 0$, dados por $r = a/b$ e $s = c/d$, produz um resultado chamado quociente, o qual é o número racional denotado por $r \div s$ e representado pelo quociente das frações a/b e c/d. Ou seja:

$$r \div s = \frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}. \tag{3.6}$$

Proposição 3.24 -

A divisão dos números racionais r e $s \neq 0$ está bem definida, no sentido de que o valor do quociente $r \div s$ independe das frações escolhidas para representar os racionais dados e, ademais, realmente $s \cdot (r \div s) = r$.

Prova:

Sendo a/b e A/B representações fracionárias do número racional r, e c/d e C/D representações do racional s, então temos de mostrar a equivalência das frações

$$\frac{ad}{bc} \text{ e } \frac{AD}{BC},$$

o que é o mesmo que provar que $adBC = bcAD$. Ora, pela equivalência das representações fracionárias dadas para r e s, temos que $aB = Ab$ e $cD = Cd$, e daí:

$$adBC = AbdC = AbcD = bcAD.$$

Resta observar que a validade de $s \cdot (r \div s) = r$ é imediata das considerações preliminares que fizemos.

CQD.

Exercício 68 -

Provar que o quociente de duas frações irredutíveis também é irredutível, sempre que os dois numeradores, bem como os dois denominadores, forem relativamente primos.

– imersão dos inteiros nos racionais

Pensando em termos de quantidades, é natural fazermos a identificação de $n \in \mathbb{Z}$ com $n/1 \in \mathbb{Q}$, a qual denotamos por:

$$n = \frac{n}{1}, \quad \forall n \in \mathbb{Z} \ .$$

Essa identificação nos permite fazer abreviações. Por exemplo, nos permite dizer que a soma das frações $2/3$ e $4/3$ é o número inteiro 2.

Notemos, ademais, que essa identificação determina uma homologia operacional:

$$\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} \quad \text{e} \quad \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}$$

que nos mostra que somar e multiplicar os racionais $a/1$ e $b/1$ dá no mesmo que somar e multiplicar os inteiros a e b. Costuma-se, por isso, dizer que, com a associação $n \in \mathbb{Z} \to n/1 \in \mathbb{Q}$, o campo $[\ \mathbb{Z}, +, \cdot\ ]$ está imerso, contido estruturalmente no campo $[\ \mathbb{Q}, +, \cdot]$, o que se costuma *abreviar* escrevendo:

$$[\ \mathbb{Z}, +, \cdot\ ] \subset [\ \mathbb{Q}, +, \cdot\ ], \quad \text{ou mesmo} \quad \mathbb{Z} \subset \mathbb{Q} \ .$$

Por outro lado, sendo a e $b \neq 0$ inteiros, temos:

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

o que nos permite afirmar que:

> o racional (dado por) a/b é o quociente dos inteiros a e b (onde $b \neq 0$).
>
> (Isto deve ser entendido como uma abreviação de "o racional dado por a/b é o resultado da divisão dos racionais dados por $a/1$ e $b/1$, onde a e $b \neq 0$ são inteiros.")

Disso tudo resulta a seguinte notação abreviada de uso tradicional:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b > 0 \right\} .$$

Para o perfeito entendimento dessa notação abreviada, o leitor precisa estar bem ciente de que ela envolve:

- considerar $\frac{a}{b}$ como indicando $a \div b$ (a rigor: $\frac{a}{1} \div \frac{b}{1}$) ;
- considerar que a igualdade entre números de $\mathbb{Q}$ é expressa em termos de equivalência de frações; ou seja, sendo a/b, c/d $\in \mathbb{Q}$, então:

$$a/b = c/d \iff ad = bc .$$

Exercício 69 -

Dar condição suficiente, a mais geral que puder, garantindo que o quociente de a/b por c/d seja um número inteiro.

Exercício 70 -

Dar condição suficiente, a mais geral que puder, garantindo que o quociente de um número inteiro por uma fração irredutível seja um número inteiro.

> Devido ao visto acima, para denotarmos o quociente dos racionais r e s, é tradicional considerarmos equivalentes as notações:
>
> $$\frac{r}{s} = r/s = r \div s$$

– estrutura de corpo de $[\mathbb{Q}, +, \cdot]$

Definição 3.25 -

Chamaremos de zero racional *o número racional que a fração* $0/1$ *representa. Indicaremos este número racional por* 0.
Chamaremos de **unidade racional** *o número racional que a fração* $1/1$ *representa. Indicaremos este número racional por* 1.

Teorema 3.26 -

O campo dos racionais, $[\mathbb{Q}, +, \cdot]$*, tem o seguinte conjunto de propriedades básicas que lhe dão uma estrutura de* corpo[4]. *Para todos os* $r,\ s,\ t \in \mathbb{Q}$*:*

i). as operações $+$ *(adição) e* $\cdot$ *(multiplicação) são fechadas em todo o* $\mathbb{Q}$*:*
$r + s \in \mathbb{Q}$ [*a operação* $+$ *é fechada*]
$r \cdot s \in \mathbb{Q}$ [*a operação* $\cdot$ *é fechada*]

ii). associatividade das operações:
$r + (s + t) = (r + s) + t$ [*associatividade da* $+$]
$r \cdot (s \cdot t) = (r \cdot s) \cdot t$ [*associatividade da* $\cdot$]

iii). existência de elemento neutro:
$r + 0 = r$ [0 *é elemento neutro da* $+$]
$r \cdot 1 = r$ [1 *é elemento neutro da* $\cdot$]

iv). existência de inverso:
$\exists r' \in \mathbb{Q}$ *tal que* $r + r' = 0$ [r' *é o simétrico de* r]
sendo $r \neq 0,\ \exists r'' \in \mathbb{Q}$ *tal que* $r \cdot r'' = 1$ [r'' *é o recíproco de* r]

v). comutatividade das operações:
$r + s = s + r$ [*comutatividade da* $+$]
$r \cdot s = s \cdot r$ [*comutatividade da* $\cdot$]

vi). distributividade da multiplicação:
$r \cdot (s + t) = r \cdot s + r \cdot t$ [*distributividade da* $\cdot$]

Prova:

Certamente, o leitor já percebeu que a prova das propriedades listadas neste teorema é imediata e pura rotina. Nos limitaremos a chamar a atenção para a existência do inverso das operações adição e multiplicação.

[4]Do alemão, *körper*, denominação introduzida por Richard Dedekind, por cerca de 1 870

É imediato se verificar que o simétrico de um racional dado por $r = a/b$ é $r' = (-a)/b = -a/b$. Assim, o simétrico de r é $-r$.

Por sua vez, também é imediato verificarmos que o recíproco r'', de todo número racional $r \neq 0$, é representado por b/a, se r é representado por a/b. Temos, assim, que $r'' = 1/r$ (quociente do racional 1 pelo racional r), o que costuma-se escrever como $r'' = r^{-1}$.

CQD.

Observação 3.27 -

Fique o leitor alertado que nem todos os autores colocam a comutatividade da multiplicação entre as propriedades de uma estrutura de corpo. Um exemplo importante e natural de "corpo" não comutativo é o dos quatérnios, o qual se inclui entre os campos de números hipercomplexos. (Vide último capítulo deste livro).

Uma das razões de termos enunciado o teorema anterior é para poder chamar a atenção do leitor que as demais propriedades algébricas dos números racionais podem ser deduzidas a partir das propriedades listadas no teorema, *sem que precisemos apelar para frações.* Como um exemplo disto, vejamos:

Proposição 3.28 (lei do cancelamento) -

Sendo $r, s \in \mathbb{Q}$*:*

i). $r + t = s + t \Rightarrow r = s, \quad \forall\, t \in \mathbb{Q}\,;$
ii). $r \cdot t = s \cdot t \Rightarrow r = s, \quad \forall\, 0 \neq t \in \mathbb{Q}$

Prova:

Para (i)
Usando a associatividade e o simétrico t' de t temos:

$$r = r + 0 = r + (t + t') = (r + t) + t' = (s + t) + t' = s + (t + t') = s + 0 = s.$$

Para (ii)
Raciocínio semelhante (Exercício). CQD.

Exercício 71 -

Conclua a demonstração do teorema e proposição anteriores.

Exercício 72 -

Usando a lei do cancelamento, prove a unicidade do simétrico e do recíproco. Em particular, conclua que essa unicidade nos permite definir a subtração e a divisão diretamente por: $r - s = r + s'$ *e* $r \div s = r \cdot s''$.

Exercício 73 -

Prove que a lei de integridade ($r \cdot s = 0 \Rightarrow\ r = 0$ *ou* $s = 0$ *) é consequência das demais propriedades listadas no teorema anterior. Isto também vale no caso do do campo dos inteiros?*

Campos numéricos com estrutura de corpo são muito frequentes em Matemática. Adiante, encontraremos outros dois: os muito importantes corpo dos números reais, $\mathbb{R}$, e o corpo dos números complexos, $\mathbb{C}$. Contudo, existem muitos outros exemplos de corpos intervindo decisivamente em problemas importantes de Matemática. Exemplos desses seriam o corpo que caracteriza os problemas geométricos solúveis com régua e compasso, os corpos usados no estudo da resolubilidade algébrica das equações polinomiais, etc.

Em Álgebra Abstrata se mostra que todo anel de integridade dá origem a um corpo, o qual pode ser visto como sendo o "corpo das frações" de elementos do anel. Neste sentido, o corpo $\mathbb{Q}$ é visto como sendo o mais simples e conhecido corpo de frações, no caso, o corpo de frações associado ao anel $\mathbb{Z}$.

3.3 Ordenação dos números racionais

– relação de ordem em $\mathbb{Q}$

Mais uma vez, tomemos nosso "amigo" bolo. Há um procedimento natural para comparar o tamanho de duas frações do mesmo bolo e que tenham o mesmo denominador: é maior a fração que envolve o maior numerador. Daí, do fato de dois quaisquer racionais sempre poderem ser representados por frações de mesmo denominador, decorre uma *ordenação* natural para o conjunto $\mathbb{Q}$, isto é, existe uma maneira natural de decidir quem é o maior entre dois racionais dados.

Com efeito, dados $r = a/b$ e $s = c/d$, temos que

$$r = \frac{ad}{bd}, \quad s = \frac{bc}{bd},$$

logo,

$$r < s \Longleftrightarrow \frac{ad}{bd} < \frac{bc}{bd} \overset{\text{se } bd > 0}{\Longleftrightarrow} ad < bc\,.$$

Definição 3.29 -

A relação de ordem entre números racionais sempre é estabelecida a partir de representações fracionárias de denominador positivo. Assim, dados dois números racionais, $r = a/b$ e $s = c/d$, onde $b, c > 0$, dizemos que r é menor do que s, e escrevemos $r < s$, quando, e só quando, tivermos $ad < bc$.

Também se usa a notação alternativa $s > r$, que se lê "s é maior do que r". Ademais, $r \leqslant s$ significa que ou $r = s$, ou $r < s$. Analogamente para $s \geqslant r$.

Exemplo 3.30 -

Por exemplo, dados $r = 15/21$ e $s = 7/10$, a definição acima nos mostra que temos $r < s$, pois $15 \times 10 < 7 \times 21$. Esta conclusão está de acordo com o raciocínio intuitivo acima:

$$\frac{15}{21} = \frac{15 \times 10}{21 \times 10} = \frac{150}{210} > \frac{147}{210} = \frac{21 \times 7}{21 \times 10} = \frac{7}{10}.$$

Exemplo 3.31 -

Mostremos que, no caso de racionais negativos, precisamos tomar a precaução de usar representações fracionárias de denominador positivo:

$$-\frac{1}{2} = \frac{-1}{2} < \frac{1}{2}, \quad \textit{pois} \quad (-1) \times 2 < 1 \times 2,$$

mas,

$$-\frac{1}{2} = \frac{1}{-2} < \frac{1}{2}, \quad \textit{apesar de termos} \quad 1 \times 2 > 1 \times (-2).$$

Teorema 3.32 -

A definição de ordem nos racionais está bem definida, ou seja, independe das representações fracionárias escolhidas, desde que as mesmas tenham denominador positivo.

Prova:

Sejam dados dois racionais, r e s, com representações fracionárias $r = a/b = A/B$ (onde $b, B > 0$) e $s = c/d = C/D$ (onde $d, D > 0$) . Queremos provar que

$$ad < bc \Longleftrightarrow AD < BC\,.$$

Ora, usando que $aB = Ab$ e $cD = Cd$, e que a multiplicação por inteiros positivos preserva relação de ordem entre inteiros, temos:

$$ad < bc \overset{BD>0}{\iff} adBD < bcBD \overset{\text{comut.}}{\iff} aBdD < bBcD$$
$$\iff AbdB < bBCd \overset{\text{comut.}}{\iff} bdAB < bdBC \overset{bd>0}{\iff} AB < BC.$$

CQD.

Exercício 74 -

i). Mostre que a noção de ordem mencionada anteriormente estende a ordem entre inteiros.

ii). Mostre que o critério mencionado na Definição 3.29 é coerente quando aplicado à representações de mesmo denominador.

iii). Mostre que nem sempre precisamos recorrer ao critério mencionado na Definição 3.29 para comparar dois racionais. Por exemplo, como você poderia decidir, de uma forma mais "econômica", quem é o maior entre $4/10^4$ *e* $32/10^5$ *? E entre* $13/8$ *e* $33/24$*? E entre* $5/6000$ *e* $7/9000$ *?*

– a estrutura de corpo ordenado de $[\,\mathbb{Q}, +, \cdot, <\,]$

Os resultados que seguem estabelecem a compatibilidade da relação de ordem com as operações aritméticas de $\mathbb{Q}$:

Teorema 3.33 -

O campo $[\,\mathbb{Q}, +, \cdot, <\,]$ *tem a estrutura de* corpo ordenado*, ou seja, é um corpo no qual a relação de ordem verifica as duas seguintes propriedades. Sendo* $r, s, t \in \mathbb{Q}$*:*

i). $r < s \iff r + t < s + t,\ \forall t \in \mathbb{Q}$ *[compatibilidade da ordem com a adição]*

ii). $r < s \iff rt < st,\ \forall t > 0$ *[compatibilidade da ordem com a multiplicação]*

Exercício 75 -

Verifique que a hipótese $t > 0$ *no item (ii) do teorema é essencial, isto é, se não sabemos que* $t > 0$*, então não podemos garantir que* $rt < st$.

Proposição 3.34 -

Sendo $r, s, t \in \mathbb{Q}$:

i). a relação de ordem é preservada *na adição:*
$r < s \iff r + t < s + t, \quad \forall t \in \mathbb{Q}$;
$r \leqslant s \iff r + t \leqslant s + t, \quad \forall t \in \mathbb{Q}$.

ii). a relação de ordem é preservada *na multiplicação por racionais positivos:*
$r < s \iff rt < st, \quad \forall t > 0$,
$r \leqslant s \iff rt \leqslant st, \quad \forall t > 0$;

iii). a relação de ordem é invertida *na multiplicação por racionais negativos:*
$r < s \iff rt > st, \quad \forall t < 0$,
$r \leqslant s \iff rt \geqslant st, \quad \forall t < 0$.

Exercício 76 -

Prove o teorema e a proposição anteriores.

Exercício 77 -

Mostre que as propriedades da proposição anterior nos permitem afirmar que, sendo $r_1, r_2, s_1, s_2 \in \mathbb{Q}$:

i). $r_1 < s_1$ *e* $r_2 < s_2 \Rightarrow r_1 + r_2 < s_1 + s_2$;
ii). $0 < r_1 < s_1$ *e* $0 < r_2 < s_2 \Rightarrow r_1 r_2 < s_1 s_2$.

Exercício 78 -

Sendo r, s números racionais, mostre que:

i). $0 < r < s \Rightarrow 1/s < /1r$;
ii). $r < s \not\Rightarrow 1/s < 1/r$.

Fique o leitor advertido de que são poucos os exemplos de corpos ordenados, pois a exigência da ordem ser compatível com a adição e multiplicação é uma exigência bastante forte. O mais importante corpo que não pode ser “ordenável”, é o muito importante corpo $\mathbb{C}$ dos números complexos.

– propriedade arquimediana[5] dos racionais

Teorema 3.35 -

$\mathbb{Q}$ possui a propriedade arquimediana: *dado um número racional $\delta > 0$, para cada escolha de $r \in \mathbb{Q}$, sempre é possível encontrar $n \in \mathbb{N}$, tal que $r < n\delta$.*

O leitor deve ver δ como sendo um módulo, ou valor de referência, com o qual procuramos fazer uma estimativa da magnitude de r.

Prova:

Escrevamos o racional dado $\delta > 0$ como $\delta = \alpha/\beta$, com α, $\beta > 0$. Como o resultado é obviamente verdadeiro para os casos $r \leqslant 0$, seja $r = a/b$, com a, $b > 0$. Assim sendo, temos de provar a existência de algum $n \in \mathbb{N}$ tal que $a/b < n\alpha/\beta$, o que equivale afirmar: $a\beta < n\alpha b$.

Ora, α, $b > 0$ implicam $\alpha b \geqslant 1$, daí $2\alpha b > 1$. Multiplicando os dois membros desta desigualdade pelo fator $a\beta > 0$, obtemos $2a\beta\alpha b > a\beta$, a qual nos permite ver que basta tomarmos $n = 2a\beta$.

CQD.

Exemplo 3.36 -

Observe que a verificação da propriedade $r < n\delta$ é imediata nos casos em que o módulo $\delta \geqslant r$. Com efeito, $n = 1$ já serve nos casos $r < \delta$, e no caso $r = \delta$, o menor n que serve é $n = 2$.

Exemplo 3.37 -

i). Temos

$$\delta = \frac{3}{2} < r = \frac{20}{3}\,,$$

mas

$$r < 10\,\delta, \ \textit{ou seja,}\ \frac{20}{3} < 10 \times \frac{3}{2}\,.$$

[5]De Archimedes, matemático que viveu no mundo grego, por cerca de 200 AC.

ii). Quando $r < 0$, qualquer $n \geqslant 0$ serve, mas podemos usar n negativo. Por exemplo, sendo $\delta = 1/10$, para $r = -3/2$, podemos tomar $n = -14$, o que equivale a dizer:

$$-\frac{3}{2} < (-14)\,\delta = (-14) \times \frac{1}{10}.$$

Proposição 3.38 -

Dado um número racional $\delta > 0$, para cada escolha de r racional acha-se um correspondente $m \in \mathbb{Z}$ tal que:

$$m\delta \leqslant r < (m+1)\delta.$$

Em particular, o menor inteiro n verificando $r < n\delta$ é $n = m + 1$.

Prova:

Deixemos de lado os casos em que r tem a forma $r = k\delta$, com k inteiro, pois são triviais. Com efeito: neles, $m = k$, uma vez que $k\delta = r < (k+1)\delta$.

Nos demais casos, em que $r \neq k\delta$, para $\forall k \in \mathbb{Z}$, precisamos provar a existência de um $m \in \mathbb{Z}$ tal que

$$m\delta < r < (m+1)\delta.$$

Casos $r \geqslant 0$.
Da propriedade arquimediana, existe ao menos um inteiro n verificando $r < n\delta$, e então $0 \leqslant r < n\delta$. Disto resulta que existe ao menos um número inteiro k, verificando $0 \leqslant k \leqslant n$ e tal que $r < k\delta$. Como todo conjunto finito (não vazio) de inteiros tem um menor elemento, seja n' o menor de tais k. Temos, então:

$$(n'-1)\cdot\delta < r < n'\cdot\delta.$$

Vemos, assim, que é só tomarmos $m = n' - 1$.

Casos $r < 0$.
Aplicando o caso anterior em $r' = -r > 0$, achamos m' tal que

$$m'\cdot\delta < r' < (m'+1)\cdot\delta \quad \therefore \quad -(m'+1)\cdot\delta < -r' < -m'\cdot\delta.$$

Escrevendo $m = -(m'+1)$, é imediato que temos $m\delta < r < (m+1)\cdot\delta$.

CQD.

Exercício 79 -

i). Qual o menor inteiro n que nos permite, a partir de $2/3$, ultrapassar $21/6$?

ii). Se de um racional a/b soubermos apenas que

$$\frac{1}{2} < \frac{a}{b},$$

como você calcularia o menor inteiro n que nos permitiria, a partir de $1/2$, ultrapassar a/b?

Exercício 80 -

Dado o racional $134/7$, determine:

i). inteiro m que satisfaça

$$m \leqslant \frac{134}{7} < m+1\,;$$

ii). inteiro m que satisfaça

$$\frac{m}{10} \leqslant \frac{134}{7} < \frac{m+1}{10}\,;$$

iii). inteiro m que satisfaça

$$\frac{m}{10^2} \leqslant \frac{134}{7} < \frac{m+1}{10^2}\,;$$

iv). inteiro m que satisfaça

$$\frac{m}{10^3} \leqslant \frac{134}{7} < \frac{m+1}{10^3}\,;$$

v). em geral, dado $n \in \mathbb{N}$, determine inteiro m que satisfaça

$$\frac{m}{10^n} \leqslant \frac{134}{7} < \frac{m+1}{10^n}\,.$$

Exercício 81 -

Idem ao exercício anterior, para o racional $15/8$.

O grande matemático David Hilbert provou, por cerca de 1 900, que dado um campo $[A, +, \cdot\ <,]$ do qual já sabemos que satisfaz todas as propriedades de corpo, exceto a comutatividade da multiplicação, e ademais, que sua ordem é compatível com essas operações e que tem a propriedade arquimediana, então a multiplicação tem de ser comutativa. Ela é consequência das demais propriedades do corpo.

3.4 Densidade dos racionais

A leitura da seção anterior pode ter levado o leitor a concluir que não encontramos nada de essencialmente novo quando passamos da ordenação dos inteiros para a dos racionais. O objetivo desta seção é mostrar que, na verdade, existe uma enorme diferença entre estes dois campos ordenados.

Iremos nos concentrar no que toca à quantidade de números intermediários entre outros dois dados. Onde, por intermediário de $x < y \in A$, sendo A um campo ordenado, entendemos qualquer $z \in A$ verificando $x < z < y$.

É simples vermos que, quando $A = \mathbb{Z}$, para cada dois $x, y \in \mathbb{Z}$ dados, temos que ou não há intermediários, ou existe uma quantidade finita deles. Por exemplo, entre 1 e 2 não há nenhum intermediário, esses dois números são consecutivos; enquanto que entre 2 e 6 existem três intermediários: $3, 4$ e 5.

Por outro lado, no campo $\mathbb{Q}$ dos números racionais, a situação é diferente: entre quaisquer dois números racionais sempre existem infinitos intermediários. Isto é consequência imediata do seguinte resultado:

Teorema 3.39 -

A média aritmética de quaisquer dois números racionais sempre é um número intermediário entre eles. Sendo $r < s \in \mathbb{Q}$:

$$r < \frac{r+s}{2} < s\,.$$

Prova:

Temos:

$$2r = r + r < r + s < s + s = 2s$$

de modo que, dividindo por 2:

$$r < \frac{r+s}{2} < s\,.$$

CQD.

A partir da aplicação repetida deste teorema é imediato construirmos uma sequência de racionais verificando:

$$r < \cdots < m_3 < m_2 < m_1 < s\,.$$

Com efeito, é só tomarmos m_1 como a média aritmética entre r e s, m_2 como a média entre r e m_1, m_3 a média entre r e m_2, etc. Conclusão:

Entre dois quaisquer números racionais distintos sempre existem infinitos outros racionais.

Exercício 82 -

(*Retirado do livro* Matemática Atual, *de Antônio José Lopes Bigode,* 7^a *série, Ed.Atual,* 1 994)

i). Dê o valor de um número racional entre $2/5$ *e* $2/3$.

ii). Apresente um número racional que seja maior do que $3/4$ *e menor do que* r*, sabendo apenas que* $3/4 < r$ *.*

Definição 3.40 -

Um conjunto A de números racionais é dito denso *(em $\mathbb{Q}$) se entre dois elementos (distintos) quaisquer de $\mathbb{Q}$ existirem infinitos elementos de A; ou seja: entre os dois elementos de $\mathbb{Q}$ dados, existem infinitos intermediários que estão em A.*

Exercício 83 -

Dado um conjunto A de números racionais, mostre que, para provar que o mesmo é denso, basta verificarmos que sempre que escolhermos dois elementos de $\mathbb{Q}$, sempre existe pelo menos um elemento de A entre eles.

Exemplo 3.41 -

Pelo Teorema 3.39, $\mathbb{Q}$ é denso. Como é imediato verificar que $\mathbb{Z}$ não é denso, temos que um dado conjunto infinito de números racionais pode ser, ou não, denso. Por outro lado, é imediato se ver que nenhum conjunto finito de $\mathbb{Q}$ pode ser denso. Nos exercícios a seguir examinamos mais exemplos.

Exercício 84 -

Verifique se os subconjuntos de $\mathbb{Q}$ a seguir são, ou não, densos:

i). A = *conjunto dos números racionais que podem ser expressos por uma fração de denominador* 4*;*

ii). B = *conjunto dos números racionais que podem ser expressos por uma fração iredutível, cujo denominador é potência inteira de* 4*;*

iii). C = *conjunto dos números racionais que podem ser expressos por uma fração da forma "inteiro par sobre inteiro ímpar".*

Exercício 85 -

i). Prove que o conjunto dos racionais representáveis por uma fração com denominador potência de 10 *é um conjunto denso.*

ii). Prove que o conjunto dos racionais representáveis por uma fração com denominador potência de 13 *é um conjunto denso.*

Exercício 86 -

(*Retirado do livro* Matemática Atual, *de Antônio José Lopes Bigode,* 7^a *série, Ed.Atual,* 1 994)
Dar três exemplos de subconjuntos de $\mathbb{Q}$*:*

i). que sejam densos;

ii). que não sejam densos.

Exercício 87 -

i). Mostre que em $\mathbb{Z}$*, sendo* x_0 *positivo, é impossível se construir uma sequência infinita de números positivos e estritamente decrescentes a partir do* x_0 *dado.*

ii). Mostre que, ao contrário, em $\mathbb{Q}$*, é perfeitamente possível tal construção.*

Exercício 88 -

Comparemos agora o que pode ocorrer com os números positivos maiores do que um número positivo dado, x_0*, conforme este número esteja em* $\mathbb{Z}$ *ou em* $\mathbb{Q}$*:*

i). Mostre que, em $\mathbb{Z}$*, toda sequência estritamente crescente de inteiros maiores do que* x_0 *tem de crescer ao infinito*
(este fato é intuitivamente óbvio, mas pede-se dar uma prova formal explorando que, se tivermos $1 \leqslant x_0 < x_1 < x_2 < \cdots$*, com todos esses* $x_n \in \mathbb{Z}$*, então* $x_n > n$*).*

ii). Mostre que, em $\mathbb{Q}$, é perfeitamente possível construirmos sequências infinitas de números racionais estritamente crescentes, mas que não crescem ao infinito.

Exercício 89 -

Seja A um subconjunto de $\mathbb{Q}$, que tem a seguinte propriedade: entre quaisquer dois elementos (distintos) de A encontramos infinitos elementos de A. Pede-se mostrar que tal conjunto A não precisa ser denso.

Cada número inteiro x admite um consecutivo e este é $x+1$. Entre eles não existe nenhum inteiro intermediário. Ademais, dados dois inteiros não consecutivos, entre eles existirá apenas uma quantidade finita de inteiros intermediários.

Um número racional, contudo, nunca tem consecutivo. Entre quaisquer dois racionais sempre existem infinitos racionais intermediários. O conjunto dos números racionais é denso.

Reiteramos:
a densidade diferencia drasticamente os campos ordenados $\mathbb{Z}$ e $\mathbb{Q}$!

CAPÍTULO 4

NÚMEROS RACIONAIS: SUA EXPANSÃO DECIMAL

4.1 Frações ordinárias x decimais

No que segue, precisaremos falar em diversos tipos de representações dos números racionais. Assim, é conveniente introduzirmos duas definições preliminares.

Definição 4.1 -

Por fração ordinária *entendemos toda fração da forma a/b, onde a é um inteiro qualquer e b um inteiro positivo.*

Proposição 4.2 -

Toda fração irredutível é fração ordinária. Em particular, todo número racional tem infinitas representações equivalentes em fração ordinária.

Prova:

Dado r racional, e a/b a fração irredutível que o representa, é imediato que

$$r = \frac{a}{b} = \frac{2a}{2b} = \frac{3a}{3b} = \dots .$$

CQD.

Note que, para cada representação em fração ordinária de um número racional r, está associada uma fração não ordinária que também o representa:

$$r = \frac{a}{b} = \frac{-a}{-b}.$$

Convenção:
a partir de agora, ao escrevermos um racional na forma a/b, *estaremos sempre subentendendo* que trata-se de uma fração ordinária. Isto significa que $b > 0$, mas não necessariamente $\mathrm{mdc}\,(a, b) = 1$.

Definição 4.3 -

Fração decimal é toda fração cujo denominador é igual a 10, 100, 1 000 *ou qualquer outra potência positiva de* 10.

São exemplos de frações decimais:

$$\frac{-2}{10}, \ \frac{7}{1\,000}, \ \frac{138}{10}, \ \frac{-733}{100}.$$

A noção de fração decimal é bastante conhecida, pois é de uso comum na prática. Contudo, aqui, nosso interesse nelas é apenas teórico: elas terão um papel fundamental na construção dos números reais, conforme veremos nos próximos capítulos.

Exemplo 4.4 -

O número racional dado pela fração $2/5$ *pode ser representado por uma fração decimal, pois* $2/5 = 4/10$.
Note que ele também pode ser representado por infinitas outras frações decimais:

$$\frac{2}{5} = \frac{4}{10} = \frac{40}{100} = \frac{400}{1000} = \cdots .$$

Exercício 90 -

V ou F? Justifique. Uma soma de racionais representáveis por frações decimais é também um racional representável por uma fração decimal.

É muito importante sempre ter em vista que *existem números racionais que não podem ser representados por nenhuma fração decimal*. O caso mais simples é o do número $1/3$. Assim, note que:

- é impossível que $1/3 = m/10$, pois $3m = 10$ não tem solução em $\mathbb{Z}$. Com efeito: $3 \times 3 < 10 < 3 \times 4$;
- é impossível que $1/3 = m/100$, pois $3m = 100$ não tem solução em $\mathbb{Z}$. Com efeito: $3 \times 33 < 100 < 3 \times 34$;
- etc., pois $3m = 9,\ 99,\ 999,\ 9\,999$ etc., se $m = 3,\ 33,\ 333,\ 3\,333$ etc., e $3(m+1) = 3m + 3$.

Exercício 91 -

Dar uma demonstração de que $1/3$ não pode ser representado por nenhuma fração decimal $m/10^n$, usando fatoração em primos nos membros da igualdade $3m = 10^n$.

Exercício 92 -

O leitor é convidado a encontrar mais exemplos de números racionais que não sejam representáveis por uma fração decimal. Sugerimos estudar os seguintes racionais:

$$\frac{1}{5}, \frac{3}{50}, \frac{2}{6}, \frac{12}{7}.$$

Surge, então, a seguinte questão de caráter geral:

> que condições sobre os números inteiros a e b nos garantem que o número racional a/b possa ser representado por uma fração decimal?

Os resultados seguintes respondem esta questão explorando que, como a fatoração em primos de 10 é $10 = 2 \times 5$, as das suas outras potências positivas são:

$$100 = 10^2 = 2^2 \times 5^2,\ 1\,000 = 10^3 = 2^3 \times 5^3\ , \ldots , 10^n = 2^n \times 5^n.$$

Teorema 4.5 -

Quando o denominador de uma fração ordinária tiver uma fatoração em primos contendo apenas os fatores 2 e/ou 5, esta fração será equivalente a uma fração decimal.

Prova:

Pela hipótese, a fatoração em primos de b é da forma $b = 2^m \cdot 5^n$, onde ao menos um dentre m e n é não nulo. Supondo que $m \geqslant n$, teremos:

$$\frac{a}{b} = \frac{a}{2^m \cdot 5^n} = \frac{a \cdot 5^{m-n}}{2^m \cdot 5^n \cdot 5^{m-n}} = \frac{a \cdot 5^{m-n}}{2^m \cdot 5^m} = \frac{a \cdot 5^{m-n}}{10^m} = \frac{a'}{10^m}\,.$$

Usa-se um raciocínio completamente análogo na possibilidade $n \geqslant m$.

CQD.

Exercício 93 -

Estudemos a recíproca do Teorema 4.5. Obviamente, devemos nos concentrar nos casos de um número racional dado por a/b, onde a e $b > 0$ são inteiros relativamente primos. Neste sentido, supondo que a/b possa ser representado por uma fração decimal, prove que, ou $b = 1$, ou $b \neq 1$ e, ademais, em sua fatoração por primos aparecem somente potências de 2 e/ou 5.

Exercício 94 -

i). Determine uma representação para o racional $3/50$ *com denominador potência de* 10. *A seguir responda: é única esta representação? Em caso negativo, quantas representações decimais existem para* $3/50$*?*

ii). Idem (i) para o racional $3/8$.

O exercício seguinte investiga se é possível encaixarmos uma fração decimal entre cada par de números racionais dados.

Exercício 95 -

i). Mostre que existem $m \in \mathbb{N}$ e $n \in \mathbb{N}$ suficientemente grandes para que

$$\frac{2}{5} < \frac{m}{10^n} < \frac{2}{3}\,.$$

ii). Sejam x e y números racionais positivos e distintos, digamos $x < y$. Mostre que existem $m \in \mathbb{N}$ e $n \in \mathbb{N}$ suficientemente grandes tais que

$$x < \frac{m}{10^n} < y\,.$$

iii). Idem (ii), mas agora

$$x < \frac{m}{10^n} < \frac{m+1}{10^n} < y\,.$$

iv). Conclua disso que arbitrariamente próximo de qualquer número racional existe uma fração decimal.

4.2 Expansão decimal dos racionais

No resto deste capítulo, estaremos envolvidos com outra forma de representar números racionais, distinta das frações ordinárias, mas também bastante conhecida pelo leitor; ela é denominada representação posicional decimal, e vulgarmente conhecida como "representação com vírgula" de um número racional.

Essa forma de representar um número racional será muito importante para a conceituação e estudo dos números reais que faremos nos capítulos que se seguem, e nada mais é do que uma extensão, para os números racionais, da mais conhecida representação posicional decimal (isto é, em base dez) dos números naturais.

– A ideia de expansão decimal de números naturais

Supomos que o leitor saiba que, usando divisões euclidianas, podemos expandir ou expressar cada número natural N como uma soma de múltiplos das potências $\geqslant 0$ do módulo base 10; ou seja, como soma de múltiplos de 1, 10, 100, 1000, ...:

$$N = a_n \times 10^n + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0\,,$$

onde os fatores de multiplicidade a_0, $a_1\, a_2, \ldots \in \{0,1,2,3,4,5,6,7,8,9\}$ e são únicos para cada N.

Também supomos que o leitor saiba que a decomposição acima costuma ser representada de um modo abreviado, como a expansão decimal:

$$N = a_n \ldots a_2 a_1 a_0\,,$$

onde a ordem é fixa e determinada pela decomposição acima. Este sistema de representação é chamado de sistema de numeração posicional decimal para os naturais, e os números a_k são chamados de algarismos ou dígitos da representação.

Esse sistema é dito ser "posicional", pois a parcela com que cada algarismo contribui na decomposição, depende da posição em que ele é colocado na representação. Exemplificando, como

$$3 \times 10^3 + 1 \times 10^2 + 9 \times 10^1 + 4 \times 10^0\,,$$

temos que sua representação posicional (ou sua expansão decimal) fica

$$3194 \overset{\text{def.}}{=} 3 \times 10^3 + 1 \times 10^2 + 9 \times 10 + 4\,.$$

Se permutarmos esses algarismos, obteremos um outro número representado. Por exemplo:

$$9413 = 9 \times 10^3 + 4 \times 10^2 + 1 \times 10 + 3\,.$$

Numa representação posicional, não é apenas decisivo quais algarismos estão sendo usados, mas também a posição em que cada um deles aparece na representação.

Resumindo

De um modo geral, achar a expansão decimal de um número natural N consiste em decompô-lo como uma soma de múltiplo da unidade, mais múltiplo da dezena, mais múltiplo de centena, etc., sendo todos os respectivos fatores de multiplicidade obrigatoriamente tirados do conjunto $\{0, 1, 2, \cdots, 9\}$. Teremos, assim, uma soma do tipo:

$$N = a_0 \times 1 + a_1 \times 10 + a_2 \times 100 + \cdots + a_n \times 1\underbrace{00\ldots0}_{n\ zeros}$$

$$= a_0 \times 10^0 + a_1 \times 10^1 + a_2 \times 10^2 + \cdots + a_n \times 10^n\,.$$

Tradicionalmente, esta decomposição é representada abreviadamente escrevendo-se apenas os fatores de multiplicidade e colocando-os, no estilo da escrita árabe, da esquerda para a direita, como:

$$N = a_n a_{n-1} \ldots a_0.$$

Observação 4.6 -

Visando uma melhor compreensão da ideia de expansão decimal, é conveniente que a comparemos com a representação posicional em uma base distinta de 10*. Com o advento dos computadores eletrônicos digitais, ficou bastante comum trabalharmos com expansões binárias (ou em base dois) de números naturais* k*, o que consiste em escrever*

$$N = (b_m b_{m-1} \ldots b_0)_2\,,$$

significando esta notação que teremos a seguinte expansão ou decomposição em potências $\geqslant 0$ *da base* 2*:*

$$N = b_m \times 2^m + b_{m-1} \times 2^{m-1} + \cdots + b_1 \times 2 + b_0\,,$$

onde $b_i \in \{0, 1\}$, *para* $0 \leqslant i \leqslant m$. *Por exemplo, a expansão binária de* 5 *é*

$$5 = (101)_2\,,$$

pois

$$5 = 1 \times 2^2 + 0 \times 2^1 + 1.$$

Na representação posicional binária os algarismos são os símbolos $\{0, 1\}$, *ditos algarismos binários*[1].

Neste livro, não precisaremos aprofundar o estudo das representações posicionais de um número natural. Nos limitaremos a usá-las e admitiremos como conhecido que todo número natural tem uma, e somente uma representação posicional.

Convenção importante.

A partir de agora, até o final do capítulo, será imprescindível, para evitar confusões, que façamos uso do símbolo $\times$ quando estivermos nos referindo a um produto. Assim, quando escrevermos simplesmente $a_2a_1a_0$, por exemplo, estaremos significando a representação do número

$$a_2 \times 10^2 + a_1 \times 10 + a_0\,,$$

número este que é completamente diferente do número

$$a_2 \times a_1 \times a_0\,.$$

[1] Apesar de uso comum em Informática, não há sentido em dizer "dígitos binários", pois dígito vem do latim: digitus (= dedo), e temos dez dedos nas mãos!

Exercício 96 -

Mostre que:

$$\begin{aligned} 10-1 &= 9 \\ 10^2-1 &= 99 \\ 10^3-1 &= 999 \\ \dots & \quad \dots \\ 10^n-1 &= \underbrace{9\dots9}_{n\ vezes},\ \forall n \in \mathbb{N}^*, \end{aligned}$$

ou seja,

$$10^n - 1 = 9 + 9\times 10 + 9\times 10^2 + \cdots + 9\times 10^{n-1}.$$

Exercício 97 -

Mostre que:

$$\begin{aligned} 10^0 \times (10^n-1) &= \underbrace{9\dots9}_{n} \\ 10^1 \times (10^n-1) &= \underbrace{9\dots9}_{n}0 \\ 10^2 \times (10^n-1) &= \underbrace{9\dots9}_{n}00 \\ 10^3 \times (10^n-1) &= \underbrace{9\dots9}_{n}000 \\ \dots & \quad \dots \\ 10^m \times (10^n-1) &= \underbrace{9\dots9}_{n}\underbrace{0\dots0}_{m}, \quad \forall m \in \mathbb{N}, n \in \mathbb{N}^*. \end{aligned}$$

– A ideia de expansão decimal de números inteiros

Quando um número inteiro, k, for negativo, teremos $-k$ positivo e, então, sabemos como escrever sua expansão decimal:

$$-k = u_n \dots u_1 u_0 = u_n \times 10^n + u_{n-1}\times 10^{n-1} + \cdots + u_1 \times 10 + u_0.$$

Ora, como:

$$k = -\big(u_n \times 10^n + u_{n-1}\times 10^{n-1} + \cdots + u_1\times 10 + u_0\big),$$

é muito natural abreviarmos esta última como:

$$k = -u_n \dots u_1 u_0.$$

Ou seja, a representação posicional decimal dos inteiros negativos é imediatamente redutível à dos inteiros positivos.

– A ideia de expansão decimal de números racionais

Passemos a mostrar o que se entende pela expansão decimal, $\operatorname{dec}(r)$, de um número racional r qualquer. Faremos isso por meio de duas reduções.

Primeira redução.

Basta sabermos fazer a expansão decimal dos racionais positivos. Com efeito, a expansão de cada racional negativo, r, será reduzida à expansão de seu simétrico, $-r$, o qual é um racional positivo. Com efeito, quando $r < 0$, como $-r > 0$, adotaremos como expansão decimal de r:

$$\operatorname{dec}(r) = -\operatorname{dec}(-r),$$

semelhantemente ao que fizemos com os números inteiros.

Admitiremos como do conhecimento do leitor a expansão decimal de qualquer número inteiro. Assim, nossa segunda redução remeterá a expansão decimal de um racional positivo r à expansão do que chamaremos de parte fracionária de r.

Proposição 4.7 -

Todo racional positivo, r, tem uma decomposição única da forma $r = r' + r''$, onde:

- *$r' \geqslant 0$ é um número inteiro (chamado de* parte inteira *de r);*
- *r'' é um racional verificando $0 \leqslant r'' < 1$ (chamado* parte fracionária *de r).*

Ademais:

- *a parte inteira r' de r pode ser obtida como o quociente, q, da divisão euclidiana de a por b, onde $r = a/b$ é uma representacão em fração ordinária de r com $a, b > 0$;*
- *a parte fracionária de r é $r - q$.*

Prova:

A existência da decomposição.
Seja $r = a/b$, com a e b inteiros positivos. A divisão euclidiana de a por b nos dá

$a = qb + R$, com $q \geqslant 0$ inteiro e $0 \leqslant R < b$. Disso resulta que $r = a/b = q + R/b$. Afirmamos que $r' = q$ e $r'' = R/b$. Com efeito, como q é inteiro, e como $R/b = a/b - q = r - q$, resta mostrar que $0 \leqslant R/b < 1$. Ora, esta desigualdade é imediata da definição de ordem entre números racionais e o fato de que $0 \leqslant R < b$.

A unicidade da decomposição.
Suponhamos que $r = r' + r''$ e $r = R' + R''$, com r' e R' inteiros $\geqslant 0$, e que $0 \leqslant r'', R'' < 1$.
É imediato vermos que $r'' = R''$ implica $r' = R'$. Resta mostrar que a possibilidade $r'' \neq R''$ resulta num absurdo. Com efeito, supondo que $r'' > R''$, como $0 \leqslant R'' < r'' < 1$, segue que $r'' - R''$ é um número racional verificando $0 < r'' - R'' < 1$. Por outro lado, a igualdade $r' + R' = r = r'' + R''$ nos dá $r'' - R'' = R' - r' =$ número inteiro, o que é um absurdo frente a $0 < r'' - R'' < 1$. Um raciocínio absolutamente análogo nos mostra que também $r'' < R''$ nos leva a absurdo.

CQD.

Como consequência, resulta a redução que segue.

Segunda redução: $\operatorname{dec}(r) = \operatorname{dec}(r')\,,\, \operatorname{dec}(r'')$.

Definimos dec de modo que a expansão decimal de todo racional positivo seja vista como a justaposição da expansão decimal de sua parte inteira com a expansão decimal de sua parte fracionária.
Adiante, veremos que podemos entender a justaposição acima como uma soma:

$$\operatorname{dec}(r) = \operatorname{dec}(r') + \operatorname{dec}(r'').$$

A expansão decimal da parte fracionária, r'', de um racional positivo r, como deveria ser esperado, tem a forma de uma decomposição em um múltiplo do décimo, somado com um múltiplo do centésimo, mais um múltiplo do milésimo, e assim por diante, onde estes múltiplos são números do conjunto de dígitos: $\{0, 1, 2, \cdots, 9\}$. De modo que buscamos uma decomposição da forma:

$$\begin{aligned} r'' &= \frac{b_1}{10} + \frac{b_2}{100} + \frac{b_3}{1000} + \cdots \\ &= \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{b_3}{10^3} + \cdots, \quad \forall\, b_i \in \{0, 1, 2, \cdots, 9\}. \end{aligned}$$

Como a expansão decimal do número racional positivo r é a soma da expansão de sua parte inteira mais a da sua parte fracionária, temos:

$$r = r' + r'' = a_n \times 10^n + \cdots + a_1 \times 10 + a_0 + \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{b_3}{10^3} + \cdots ,$$

o que será abreviado como

$$r = a_n \ldots a_1 a_0, b_1 b_2 b_3 \ldots$$

(Adiante, gradativamente, elucidaremos o significado do segundo ... acima. Por enquanto, o leitor deve interpretá-lo como uma reticência).

Como consequência da primeira redução, dado um racional $r < 0$, uma vez achada a expansão decimal do racional positivo $-r$, digamos $-r = a_m \ldots a_1 a_0 \,,\, b_1 b_2 b_3 \ldots$, a expansão de r fica:

$$-r = a_m \ldots a_1 a_0 \,,\, b_1 b_2 b_3 \ldots \quad \Rightarrow \quad r = -\, a_m \ldots a_1 a_0 \,,\, b_1 b_2 b_3 \ldots .$$

Acima, não mencionamos o caso $r = 0$, o qual tem expansão trivial: $0 = 0,0 = 0,00 = 0,000 = \cdots$.

4.3 Conversão: de fração ordinária para expansão decimal

– O caso especial das frações decimais

Dizemos que este é um caso especial pois, conforme já sabemos, nem todo número racional pode ser representado por uma fração decimal; infelizmente, pois este tipo de fração é facilmente expandido. No que segue, veremos a ideia básica e depois formalizaremos.

Exemplo 4.8 -

Seja determinar a expansão decimal do número racional r , dado por $r = \frac{27\,498}{1\,000}$. Iniciamos fazendo a expansão do numerador da fração e depois obtemos uma soma *de frações decimais que serão simplificadas:*

$$\begin{aligned}\frac{27\,498}{1\,000} &= \frac{20\,000+7\,000+400+90+8}{1\,000}\\ &= \frac{20\,000}{1\,000}+\frac{7\,000}{1\,000}+\frac{400}{1\,000}+\frac{90}{1\,000}+\frac{8}{1\,000}\\ &= 20+7+\frac{4}{10}+\frac{9}{100}+\frac{8}{1\,000}\\ &= 27+\frac{4}{10}+\frac{9}{100}+\frac{8}{1\,000}=27,498.\end{aligned}$$

Na prática se procede mais rapidamente:

$$\begin{aligned}\frac{27\,498}{1\,000} &= \frac{27\,000}{1\,000}+\frac{400}{1\,000}+\frac{90}{1\,000}+\frac{8}{1\,000}\\ &= 27+\frac{4}{10}+\frac{9}{100}+\frac{8}{1\,000}=27,498.\end{aligned}$$

Formalizando e generalizando:

Teorema 4.9 -

A parte fracionária de cada fração decimal (positiva) pode ser decomposta como uma soma de frações decimais especiais, e cada uma delas tem como numerador um dos dígitos que expressa o numerador da fração original.

Exemplo 4.10 -

Para a fração decimal acima, $\frac{27\,498}{1\,000}$*, temos que sua parte fracionária,* $\frac{498}{1000}$*, pode ser assim ser decomposta:*

$$\frac{498}{1\,000}=\frac{4}{10}+\frac{9}{100}+\frac{8}{1\,000}=0,498.$$

Por outro lado, observe:

$$\frac{37}{1\,000}=\frac{037}{1\,000}=\frac{0}{10}+\frac{3}{100}+\frac{7}{1\,000}=0,037.$$

Corolário 4.11 -

Todo número racional dado por uma fração decimal*, positiva ou negativa, tem uma quantidade finita de dígitos na parte fracionária de sua expansão decimal. Consequentemente, esta expansão tem de ter a forma:*

$$\pm a_n \dots a_1 a_0 \, , \, b_1 b_2 b_3 \dots b_m \, .$$

– O caso das frações ordinárias equivalentes a uma fração decimal

Antes de mais nada, observemos que, da definição de frações equivalentes e do item anterior, é imediata a validade do seguinte resultado:

Teorema 4.12 -

Todo número racional dado por uma fração ordinária equivalente a uma fração decimal, positiva ou negativa, tem uma quantidade finita de dígitos na parte fracionária de sua expansão decimal. Consequentemente, esta expansão tem de ter a forma:

$$\pm a_n \dots a_1 a_0 \, , \, b_1 b_2 b_3 \dots b_m \, .$$

Reciprocamente, toda expansão decimal finita representa um número racional que é dado por uma fração decimal.

Passando à obtenção de tal expansão, lembremos que é o Teorema 4.5 que vai nos permitir afirmar que a fração ordinária é, ou não, equivalente a alguma fração decimal. Caso isto ocorra, a expansão decimal de tal fração ordinária fica reduzida à expansão da fração decimal equivalente. Podemos obter esta expansão ou transformando a fração dada em uma fração decimal, ou trabalhando diretamente com a fração ordinária dada. Vejamos.

Método da transformação
usando o Teorema 4.5, decidimos se é o caso da fração dada ser equivalente a uma fração decimal. Se assim for, multiplicando o numerador e denominador da fração dada por um fator adequado, a transformamos numa fração decimal e, então, escrevemos sua expansão decimal usando o teorema anterior.

Exemplo 4.13 -

Determinar a expansão decimal do número racional dado pela fração $17/5$.

Pelo Teorema 4.5, é imediato que a mesma é equivalente a uma fração decimal. Com efeito, $17/5 = 34/10$. *Decompondo esta última em parte inteira e parte fracionária, fica imediato usarmos o teorema anterior:*

$$\frac{17}{5} = \frac{34}{10} = 3 + \frac{4}{10} = 3,4\,.$$

Exemplo 4.14 -

Determinar a expansão decimal da fração $3837/250$.

Seu denominador tem como fatoração em primos: $250 = 25\times 10 = 5^2\times 2\times 5 = 2\times 5^3$. *Como esta fatoração contém apenas potências de 2 e 5, pelo Teorema 4.5, segue que tal fração é equivalente a uma fração decimal. Para obter tal fração decimal, transformamos* 2×5^3 *num produto de fatores elevados à potências iguais. Ou seja: transformamos* 2×5^3 *em* $2^3\times 5^3 = 4\times 2\times 5^3$. *Com isso, vemos que temos a equivalência:*

$$\frac{3837}{250} = \frac{4\times 3837}{4\times 250} = \frac{15\,348}{1\,000} = 15 + \frac{348}{1\,000}\,.$$

Podemos, enfim, aplicar o Teorema 4.9, para concluir:

$$\frac{3837}{250} = 15 + \frac{348}{1\,000} = 15,348\,.$$

Método das divisões
usando o Teorema 4.5, decidimos se é o caso da fração dada ser equivalente a uma fração decimal. Se assim for, fazemos sucessivas divisões euclidianas para determinar, pela ordem, a parte inteira da expansão, a parte dos décimos, a dos centésimos, a dos milésimos, etc. da parte fracionária.
(Paramos quando encontrarmos o primeiro resto nulo. Como a parte fracionária consiste em uma lista finita de dígitos, esta parada obrigatoriamente terá de ocorrer. Ou seja: este processo é terminante! Confira nos teoremas a seguir.)

Observação 4.15 -

Como o leitor deverá observar nos exemplos que se seguem, este método é mais complicado do que o método da transformação. Contudo, ele tem a vantagem de poder ser aplicado nos casos em que a fração dada não seja equivalente a uma fração decimal, casos que veremos adiante.

Exemplo 4.16 -

Determinar, pelo método das divisões, a expansão decimal do número racional dado pela fração $3837/250$*.*

Já vimos acima que esta fração é equivalente a uma decimal. Concentremo-nos, então, na exemplificação do método propriamente dito.

– Parte inteira:
como $3837 = 15 \times 250 + 87$*, temos:*

$$\frac{3837}{250} = 15 + \frac{87}{250}\,.$$

– Parte dos décimos, ou casa dos décimos:
observemos que

$$\frac{87}{250} = \frac{1}{10} \times \frac{870}{250} = \frac{1}{10} \times \frac{3 \times 250 + 120}{250} = \frac{3}{10} + \frac{120}{2500},$$

e, portanto, que cabem apenas 3 *décimos em* $87/250$*, pois* $0 < 120 < 250$ *permite escrever* $0 < 120/2500 < 1/10$*; assim que a expansão até a casa dos décimos fica:*

$$\frac{3837}{250} = 15 + \frac{87}{250} = 15 + \frac{3}{10} + \frac{120}{2500} = 15,3 + \frac{120}{2500}\,.$$

– Parte dos centésimos, ou casa dos centésimos:
prosseguindo de modo semelhante, como

$$\frac{120}{2500} = \frac{1}{10} \times \frac{1200}{2500} = \frac{1}{100} \times \frac{1200}{250} = \frac{1}{100} \times \frac{4 \times 250 + 200}{250} = \frac{4}{100} + \frac{200}{25000}\,,$$

e, como cabem apenas 4 *centésimos em* $12/250$ *(pois* $0 < 200 < 250$ *nos permite escrever* $200/25000 < 1/100$*), então a expansão até a casa dos centésimos fica:*

$$\frac{3837}{250} = 15,3 + \frac{120}{2500} = 15,3 + \frac{4}{100} + \frac{200}{25000}$$

$$= 15,3 + 0,04 + \frac{200}{25000} = 15,34 + \frac{200}{25000}\,.$$

– *Casa dos milésimos:*

$$\frac{200}{25000} = \frac{1}{10} \times \frac{2000}{25000} = \frac{1}{1000} \times \frac{8 \times 250 + 0}{250} = \frac{8}{1000},$$

de modo que podemos concluir, escrevendo:

$$\frac{3837}{250} = 15,34 + \frac{200}{25000} = 15,34 + \frac{8}{1000} = 15,34 + 0,008 = 15,348,$$

o que significa:

$$\frac{3837}{250} = 15 + \frac{3}{10} + \frac{4}{100} + \frac{8}{1\,000}.$$

Exemplo 4.17 -

Determinar, pelo método das divisões, a expansão decimal da fração $7/20$.

Como $20 = 4 \times 5 = 2^2 \times 5$, *é imediato que esta fração seja equivalente a uma decimal. Passemos a achar, gradativamente e sem procurar fazer improvisações, a sua parte inteira, e os valores das casas dos décimos, centésimos, etc. de sua expansão decimal.*

– *Parte inteira:*
como $0 < 7/20 < 1$, *segue que a parte inteira é nula:* $7/20 = 0 + 7/20$.

– *Casa dos décimos:*

$$\frac{7}{20} = \frac{1}{10} \times \frac{70}{20} = \frac{1}{10} \times \frac{3 \times 20 + 10}{20} = \frac{3}{10} + \frac{10}{200} = 0,3 + \frac{10}{200}\,.$$

– *Casa dos centésimos:*
como

$$\frac{10}{200} = \frac{1}{100} \times \frac{100}{20} = \frac{1}{100} \times \frac{5 \times 20 + 0}{20} = \frac{5}{100} + 0\,,$$

concluímos que:

$$\frac{7}{20} = 0,3 + \frac{10}{200} = 0,3 + \frac{5}{100} = 0,3 + 0,05 = 0,35\,,$$

o que é uma abreviação para:

$$\frac{7}{20} = \frac{3}{10} + \frac{5}{100}\,.$$

Exemplo 4.18 -

Determinar, pelo método das divisões, a expansão decimal do número racional dado pela fração $-1/40$.

Como $40 = 8\times 5 = 2^3\times 5$, *é imediato que esta fração seja equivalente a uma decimal. Passemos a determinar sua expansão decimal.*

– Parte inteira:
como $0 < 1/40 < 1$, *segue que a parte inteira é nula:* $1/40 = 0 + 1/40$.

– Casa dos décimos:
$\frac{1}{40} < \frac{1}{10}$, *de modo que a casa dos décimos também é nula:*

$$\frac{1}{40} = \frac{1}{10}\times\frac{10}{40} = \frac{1}{10}\times\frac{0\times 40+10}{40} = \frac{0}{10}+\frac{10}{400},$$

ou seja:

$$\frac{1}{40} = \frac{0}{10}+\frac{10}{400} = 0,0+\frac{10}{400}\,.$$

– Casa dos centésimos:
é não nula, pois $40 < 100$ *dá* $1/100 < 1/40$*; para determinar seu valor:*

$$\frac{10}{400} = \frac{1}{100}\times\frac{100}{40} = \frac{1}{100}\times\frac{2\times 40+20}{40} = \frac{2}{100}+\frac{20}{4000} = 0,02+\frac{20}{4000}\,.$$

– Casa dos milésimos:

$$\frac{20}{4000} = \frac{1}{1000}\times\frac{200}{40} = \frac{1}{1000}\times\frac{5\times 40+0}{40} = \frac{5}{1000}+0\,,$$

de modo que:

$$\frac{1}{40} = 0,02+\frac{20}{4000} = 0,02+\frac{5}{1000} = 0,025\,.$$

Podemos concluir, afirmando que:

$$-\frac{1}{40} = -0,025 = -\frac{0}{10}-\frac{2}{100}-\frac{5}{1000}\,.$$

Observação 4.19 (importante) -

O método das divisões é apenas um detalhamento do método que todos aprendemos no Ensino Fundamental. Comprovemos isto comparando os restos obtidos nas divisões euclidianas dos exemplos anteriores, com os cálculos feitos à moda tradicional do Ensino Fundamental.

Para o exemplo $3837/250$, *os restos obtidos foram, pela ordem:* $87, 120, 200, 0$. *Compare com o cálculo tradicional:*

```
         3837      | 250
                    --------
         250        15,348
         1337
         1250
resto---> 87
           870
           750
resto---> 120
           1200
           1000
resto--->  200
            2000
            2000
resto--->     0
```

Note que, de antemão, é impossível saber onde a divisão vai parar, a menos que usemos que o número dado pode ser escrito como $3837/250 = 15 + 87/250 = 15 + 348/1000$. *Com efeito, como o método da divisão vai determinando sucessivamente o valor da casa dos décimos, dos centésimos, etc., ele terá de parar na casa dos milésimos, no caso deste número.*

Como exercício, deixamos para o leitor fazer a mesma comparação nos demais exemplos.

Exercício 98 -

i). Seja a/b *uma fração irredutível positiva e equivalente a uma fração decimal* a'/b'. *Sabemos que isto implica a existência de um* k *inteiro positivo tal que* $a' = ka$ *e* $b' = kb$. *Assim, pede-se provar que a aplicação do método das divisões em* a'/b' *produz os mesmos quocientes que a aplicação em* a/b, *mas os restos são* k *vezes maiores.*

ii). Comprove isto no caso de $a/b = 87/250$ *e* $a'/b' = 348/1000$.

Exercício 99 -

Prove que ambos os métodos acima, quando aplicados a um número racional equivalente a uma fração decimal, produzem uma mesma expansão decimal, e esta sempre é terminante, ou seja: os dois resultados são uma mesma lista finita de dígitos.

Formalização do método das divisões:

Vamos nos concentrar no caso que no momento nos interessa, que é o dos racionais dados por uma fração a/b equivalente a uma fração decimal, e onde $0 < a < b$.

– Casa dos décimos:
fazendo uma primeira divisão euclidiana:

$$\frac{a}{b} = \frac{10 \times a}{10 \times b} = \frac{1}{10}\frac{q_1 \times b + r_1}{b} = \frac{q_1}{10} + \frac{r_1}{10 \times b},$$

onde $0 \leqslant r_1 < b$.
Como $0 < 10 \times a < 10 \times b$ pode ser escrito como $0 < q_1 \times b + r_1 < 10 \times b$, e como $r_1 \geqslant 0$, segue que $0 \leqslant q_1 \leqslant 9$. Por outro lado, $0 \leqslant r_1 < b$ dá $0 \leqslant r_1/(10 \times b) < 1/10$, e então segue que em a/b cabem apenas q_1 décimos.
Resumindo:

$$\frac{a}{b} = \frac{q_1}{10} + \frac{r_1}{10 \times b}, \quad 0 \leqslant \frac{r_1}{10 \times b} < \frac{1}{10}.$$

Logo, se $r_1 = 0$, temos a expansão $a/b = q_1/10$. Se $r_1 \neq 0$, precisamos ir para a próxima casa.

– Casa dos centésimos:
supondo, então, $0 < r_1 < b$, fazemos uma segunda divisão euclidiana:

$$\frac{r_1}{10 \times b} = \frac{10 \times r_1}{100 \times b} = \frac{1}{100}\frac{q_2 \times b + r_2}{b} = \frac{q_2}{100} + \frac{r_2}{100 \times b},$$

onde $0 \leqslant r_2 < b$.
Como $0 < 10 \times r_1 < 10 \times b$ pode ser escrito como $0 < q_2 \times b + r_2 < 10 \times b$, e como $r_2 \geqslant 0$, segue que $0 \leqslant q_2 \leqslant 9$. Por outro lado, $0 \leqslant r_2 < b$ dá $0 \leqslant r_2/(100 \times b) < 1/100$, e então segue que em a/b cabem apenas q_2 centésimos.
Resumindo:

$$\frac{a}{b} = \frac{q_1}{10} + \frac{q_2}{100} + \frac{r_2}{100 \times b}, \quad 0 \leqslant \frac{r_2}{100 \times b} < \frac{1}{100}.$$

Logo, se $r_2 = 0$, temos a expansão $a/b = q_1/10 + q_2/100$. Se $r_2 \neq 0$, precisamos ir para a próxima casa.

– Casa dos milésimos:
supondo, então, $0 < r_2 < b$, fazemos uma terceira divisão euclidiana:

$$\frac{r_2}{100 \times b} = \frac{1}{1000}\frac{10 \times r_2}{b} = \frac{1}{1000}\frac{q_3 \times b + r_3}{b} = \frac{q_3}{1000} + \frac{r_3}{1000 \times b}$$

onde $0 \leqslant r_3 < b$.
Como $0 < 10 \times r_2 < 10b$ pode ser escrito como $0 < q_3 \times b + r_3 < 10 \times b$, e como $r_3 \geqslant 0$, segue que $0 \leqslant q_3 \leqslant 9$. Por outro lado, $0 \leqslant r_3 < b$ dá $0 \leqslant r_3/(1000 \times b) < 1/1000$, e então, segue que em a/b cabem apenas q_3 milésimos.
Resumindo:

$$\frac{a}{b} = \frac{q_1}{10} + \frac{q_2}{100} + \frac{q_3}{1000} + \frac{r_3}{1000 \times b}, \quad 0 \leqslant \frac{r_3}{1000 \times b} < \frac{1}{1000}.$$

Logo, se $r_3 = 0$, temos a expansão $a/b = q_1/10 + q_2/100$. Se $r_2 \neq 0$, precisamos ir para a próxima casa.

Enquanto encontrarmos restos não nulos, continuaremos semelhantemente este processo. Ou seja, tendo sido determinado o dígito da k-ésima casa depois da vírgula, se tivermos $0 < r_k/(10^k \times b) < 1/10^k$, passamos a determinar o dígito da $(k+1)$-ésima casa; para isso, fazemos uma nova divisão euclidiana, para ver qual o maior múltiplo de $1/10^{k+1}$ que cabe em $r_k/(10^k \times b)$.

Resumo: para gerar uma expansão decimal $a/b = 0, q_1 q_2 q_3 \ldots$ de um racional $0 < a/b < 1$, o método das divisões consiste em fazer sucessivas divisões euclidianas:

$$\begin{aligned} 10 \times a &= q_1 \times b + r_1, \quad \text{com } 0 \leqslant r_1 < b \\ 10 \times r_1 &= q_2 \times b + r_2, \quad \text{com } 0 \leqslant r_2 < b \\ 10 \times r_2 &= q_3 \times b + r_3, \quad \text{com } 0 \leqslant r_3 < b \\ &\ldots \end{aligned}$$

até chegar ao primeiro resto nulo.

– O caso das frações ordinárias não equivalentes a uma fração decimal

Para este caso, temos dois fatos fundamentais. O primeiro é imediata consequência do que já vimos e o segundo constituirá o teorema a seguir.

- Fato 1:
  a expansão decimal dos números racionais não equivalentes a uma fração decimal é não terminante: contém infinitos dígitos
- Fato 2:
  apesar disso, podemos obter a expansão decimal de tais racionais pelo método das divisões. Com efeito, há uma clara regularidade nesta infinitude de dígitos: a partir de uma certa casa, aparece um *primeiro* e *menor* bloco de dígitos (que chamaremos período da expansão) tal que, a partir dele, a lista dos dígitos consiste exclusivamente na repetição sucessiva de tal bloco.
  Dizemos que trata-se de uma expansão decimal periódica.

Teorema 4.20 -

Todo racional não equivalente a uma fração decimal tem uma expansão decimal infinita periódica.

Prova:

Como a informação mencionada refere-se tão somente à parte depois da vírgula, vamos nos concentrar no caso de um racional $0 < r = a/b < 1$.
Como a expansão decimal deste a/b não pode ser terminante, teremos, na notação usada na formalização do método das divisões:

$$0 < r_1, r_2, r_3, \ldots < b, \quad \text{ou seja:} \quad 0 < r_1, r_2, r_3, \ldots \leqslant b-1\,.$$

Assim – no máximo, após as primeiras $b-1$ divisões – veremos um resto r_j repetindo o valor de um resto r_i já obtido $(1 \leqslant i < j)$. Isso implica que a expansão de a/b terá de ter a forma:

$$\frac{a}{b} = 0, q_1 q_2 \ldots q_i q_{i+1} \ldots q_j q_i q_{i+1} \ldots q_j \ldots\ .$$

Vale a pena exemplificar. Se $r_3 = r_1$, teremos:

```
a=r0 --> q1
  r1 --> q2
  r2 --> q3
  r3 --> q2
  r4 --> q3
  r5 --> q2
     etc.
```

de modo que a expansão fica:

$$\frac{a}{b} = 0, q_1 q_2 q_3 q_2 q_3 \ldots = \frac{q_1}{10} + \frac{q_2}{100} + \frac{q_3}{1000} + \frac{q_2}{10\,000} + \frac{q_3}{100\,000} + \cdots ,$$

onde a reticência indica repetição do padrão. CQD.

> O método das divisões se aplica tanto no caso de números racionais equivalentes a fração decimal, como no de não equivalentes:
>
> - no caso de fração equivalente a decimal, paramos quando acharmos o primeiro resto nulo;
> - no caso de fração não equivalente a decimal, paramos quando houver a primeira repetição de resto.

Exemplo 4.21 -

Determinar a representação decimal de $17/37$.

Antes de mais nada, observemos que esta fração é irredutível, mas não é equivalente a nenhuma fração decimal, uma vez que a fatoração em primos de 37 *não é do tipo* $2^m \times 5^n$. *Consequentemente, sua expansão decimal será infinita periódica. Para achar tal expansão, pelo que vimos anteriormente, tudo o que temos de fazer é aplicar o método das divisões até encontrarmos uma primeira repetição de resto.*

– Casa dos décimos:
quantos décimos existem no racional $17/37$? *Observemos que*

$$\frac{17}{37} = \frac{1}{10} \times \frac{170}{37} = \frac{1}{10} \times \frac{4 \times 37 + 22}{37} = \frac{4}{10} + \frac{22}{370} ,$$

e que cabem apenas 4 *décimos em* $17/37$, *pois* $0 < 22 < 37$ *dá* $0 < 22/370 < 1/10$. *Portanto, a expansão até a casa dos décimos é*

$$\frac{17}{37} = \frac{4}{10} + \frac{22}{370} = 0,4 + \frac{22}{370} ,$$

sendo que, por enquanto, temos um único resto: $r_1 = 22$.

– Casa dos centésimos:
determinamos quantos centésimos cabem em $22/370$, *observando que*

$$\frac{22}{370} = \frac{1}{100} \times \frac{220}{37} = \frac{1}{100} \times \frac{5 \times 37 + 35}{37} = \frac{5}{100} + \frac{35}{3700} ,$$

e que cabem apenas 5 *centésimos em* 22/370*, pois* $0 < 35 < 37$ *dá* $0 < 35/3700 < 1/100$*. Portanto, a expansão até a casa dos centésimos é*

$$\frac{17}{37} = \frac{4}{10} + \frac{5}{100} + \frac{35}{3700}\,,$$

ou ainda:

$$\frac{17}{37} = 0,45 + \frac{35}{3700}\,.$$

– Casa dos milésimos:
por enquanto, a lista dos restos é: $r_1 = 22$ *e* $r_2 = 35$*; como ela não tem repetição, precisamos continuar, determinando quantos milésimos cabem em* 35/3700*. Observemos que*

$$\frac{35}{3700} = \frac{1}{1000} \times \frac{350}{37} = \frac{1}{1000} \times \frac{9 \times 37 + 17}{37} = \frac{9}{1000} + \frac{17}{37000}\,,$$

e que cabem apenas 9 *milésimos em* 35/3700*, pois* $0 < 17 < 37$ *nos permite escrever* $0 < 17/3700 < 1/1000$*. Portanto, a expansão até a casa dos milésimos é*

$$\frac{17}{37} = 0,45 + \frac{35}{3700} = 0,45 + \frac{9}{1000} + \frac{17}{37000} = 0,459 + \frac{17}{37000}\,.$$

– Casa dos décimos de milésimos:
por enquanto, a lista dos restos é: $r_1 = 22$, $r_2 = 35$ *e* $r_3 = 17$*; como ela não tem repetição, precisamos continuar, determinando quantos décimos de milésimos cabem em* 17/37 000*. Observando que*

$$\frac{17}{37\,000} = \frac{1}{10\,000} \times \frac{170}{37} = \frac{1}{10\,000} \times \frac{4 \times 37 + 22}{37}\,,$$

vemos que podemos parar[2]*, pois temos uma repetição de restos:* $r_4 = 22 = r_1$*. Consequentemente, a expansão é periódica e se escreve:*

$$\begin{aligned}\frac{17}{37} &= 0,\,459\,459\,459\ldots\\ &= \frac{4}{10} + \frac{5}{100} + \frac{9}{1\,000} + \frac{4}{10\,000} + \frac{5}{100\,000} + \frac{9}{1\,000\,000} + \\ &+ \frac{4}{10\,000\,000} + \frac{5}{100\,000\,000} + \frac{9}{1\,000\,000\,000} + \cdots\,.\end{aligned}$$

[2]O leitor atento deve ter observado que nem era necessário fazer essa última divisão, pois ela já havia sido feita na casa dos décimos.

Exercício 100 -

Ver como ocorre o processo de repetição de restos, e então de dígitos, no procedimento de divisão abreviada que se aprende no Ensino Fundamental. (*Para tal, faça uma análise semelhante à que fizemos na Observação 4.19*).
Sugestões: estude os casos $r = 1/9 = 0,111\,111\,111\ldots$, $r = 2/27 = 0,074\,074\ldots$ *e* $r = 7/12 = 0,5833333\ldots$. *Em cada um deles, inicie provando que a expansão tem de ser não terminante.*

Exercício 101 -

Comprove a validade da expansão decimal $1/7 = 0,184457\,184457\ldots$.
Podemos usar este exemplo para concluir que:

- *numa fração irredutível* a/b, *realmente pode ocorrer que o tamanho do bloco repetitivo seja o maior possível, ou seja: igual a* $b-1$;
- *quem determina o início da repetição periódica dos dígitos de uma expansão decimal é a primeira coincidência de restos das divisões, e não a primeira repetição de dígitos na expansão.*

Observação 4.22 -

Já sabemos que, se um racional a/b (*com* a *e* b *relativamente primos*) *tiver uma expansão decimal periódica, o bloco de repetição pode ter tamanho de até* $b-1$ *dígitos. Em particular, pode ser grande, desde que* b *também seja. Assim, pede-se achar o bloco repetitivo na expansão seguinte:*

$$\frac{1}{17} = 0,05882352941176470588235294117647058823529411764705\ldots \ .$$

Uma consequência prática deste fato é o cuidado que devemos ter quando tentamos descobrir o bloco repetitivo usando calculadoras eletrônicas. Assim, usando calculadora, obtemos $1/81 = 0,012345679$ *o que poderia nos levar a conjecturar que temos um bloco repetitivo* 0123456789, *o qual foi arredondado pela calculadora como* 012345679. *Contudo, um cálculo à mão produz*

$$\frac{1}{81} = 0,012345679012345679012345679012345679\ldots \ .$$

Exercício 102 -

É possível aplicar o método das divisões no caso $301/300$?

4.4 Elucidando as dízimas geradas por números racionais

Terminologia:

Já sabemos que todo número racional tem uma expansão decimal da forma:

$$r = \pm a_m \dots a_1 a_0 , b_1 b_2 b_3 \dots ,$$

onde cada a_k e cada b_k são um dígito. Tradicionalmente, emprega-se a denominação dízima para denotar listas de dígitos desta forma.

Para tornar mais leve a leitura do que se segue, diremos que um bloco finito de dígitos $d_1 d_2 \dots d_k$ é 9-repetido, se tivermos $d_1 = d_2 = \dots = d_k = 9$.

É importante lembrarmos que já sabemos que:

- os números racionais equivalentes a uma fração decimal são precisamente os que têm uma expansão decimal finita, ou dízima finita:

$$r = \pm a_m \dots a_1 a_0 , b_1 b_2 b_3 \dots b_n ;$$

- os demais números racionais têm uma expansão decimal infinita, mas periódica, ou seja:
  - ou uma dízima periódica simples:

$$\begin{aligned} &\text{ou } r = \pm\, a_m \dots a_1 a_0 , b_1 b_1 b_1 \dots \\ &\text{ou } r = \pm\, a_m \dots a_1 a_0 , b_1 b_2 b_1 b_2 \dots \\ &\text{ou } r = \pm\, a_m \dots a_1 a_0 , b_1 b_2 b_3 b_1 b_2 b_3 \dots \\ &\qquad \text{etc.,} \end{aligned}$$

  - ou uma dízima periódica composta:

$$\begin{aligned} &\text{ou } r = \pm\, a_m \dots a_1 a_0 , b_1 b_2 \dots b_n c_1 c_1 c_1 \dots \\ &\text{ou } r = \pm\, a_m \dots a_1 a_0 , b_1 b_2 \dots b_n c_1 c_2 c_1 c_2 \dots \\ &\text{ou } r = \pm\, a_m \dots a_1 a_0 , b_1 b_2 \dots b_n c_1 c_2 c_3 c_1 c_2 c_3 \dots \\ &\qquad \text{etc.} \end{aligned}$$

Notação:

Está se fazendo necessária uma notação que torne mais precisa e mais abreviada a escritura das expansões decimais periódicas. Para isto, foram inventadas várias notações. Aqui no Brasil, costuma-se empregar um vinculum para fazer tal abreviação. Isto consiste em usarmos uma barra sobre todo bloco que se repete sucessivamente:

Exemplo 4.23 -

Para indicarmos que em $0,444\ldots$ *o 4 se repete indefinidamente, escrevemos* $0,\overline{4}$.

Note que $0,23\overline{8} = 0,23\overline{88} = 0,23\overline{888} = 0,23\overline{8888} = \ldots = 0,238\,888\,888\ldots$.

A expansão $-0,235747474\ldots$*, onde o bloco 74 se repete "sem parar", pode ser escrita como* $-0,235\overline{74}$*, como* $-0,235\overline{7474}$ *e também como* $-0,2357\overline{47}$*.*

Outra notação – usada principalmente em países europeus e alguns asiáticos – consiste em envolver o bloco repetitivo com parêntesis, assim tendo-se, por exemplo: $0,235747474\ldots = 0,235\overline{74} = 0,235(74)$.

Com esta notação, podemos caracterizar mais precisamente:

- as expansões decimais periódicas simples, ou dízimas periódicas simples, como:

$$\pm a_m \ldots a_1 a_0, \overline{b_1 b_2 \ldots b_n}\,,$$

  tendo-se que todos os a_i e b_j são dígitos;
- as expansões decimais periódicas compostas, ou dízimas periódicas compostas, como:

$$\pm a_m \ldots a_1 a_0, b_1 b_2 \ldots b_n \overline{c_1 c_2 \ldots c_p}\,,$$

  tendo-se que todos os a_i, b_j e c_k são dígitos, e que os b_j são tais que a expansão não pode ser vista como simples.

Exemplo 4.24 -

Uma dízima periódica simples é $5,\overline{12}$*, enquanto que* $0,235\overline{74}$ *é um exemplo de dízima composta.*

Definição 4.25 -

Chamamos de período *de uma dízima periódica o primeiro*[3] *e menor bloco de dígitos que, repetindo-se sucessivamente, gera o restante da dízima.*

[3] Lendo do primeiro dígito depois da vírgula para a direita.

Exemplo 4.26 -

Em $5,121212\ldots$ *, o bloco* 1212 *se repete sucessivamente, mas o período é* 12*; enquanto que em* $0,235\overline{74}$*, o período é* 74*.*

No caso das dízimas simples, o bloco $b_1b_2\ldots b_n$ é o período, desde que não possa ser "encurtado". No caso das dízimas compostas, $\pm a_m\ldots a_1a_0, b_1b_2\ldots b_n\overline{c_1c_2\ldots c_p}$, além de nos preocuparmos com o tamanho do bloco, temos de verificar se não existe um bloco repetitivo iniciando em algum b_k. Ou seja, temos de verificar se o "candidato" a período é realmente o primeiro e menor bloco repetitivo. Com efeito, observe que $0,1424242\cdots = 0,1\overline{42} = 0,14\overline{24}$, mas o período é 42.

Exercício 103 -

Mostre que numa dízima composta $\pm a_m\ldots a_1a_0, b_1b_2\ldots b_n\overline{c_1c_2\ldots c_p}$*, se tivermos* $b_n = c_p$*, então* $c_1c_2\ldots c_p$ *não é o período.*

Observando que

$$\frac{b_1}{10}+\frac{b_2}{10^2}+\cdots+\frac{b_n}{10^n}=\frac{b_1}{10}+\frac{b_2}{10^2}+\cdots+\frac{b_n}{10^n}+\frac{0}{10^{n+1}}+\frac{0}{10^{n+2}}+\cdots,$$

escreveremos:

$$\pm a_m\ldots a_1a_0,\, b_1b_2\ldots b_n = \pm a_m\ldots a_1a_0,\, b_1b_2\ldots b_n00\ldots\ ,$$

de modo que podemos dizer que

> *toda expansão decimal finita pode ser vista como uma expansão decimal infinita de período* 0 *(zero). Exemplos:*
> $1/2 = 0,5 = 0,5000\ldots = 0,5\overline{0}$ e
> $-234/100 = -2,34 = -2,34000\ldots = -2,34\overline{0}$.

Com essa observação, podemos resumir de uma maneira bem simples e direta o que já conhecemos sobre a expansão decimal dos números racionais:

Teorema 4.27 -

Todo racional tem como expansão decimal uma dízima periódica (talvez de período zero).

> *Uma consequência deste teorema é que dízimas não periódicas, como é o caso de* $0,10100100010000\ldots$ *, simplesmente não têm sentido no contexto dos números racionais. Assim, o estudo dos números racionais limita-se ao estudo das expansões periódicas.*

Nesse sentido, uma próxima questão que se impõe é a seguinte:

> *será verdade que, para* qualquer *período que imaginemos, sempre existirá algum número racional cuja expansão decimal (pelo método das divisões) tem tal período?*

O teorema seguinte diz que a resposta é negativa.

Teorema 4.28 -

O método das divisões nunca gera uma expansão decimal cujo período é formado somente por 9's.

Prova:

A prova é por absurdo e basta considerar os casos $0 < a/b < 1$. Ademais, a fim de que o leitor não se distraia com a pesada notação, vamos considerar um caso particular significativo, deixando a prova do caso geral como um exercício posterior. Assim, suponhamos que o método das divisões tenha produzido, por exemplo:

$$a/b = 0, q_1 q_2 999\ldots = 0, q_1 q_2 \overline{9},$$

e mostremos que isso produz um absurdo.
Iniciemos observando que as três etapas iniciais do método das divisões produzem os seguintes resultados:

$$\begin{aligned} 10 \times a &= q_1 \times b + r_1, \quad \text{com } 0 \leqslant r_1 < b \\ 10 \times r_1 &= q_2 \times b + r_2, \quad \text{com } 0 \leqslant r_2 < b \\ 10 \times r_2 &= 9 \times b + r_3, \quad \text{com } 0 \leqslant r_3 < b. \end{aligned}$$

A partir deste ponto, as divisões seguintes têm a forma $10 \times r_n = 9 \times b + r_{n+1}$, sendo que todos os restos verificam $0 \leqslant r_{n+1} < b$. Consequentemente, cedo ou tarde, teremos uma repetição, digamos, $r_4 = r_7$. Isso significa que teremos:

$$\begin{array}{ll} 10 \times r_2 = 9 \times b + r_3, & \text{com } 0 \leqslant r_3 < b\,, \\ 10 \times r_3 = 9 \times b + r_4, & \text{com } 0 \leqslant r_4 < b\,, \\ 10 \times r_4 = 9 \times b + r_5, & \text{com } 0 \leqslant r_5 < b\,, \\ 10 \times r_5 = 9 \times b + r_6, & \text{com } 0 \leqslant r_6 < b\,, \\ 10 \times r_6 = 9 \times b + r_4, & \text{com } 0 \leqslant r_4 < b\,. \end{array}$$

Ora, somando as igualdades envolvendo $10 \times r_4$, $10 \times r_5$ e $10 \times r_6$, obtemos:

$$10 \times (r_4 + r_5 + r_6) = 3 \times 9 \times b + (r_5 + r_6 + r_4),$$

de modo que, simplificando:

$$9 \times (r_4 + r_5 + r_6) = 3 \times 9 \times b,$$

de onde tiramos $r_4 + r_5 + r_6 = 3 \times b$; o que é uma impossibilidade frente a $0 \leqslant r_4, r_5, r_6 < b$.

CQD.

Exemplo 4.29 -

Pelo teorema, o método das divisões não pode produzir expansões como:
$0,999\ldots = 0,\overline{9}$
$0,4999\ldots = 0,4\overline{9}$.

Exercício 104 -

Onde o raciocínio acima falha quando tentamos adaptá-lo para provar a impossibilidade de uma expansão tipo $0,q_1q_2\overline{8}$ *?*

Exercício 105 -

Escrever a demonstração do teorema acima no caso $0,q_1q_2\ldots q_n\overline{9}$.

A elucidação das dízimas de números racionais iniciou por cerca de 1 700. Após o surgimento de algumas regras empíricas, vários grandes matemáticos daquele século, tais como J. H. Lambert, L. Euler e L. Lagrange, iniciaram a construção de uma teoria sistemática para as dízimas periódicas.

Mas o maior expoente que se dedicou ao assunto foi K. F. Gauss. Em 1 801, Gauss publicou um dos livros mais importantes já escritos sobre Matemática, o Disquisitiones Arithmeticae (Investigações de Aritmética). No sexto capítulo deste livro, Gauss estuda as dízimas periódicas. Para tal, introduziu noções hoje fundamentais para muitos campos matemáticos: a ideia de congruências modulares de números inteiros e sua aritmética.

Seu ponto de partida foi a observação que toda fração ordinária pode ser decomposta como uma soma de frações simples, ou seja, de frações cujo denominador é primo, ou potência de número primo. Por exemplo:

$$\frac{251}{351} = \frac{11}{3^3} + \frac{4}{13}.$$

A partir daí, ele usa a aritmética modular para calcular o período de cada uma dessas parcelas, e então a expansão decimal de cada uma delas. Somando-as, ele obtém a dízima da fração original. No caso de nosso exemplo:

$$\frac{11}{27} = 0,\overline{407},\ \frac{4}{13} = 0,\overline{307692} \Rightarrow \frac{251}{351} = 0,\overline{407407} + 0,\overline{307692} = 0,\overline{715099}.$$

Os resultados de Gauss e muitos outros sobre propriedades das dízimas periódicas são tratados em cursos de Aritmética, e têm inúmeras aplicações (fatoração de inteiros, provas de irracionalidade de números reais, cálculo rápido com frações, etc.).

Exercício 106 -

Dentre os racionais da forma $1/n$, o primeiro que tem um período maior do que a capacidade do visor das calculadoras eletrônicas é $1/17$. Contudo, podemos usar artifícios para calculá-lo. Nesse sentido, observe as seguintes divisões euclidianas:

$$\begin{aligned} 10^7 &= 17 \times 588235 + 5 \\ 5 \times 10^7 &= 17 \times 2941176 + 8 \\ 8 \times 10^2 &= 17 \times 47 + 1. \end{aligned}$$

Observando que o último resto obtido foi 1, pede-se explicar por que esses cálculos nos permitem afirmar que:

$$\frac{1}{17} = 0,\overline{058\,823\,529\,411\,7647}.$$

Resumo:

Para gerar uma expansão decimal $a/b = 0,q_1q_2q_3\dots$ de um racional $0 < a/b < 1$, o método das divisões faz sucessivas divisões euclidianas:

$$\begin{aligned} 10 \times a &= q_1 \times b + r_1, \quad \text{com } 0 \leqslant r_1 < b\,, \\ 10 \times r_1 &= q_2 \times b + r_2, \quad \text{com } 0 \leqslant r_2 < b\,, \\ 10 \times r_2 &= q_3 \times b + r_3, \quad \text{com } 0 \leqslant r_3 < b\,, \\ &\dots \end{aligned}$$

tendo-se que:

- se a/b for equivalente a uma fração decimal, obteremos uma expansão da forma:

  $$a/b = 0,q_1q_2\dots q_n = 0,\, b_1b_2\dots b_n = 0,\, b_1b_2\dots b_n000\dots\,,$$

  onde n é o primeiro valor de k dando $r_k = 0$;

- se a/b não for equivalente a uma fração decimal, o processo de divisões sucessivas nunca terminará (todos os restos $r_k \neq 0$), mas os dígitos, cedo ou tarde, passarão a se repetir em bloco, resultando
  - ou uma expansão periódica simples:

    $$a/b = 0,\, \overline{q_1q_2\dots q_n} = 0,\, \overline{b_1b_2\dots b_n}\,;$$

  - ou uma expansão periódica composta:

    $$a/b = 0,\, q_1q_2\dots q_n\overline{q_{n+1}q_{n+2}\dots q_{n+p}} = 0,\, b_1b_2\dots b_n\overline{c_1c_2\dots c_p}\,.$$

4.5 Recuperação de dízimas

Terminologia:

Por geratriz de uma dízima entendemos o número racional, se houver, cuja expansão decimal produz tal dízima.

O problema a resolver:

Dada uma lista de dígitos da forma $\pm a_n \ldots a_1 a_0, b_1 b_2 b_3 \ldots$ (ou seja: dada uma dízima), queremos saber se ela é a expansão decimal (pelo método das divisões) de algum número racional e, caso seja, desejamos encontrar uma representação em fração ordinária para tal racional.

Pelo que já sabemos sobre a expansão decimal de números racionais:

- devemos nos restringir às dízimas finitas e às periódicas;
- devemos descartar as periódicas de período 9-repetido.

– Conversão de dízima finita em fração ordinária

Já sabemos que uma dízima desse tipo é a expansão de um número racional equivalente a uma fração decimal, fração esta que é obtida somando-se as parcelas envolvidas na expansão:

$$0, b_1 b_2 \ldots b_n = \frac{b_1}{10} + \cdots + \frac{b_n}{10^n} = \frac{b_1 \times 10^{n-1} + b_2 \times 10^{n-2} + \cdots + b_n}{10^n}\,.$$

– Conversão de dízima periódica simples em fração ordinária

Proposição 4.30 -

Se $b_1 b_2 \ldots b_n$ é um bloco de dígitos não 9-repetido, o método das divisões produz a expansão decimal:

$$\frac{b_1 b_2 \ldots b_n}{\underbrace{99\ldots9}_{n}} = 0, \overline{b_1 b_2 \ldots b_n}\,.$$

Ou seja, explicitando para $n = 1, 2, 3, \ldots$:

$$\frac{b_1}{9} = 0, \overline{b_1} = 0, b_1 b_1 b_1 \ldots$$

$$\frac{b_1 b_2}{99} = 0, \overline{b_1 b_2} = 0, b_1 b_2 b_1 b_2 \ldots$$

$$\frac{b_1 b_2 b_3}{999} = 0, \overline{b_1 b_2 b_3} = 0, b_1 b_2 b_3 b_1 b_2 b_3 \ldots$$

$$\ldots$$

Prova:

Para que o leitor não tenha sua atenção distraída pela notação, tomemos um caso particular significativo: o do bloco $b_1 b_2 b_3 \neq 999$. [4] Passando às sucessivas divisões euclidianas de $a = b_1 b_2 b_3$ por $b = 999$, e atentando aos respectivos restos:

– escrevendo $10 \times a = 10 \times b_1 b_2 b_3 = 999 \times b_1 + r_1$, então:

$$\begin{aligned} r_1 &= 10 \times b_1 b_2 b_3 - 999 \times b_1 \\ &= 10(100 \times b_1 + 10 \times b_2 + b_3) - 999 \times b_1 \\ &= b_1 + 100 \times b_2 + 10 \times b_3 = b_2 b_3 b_1 < 999, \quad \text{logo, } r_1 \text{ é resto;} \end{aligned}$$

– escrevendo $10 \times r_1 = 999 \times b_2 + r_2$, então:

$$\begin{aligned} r_2 &= 10 \times r_1 - 999 \times b_2 = 10 \times b_2 b_3 b_1 - 999 \times b_2 \\ &= 10(100 \times b_2 + 10 \times b_3 + b_1) - 999 \times b_2 \\ &= b_2 + 100 \times b_3 + 10 \times b_1 = b_3 b_1 b_2 < 999, \quad \text{logo, } r_2 \text{ é resto;} \end{aligned}$$

– escrevendo $10 \times r_2 = 999 \times b_3 + r_3$, então:

$$\begin{aligned} r_3 &= 10 \times r_2 - 999 \times b_3 = 10 \times b_3 b_1 b_2 - 999 \times b_3 \\ &= 10(100 \times b_3 + 10 \times b_1 + b_2) - 999 \times b_3 \\ &= b_3 + 100 \times b_1 + 10 \times b_2 = b_1 b_2 b_3 < 999, \quad \text{logo, } r_3 \text{ é resto.} \end{aligned}$$

Observemos agora que encontramos uma repetição de restos: $r_3 = r_0 = a = b_1 b_2 b_3$. Isto significa que temos uma repetição cíclica dos restos produzidos pelo método, neste caso:

$$r_0 = a = b_1 b_2 b_3 \to r_1 = b_3 b_1 b_2 \to r_2 = b_2 b_3 b_1 \to r_3 = b_1 b_2 b_3 \to \ldots$$

[4] Note que essa hipótese implica que também valem $b_1 b_2 b_3 < 999$, $b_3 b_1 b_2 < 999$ e $b_2 b_3 b_1 < 999$, as quais serão usadas a seguir.

o que provoca o seguinte sequencionamento dos dígitos:

$$b_1 \to b_2 \to b_3 \to b_1 \to b_2 \to b_3 \to b_1 \dots$$

ou seja, temos a expansão decimal:

$$\frac{b_1b_2b_3}{999} = 0,\overline{b_1b_2b_3} = 0,b_1b_2b_3b_1b_2b_3\dots\ .$$

CQD.

Exercício 107 -

i). Refazer o raciocínio da prova da proposição anterior no caso concreto $234/999$, *observando a permutação cíclica dos dígitos dos restos e, assim, a repetição periódica dos dígitos da expansão.*

ii). Escrever a prova da proposição anterior no caso $b_1b_2/99$.

iii). Escrever a prova da proposição anterior no caso geral $b_1b_2\dots b_n/99\dots 9$.

Tratemos agora da recíproca: será que toda lista de dígitos, infinita e periódica de período não formado só por 9's, é a expansão decimal de algum número racional?

Teorema 4.31 -

Toda dízima periódica simples $0,\overline{b_1b_2\ \dots\ b_n}$ *, onde o bloco* $b_1b_2\ \dots\ b_n$ *não é 9-repetido, é a expansão decimal, obtida pelo método das divisões, de exatamente um número racional* $0 < r < 1$*. Ademais, este racional é dado pela fração ordinária:*

$$r = \frac{b_1b_2\dots b_n}{\underbrace{99\dots 9}_{n}}\,,$$

ou seja,

$$r = \frac{b_1b_2\dots b_n}{10^n - 1}\,.$$

O que podemos resumir como:

$$\boxed{0,\overline{b_1b_2\dots b_n} = \frac{b_1b_2\dots b_n}{\underbrace{99\dots 9}_{n}} = \frac{b_1b_2\dots b_n}{10^n - 1}\,.}$$

Exemplo 4.32 -

Antes de passarmos à prova desse teorema, exemplifiquemos o seu significado e a notação empregada.
Esse teorema nos garante que a dízima $0,121212\ldots$ *é proveniente de um número racional e que este racional é dado por*

$$\frac{12}{99} = \frac{4}{33}.$$

Confiramos diretamente. Como:

$$\begin{aligned} 40 &= 1 \times 33 + 7 \\ 70 &= 2 \times 33 + 4, \end{aligned}$$

segue que $r_1 = 7$, $r_2 = 4$, $r_3 = 7$, *e a expansão decimal de* $4/33$ *é, com efeito,* $0,121212\ldots.$

Prova do teorema:

Pela Proposição 4.30, já temos um número racional cuja expansão decimal é a dízima dada. Nos resta provar que somente ele serve, ou seja, que todo racional – cuja expansão decimal (pelo método das divisões) é a dízima dada – tem de ser equivalente à fração ordinária $b_1 b_2 \ldots b_n / 99 \ldots 9$.

Novamente, para que o leitor não tenha sua atenção distraída pela notação, tomemos um caso particular significativo: $r = a/b = 0,\overline{b_1 b_2 b_3}$. Ficará como exercício posterior provar o caso geral.

Suponhamos então que a dízima dada seja a expansão de um racional $0 < a/b < 1$. Isto significa que temos a seguinte sequência de igualdades:

$$\begin{aligned} 10 \times a &= b_1 \times b + r_1, \text{ com } 0 \leqslant r_1 < b \\ 10 \times r_1 &= b_2 \times b + r_2, \text{ com } 0 \leqslant r_2 < b \\ 10 \times r_2 &= b_3 \times b + r_3, \text{ com } 0 \leqslant r_3 < b \\ 10 \times r_3 &= b_1 \times b + r_4, \text{ com } 0 \leqslant r_4 < b \\ 10 \times r_4 &= b_2 \times b + r_5, \text{ com } 0 \leqslant r_5 < b \\ 10 \times r_5 &= b_3 \times b + r_6, \text{ com } 0 \leqslant r_6 < b \\ 10 \times r_6 &= b_1 \times b + r_7, \text{ com } 0 \leqslant r_7 < b \\ &\cdots \end{aligned}$$

Pela periodicidade, e o fato de que os restos têm de estar compreendidos entre 0 e b, segue que, cedo ou tarde, numa dessas igualdades voltará aparecer $b_1 \times b + r_1$. Por exemplo, suponhamos que isso ocorra quando $b_1 \times b + r_7 = b_1 \times b + r_1$. Ora, isto implica que $r_6 = a$ e, então:

$$\begin{aligned}
100 \times a &= 10 \times b_1 \times b + 10 \times r_1 = 10 \times b_1 + b_2 \times b + r_2 \\
&= b_1 b_2 \times b + r_2 \\
1000 \times a &= 100 \times b_1 \times b + 10 \times b_2 \times b + 10 \times r_2 = 100 \times b_1 \times b + 10 \times b_2 \times b + b_3 \times b + r_3 \\
&= b_1 b_2 b_3 \times b + r_3 \\
10\,000 \times a &= 1000 \times b_1 \times b + 100 \times b_2 \times b + 10 \times b_3 \times b + 10 \times r_3 \\
&= 1000 \times b_1 \times b + 100 \times b_2 \times b + 10 \times b_3 \times b + b_1 \times b + r_4 \\
&= b_1 b_2 b_3 b_1 \times b + r_4 \\
&\dots \\
1\,000\,000 \times a &= b_1 b_2 b_3 b_1 b_2 b_3 \times b + r_6 = b_1 b_2 b_3 b_1 b_2 b_3 \times b + a\,,
\end{aligned}$$

de modo que $999\,999 \times a = b_1 b_2 b_3 b_1 b_2 b_3 \times b$ e, então:

$$\frac{a}{b} = \frac{b_1 b_2 b_3 b_1 b_2 b_3}{999\,999} \overset{\text{exerc.}}{=} \frac{b_1 b_2 b_3}{999}\,. \quad \text{CQD.}$$

Exercício 108 -

i). Determine racional que tenha representação decimal igual a $0,\overline{123456}$, *expressando-o através de uma fração irredutível.*

ii). Determine racional que tenha representação decimal igual a $5,\overline{123456}$, *expressando-o através de uma fração irredutível.*

Exercício 109 -

i). Sendo b_1, b_2 *dígitos, prove que:*

$$\frac{b_1 b_2}{99} = \frac{b_1 b_2 b_1 b_2}{9999} = \frac{b_1 b_2 b_1 b_2 b_1 b_2}{999999} = \cdots\,.$$

Dica: inicie provando que $(10000 - 1) \times b_1 b_2 = (100 - 1) \times b_1 b_2 b_1 b_2$.

ii). Enuncie e prove a versão geral do resultado de (i): $b_1 b_2 \dots b_n / 99 \dots 9 =$ *etc.*

Exercício 110 -

i). Escrever a prova do teorema anterior no caso $n = 2$.

ii). Idem para o caso $n = 1$.

iii). Escrever a prova do teorema anterior no caso geral $n \geqslant 1$.

– Conversão de dízimas periódicas compostas em frações ordinárias

Exercício 111 -

Sejam dígitos $b_1, b_2, \ldots, b_n$, $c_1, c_2, \ldots, c_p$. *Pede-se provar:*

i). para $n = 2$ *e* $p = 3$*:*

$$\frac{b_1b_2}{100} + \frac{c_1c_2c_3}{99900} = \frac{b_1b_2c_1c_2c_3 - b_1b_2}{99900};$$

ii). para quaisquer $n \geqslant 1$ *e* $p \geqslant 1$*:*

$$\frac{b_1b_2\ldots b_n}{10^n} + \frac{c_1c_2\ldots c_p}{\underbrace{99\ldots9}_{p}\underbrace{0\ldots0}_{n}} = \frac{b_1\ldots b_nc_1c_2\ldots c_p - b_1\ldots b_n}{\underbrace{99\ldots9}_{p}\underbrace{0\ldots0}_{n}}.$$

Teorema 4.33 -

Toda dízima periódica composta

$$0, b_1b_2\ldots b_n\overline{c_1c_2\ldots c_p},$$

onde o bloco $c_1c_2\ldots c_p$ *não é 9-repetido, é a expansão decimal (obtida pelo método das divisões) de exatamente um número racional* $0 < r < 1$. *Ademais, este racional é dado pela fração ordinária:*

$$r = \frac{b_1b_2\ldots b_n}{10^n} + \frac{c_1c_2\ldots c_p}{\underbrace{99\ldots9}_{p}\underbrace{0\ldots0}_{n}}.$$

Ou equivalentemente,

$$r = \frac{b_1\ldots b_nc_1c_2\ldots c_p - b_1\ldots b_n}{\underbrace{99\ldots9}_{p}\underbrace{0\ldots0}_{n}}.$$

Podemos resumir isso como:

$$\boxed{0, b_1b_2\ldots b_n\overline{c_1c_2\ldots c_p} = \frac{b_1\ldots b_nc_1c_2\ldots c_p - b_1\ldots b_n}{\underbrace{99\ldots9}_{p}\underbrace{0\ldots0}_{n}}.}$$

O que também podemos resumir, repetindo a regra que aparece nos livros do Ensino Fundamental.

> Para recuperarmos a fração ordinária a partir da qual o método das divisões gera uma dízima da forma
>
> $$0, b_1 b_2 \dots b_n \overline{c_1 c_2 \dots c_p}$$
>
> (onde o bloco periódico não é 9-repetido), toma-se:
>
> - como numerador a diferença de dois inteiros, o primeiro formado pela parte não-periódica da expansão seguida do período, e o segundo formado pela parte não-periódica;
> - como denominador o inteiro formado de tantos 9's quantos são os dígitos do período, seguidos de tantos 0's quantos são os dígitos da parte não-periódica.

Prova:

A fim de que o leitor não seja distraído com a complicada notação, raciocinaremos com um caso particular significativo, $0,\ b_1 b_2 \overline{c_1 c_2 c_3}$, deixando o caso geral como um exercício posterior.

Novamente, o raciocínio terá duas partes: na parte inicial, mostraremos que, se a dízima dada for a expansão decimal (produzida pelo método das divisões) de um racional, então necessariamente este racional só pode ser dado pela fração ordinária do enunciado do teorema; na parte final do raciocínio, mostraremos que efetivamente essa fração ordinária tem a expansão decimal dada.

Primeira parte.
Supondo que a dízima dada tenha sido produzida fazendo a expansão de um racional $0 < a/b < 1$, teremos a seguinte sequência de igualdades:

$$\begin{aligned}
10 \times a &= b_1 \times b + r_1, \text{ com } 0 \leqslant r_1 < b \\
10 \times r_1 &= b_2 \times b + r_2, \text{ com } 0 \leqslant r_2 < b \\
10 \times r_2 &= c_1 \times b + r_3, \text{ com } 0 \leqslant r_3 < b \\
10 \times r_3 &= c_2 \times b + r_4, \text{ com } 0 \leqslant r_4 < b \\
10 \times r_4 &= c_3 \times b + r_5, \text{ com } 0 \leqslant r_5 < b \\
&\cdots
\end{aligned}$$

Para acharmos a/b, iniciamos multiplicando a primeira igualdade por 10, o que nos dá: $100 \times a = 10 \times b_1 \times b + 10 \times r_1 = (10 \times b_1 + b_2) \times b + r_2$, ou seja:

$$\frac{a}{b} = \frac{b_1 b_2}{100} + \frac{r_2}{100 \times b}.$$

Para determinar o valor da última parcela, basta observarmos que, a partir da terceira igualdade acima, temos uma situação análoga à que encontramos na prova do Teorema 4.31, de modo que seguramente podemos escrever:

$$\frac{r_2}{b} = \frac{c_1 c_2 c_3}{999},$$

e assim, finalmente:

$$\frac{a}{b} = \frac{b_1 b_2}{100} + \frac{r_2}{100 \times b} = \frac{b_1 b_2}{100} + \frac{c_1 c_2 c_3}{99900}.$$

Resta aplicarmos o Exercício 111, para concluirmos que:

$$r = \frac{b_1 b_2 c_1 c_2 c_3 - b_1 b_2}{99900}.$$

Segunda parte.
Verificaremos agora que, efetivamente, o candidato

$$\frac{a}{b} = \frac{b_1 b_2}{100} + \frac{c_1 c_2 c_3}{99900} = \frac{b_1 b_2}{100} + \frac{1}{100} \times \frac{c_1 c_2 c_3}{999}$$

acima tem como expansão decimal a dízima dada, $0, b_1 b_2 \overline{c_1 c_2 c_3}$.
Para isso, iniciamos observando que, como o bloco $c_1 c_2 c_3$ é suposto ser não 9-repetido, teremos

$$0 < \frac{1}{100} \times \frac{c_1 c_2 c_3}{999} < \frac{1}{100}.$$

Isso implica que a parcela $c_1 c_2 c_3/999$ só pode influenciar a expansão decimal de a/b a partir da casa dos milésimos. Esse fato e mais a igualdade $b_1 b_2/100 = b_1/10 + b_2/100$ determinam que, com certeza, a expansão decimal da fração a/b dada, até a casa dos centésimos, é $a/b = b_1/10 + b_2/100 + \dots$, sendo que os dígitos a partir da casa dos milésimos serão determinados apenas pela parcela $c_1 c_2 c_3/99900$.

Ora, da Proposição 4.30, sabemos que o método da divisão aplicado a $c_1 c_2 c_3/999$ gera uma sequência de dígitos que tem $c_1 c_2 c_3$ como período, e inicia na casa dos décimos. Consequentemente, esse método aplicado a $c_1 c_2 c_3/99900$ gera uma sequência de dígitos que tem $c_1 c_2 c_3$ como período, e inicia na casa dos milésimos. Podemos concluir afirmando que o método das divisões produz a expansão:

$$\frac{a}{b} = \frac{b_1 b_2}{100} + \frac{c_1 c_2 c_3}{99900} = 0,\ b_1 b_2 \overline{c_1 c_2 c_3}.$$

CQD.

Exemplo 4.34 -

Pelo teorema, temos que $0,58\overline{3} = 0,583333\ldots$ *é gerada pelo número racional*

$$r = \frac{583-58}{900} = \frac{525}{900} = \frac{105}{180} = \frac{21}{36} = \frac{7}{12}\,.$$

Confiramos diretamente. Como:

$$\begin{aligned} 70 &= 5 \times 12 + 10 \\ 100 &= 8 \times 12 + 4 \\ 40 &= 3 \times 12 + 4\,, \end{aligned}$$

segue que $r_1 = 10$, $r_2 = r_3 = \cdots = 4$, *e a expansão decimal de* r *é, com efeito,* $0,583333\ldots$ *.*

Exercício 112 -

i). Determine fração ordinária representando o racional cuja expansão decimal é igual a $0,12\overline{123456}$*. A seguir, expresse-o também por meio de fração irredutível.*

ii). Idem para $5,12\overline{123456}$*.*

Exercício 113 -

i). Aplique a regra anterior nos seguintes casos particulares: $0,00555$*,* $0,0004848$ *e* $0,00\overline{012}$ *.*

ii). Formule uma regra especial para os casos $0,00\ldots0\overline{c_1c_2\ldots c_p}$*.*

Exercício 114 -

i). Escrever a prova do Teorema 4.33 no caso $n = 2$*.*

ii). Idem para o caso $n = 1$*.*

iii). Idem para o caso geral $n \geqslant 1$*.*

Exercício 115 -

Para encontrar a geratriz de $0,3454545\ldots$ *, vamos observar que esta dízima pode ser escrita como* $0,3\overline{45}$ *, e como* $0,34\overline{54}$*. Pede-se aplicar a regra acima nos dois casos e verificar que determinam o mesmo racional. Essa conclusão vale em geral? Justifique.*

Exercício 116 -

Mostre que mesmo que forcemos a ver uma dízima simples como composta (exemplo: $0,\overline{4} = 0,4\overline{4}$*) e apliquemos o Teorema 4.33 para achar sua geratriz, a fração que se obtém é a correta. O que V. conclui disto?*

Exercício 117 -

Pesquise nos livros-texto de Ensino Fundamental e Médio como é feita a dedução da regra que converte uma dízima periódica em um número racional. A seguir, faça uma discussão, comparando a maneira vista aqui com a maneira exposta em tais livros. Em particular, deseja-se que o leitor atine que a maioria desses livros, visando a simplicidade, relega a um segundo plano o rigor matemático. Mais especificamente, deseja-se que o leitor aponte o ponto exato dessa falta de rigor matemático e, assim, entenda o porquê de nossas demonstrações mais complicadas.

4.6 Apreciação do que fizemos até aqui

– Pontos positivos

Vimos que todo número racional tem uma expansão decimal, e vimos também como determiná-la. Reciprocamente, vimos que toda dízima não 9-repetida é a expansão decimal de exatamente um número racional, e também vimos como calculá-la.

– Deficiências de nosso tratamento dos números racionais

- *Tratamos muito brevemente o significado das expansões decimais com infinitos dígitos.*
  Expansões como $1/3 = 0,333333\ldots$ foram introduzidas como meras expansões, nas quais o método das divisões fica produzindo dígitos sem cessar: não pára! Não exploramos que, por trás disso, está a possibilidade de produzirmos aproximações com quantidade finita de dígitos, mas de exatidão crescente. O uso prático dos números racionais por meio de suas expansões decimais – nas ciências, tecnologia e cotidiano – torna imperioso que estudemos a fundo a ideia de aproximação.
- *Não demos um caráter plenamente numérico às dízimas.*
  Embora tenhamos visto que elas sejam capazes de expressar quantidades (os números racionais que as geram), não lhe demos um carácter aritmético: não vimos como somá-las e multiplicá-las.

Problema de S. Stevin[5]:
substituir integralmente a aritmética das frações ordinárias pela aritmética das dízimas.

Este problema apresenta dificuldades técnicas e conceituais, não podendo se resumir na operação direta com as dízimas. Exemplifiquemos. A ideia intuitiva de considerar $0,1 + 0,2 = 0,3$ como a versão "soma de dízimas" de $1/10 + 2/10 = 3/10$, funciona perfeitamente. Poderíamos ficar encorajados de dizer que $0,111\ldots + 0,222\ldots = 0,333\ldots$ e nos entusiasmar ao verificar que $1/9 + 2/9 = 3/9 = 1/3 = 0,333\ldots$. Porém, não temos, ao menos ainda, como interpretar e compatibilizar:

$$0,111\ldots + 0,888\ldots = 0,999\ldots, \quad \text{versus} \quad \frac{1}{9} + \frac{8}{9} = \frac{9}{9} = 1.$$

Como associar naturalmente a dízima $0,999\ldots$, e as demais dízimas 9-repetidas, a números racionais?

A definição de multiplicação de dízimas é ainda mais difícil. Se ela é fácil para o caso de duas dízimas finitas, ela não é óbvia no caso das infinitas. Por exemplo, como definir e calcular: $0,555\ldots \times 0,888\ldots$?

– Deficiências do campo dos números racionais

Os números racionais estão muito longe de constituirem um campo numérico matematicamente satisfatório: existem muitos problemas que ficariam sem solução, se nos contentássemos com eles. Por enquanto, nos limitaremos a observar uma *insuficiência aritmética* do campo dos racionais, qual seja: sua incapacidade de atribuir um resultado à simples operação de extração de raízes quadradas. Vejamos.

Para qualquer tipo de número y que possamos multiplicar, entendemos por *raiz quadrada* de tal y um número x de mesmo tipo e que seja tal que $x^2 = x \times x = y$. Abreviamos isto escrevendo $x = \sqrt{y}$.

No caso dos números racionais, temos que $x \in \mathbb{Q} \Rightarrow x^2 \geqslant 0$, daí somente podemos esperar poder calcular a raiz quadrada de racionais positivos e do zero. Ainda mais importante é constatar a seguinte situação, no mínimo, deselegante:

[5] Foi Stevin que – por meio de seu livro La Disme, escrito cerca de 1 600 – divulgou no Mundo Cristão a aritmética das dízimas, já conhecida há séculos no Mundo Islâmico, India e China.

Alguns racionais positivos têm raiz quadrada e outros não!
Esta inconveniência já ocorre na lista dos inteiros positivos:

$$1, 2, 3, 4, 5, 6, \cdots \quad \Rightarrow \quad \sqrt{1} = 1\,,\ \sqrt{2} = ?\,,\ \sqrt{3} = ?\,,\ \sqrt{4} = 2\,,\ \sqrt{5} = ?\,, \cdots .$$

Provemos, por enquanto, apenas a primeira "insolubilidade" da lista acima. Ou seja, provemos que não existe nenhum número racional a/b cujo quadrado seja 2. Ou seja, que não existem inteiros positivos e relativamente primos, a e b, tais que:

$$a^2 = 2b^2.$$

Ora, do Teorema Fundamental da Aritmética é imediato que as fatorações em primos dos quadrados a^2 e b^2 só podem conter potências pares de primos. Assim, o fato de termos $a^2 = 2b^2$, nos levaria ao absurdo de termos que na fatoração de a^2 o primo 2 entra com potência ímpar.

Na verdade, o fato acima é muito mais do que deselegante, uma vez que o cálculo de raízes quadradas é uma operação extremamente comum em Matemática (uso do Teorema de Pythagoras, da fórmula de Bhaskara, etc.). Nos capítulos adiante, trabalharemos mais profunda e detalhadamente a questão das "insuficiências" aritméticas, bem como as insuficiências algébricas e geométricas do campo dos racionais.

– A saída: generalizar o conceito de número, indo aos números reais

A importância prática e teórica das frações e das expansões decimais mostram que seria um total absurdo pensarmos em abrir mão dos números racionais. Logo, para resolvermos as deficiências acima, só nos resta uma saída: adotar um ponto de vista mais geral, criar um campo numérico que inclua os racionais e seja mais satisfatório. Este campo será o dos números reais, assunto dos próximos capítulos.

Exercício 118 -

i). *Generalize o raciocínio acima para provar que* $\sqrt{p}$ *nunca pode ser racional, se* p *for primo.*

ii). *Mostre que o raciocínio acima não aborda todas as impossibilidades de resultado racional para* $\sqrt{y}$*, com* y *inteiro positivo. Ou seja, prove que, apesar de* 6 *não ser primo,* $\sqrt{6}$ *não pode ser racional.*

Exercício 119 -

Como um exemplo da utilidade de podermos considerar $0,999\ldots$ *como uma representação decimal legítima de* 1*, calcule* $1 - r$*, onde* $r = 0,5212121\ldots = 0,5\overline{21}$*. Para tal, escreva* $1 - r = 0,99999\ldots - 0,52121\ldots =$ *etc.*

4.7 Leitura complementar: elucidando as geratrizes

Veremos aqui alguns resultados que, a partir de informações sobre uma dízima, nos permitem concluir propriedades da fração ordinária irredutível que tem como expansão decimal tal dízima. Nos limitaremos aos resultados mais simples e, desde já, salientamos que os mesmos não serão utilizados nos capítulos posteriores.

Proposição 4.35 -

Uma fração irredutível que gera uma dízima (verdadeiramente) composta não pode ter numerador terminando com o dígito 0.

Prova:

Do Teorema 4.33, sabemos que

$$0, b_1 b_2 \dots b_n \overline{c_1 c_2 \dots . c_p} = \frac{b_1 \dots b_n c_1 c_2 \dots c_p - b_1 \dots b_n}{\underbrace{99 \dots 9}_{p}\underbrace{0 \dots 0}_{n}} .$$

Logo, para que o numerador da fração ordinária geratriz termine com o dígito 0, temos de ter $c_p = b_n$, o que contradiz estarmos tratando com uma dízima composta.

CQD.

Proposição 4.36 -

Para uma fração irredutível, se sua dízima é periódica simples, então seu denominador não pode ter nem 2 *e nem* 5 *como fator.*

Prova:

Do Teorema 4.31 temos que

$$0, \overline{b_1 b_2 \dots b_n} = \frac{b_1 b_2 \dots b_n}{\underbrace{99 \dots 9}_{n}} .$$

Como este denominador só contém dígitos 9, segue que é impossível o mesmo ter fator 2 ou 5, e isso mesmo depois de eventuais simplificações com o numerador visando chegar a uma fração irredutível.

CQD.

Proposição 4.37 -

Se uma fração irredutível tiver dízima periódica composta, então o denominador desta fração terá como fator ao menos um dentre 2 e 5, e este fator terá um expoente igual ao número de dígitos da parte não-periódica da dízima (entendendo-se que esta esteja escrita em sua forma mais "econômica").

Prova:

Como temos feito, para não distrair o leitor com a complicada notação, mostremos o raciocínio num caso significativo, o da dízima $0,b_1b_2\overline{c_1c_2c_3}$. Ficará para o leitor, como exercício posterior, redigir a prova do caso geral.

Sabemos, do Teorema 4.33, que

$$0,b_1b_2\overline{c_1c_2c_3} = \frac{b_1b_2c_1c_2c_3 - b_1b_2}{99900}\,,$$

e queremos mostrar que o denominador da correspondente fração irredutível admite ao menos um dentre 2^2 e 5^2 como fator.

Iniciemos observando que o denominador acima se escreve como

$$99900 = 999 \times 100 = 999 \times 2^2 \times 5^2\,.$$

Consequentemente, ao simplificarmos a geratriz, tendo em vista que a Proposição 4.35 proibe de obtermos numerador com fator 10, podemos eliminar um fator 2 ou um 5, mas nunca os dois ao mesmo tempo. Consequentemente, após a simplificação, sobrará 2^2 ou 5^2, ou ambos.

CQD.

Teorema 4.38 -

Uma fração irredutível gera uma dízima finita $\Longleftrightarrow$ *seu denominador é da forma* $2^\alpha \times 5^\beta$*, onde os inteiros* α, $\beta \geqslant 0$.

Prova:

Este resultado é mero resumo do que dizem o Teorema 4.5 e o Exercício 93.

CQD.

Teorema 4.39 -

Uma fração irredutível gera uma dízima periódica simples $\iff$ seu denominador não tem nem 2 e nem 5 como fator.

Prova:

A proposição 4.36 nos mostra que a condição é necessária. Resta mostrar que é suficiente, ou seja, que se o denominador não tem nem 2 e nem 5 como fator, então a dízima é periódica simples. Ora, isto é verdadeiro, pois é a contrapositiva do Teorema 4.37.

CQD.

Teorema 4.40 -

Uma fração irredutível gera uma dízima periódica composta $\iff$ seu denominador tem, com outros fatores, ao menos um dentre 2 e 5 como fator.

Prova:

O enunciado desse teorema é a versão $\neg p \iff \neg q$ do teorema anterior.

CQD.

Exercício 120 -

Escrever a prova para o caso geral da Proposição 4.37.

Exercício 121 -

Escrever a prova do Teorema 4.39, sem apelar diretamente para o Teorema 4.37.

Exercício 122 -

Escrever a prova do Teorema 4.40, sem apelar diretamente para o Teorema 4.39.

CAPÍTULO 5

NOÇÕES BÁSICAS SOBRE A RETA EUCLIDIANA

Neste capítulo apresentaremos e discutiremos alguns resultados básicos da Geometria Euclidiana, relativos à noção de reta. A razão dessa breve incursão em Geometria Euclidiana é que, no capítulo seguinte, iremos considerar o problema da medição de segmentos de reta e, para que possamos fazer isto de maneira matematicamente consistente, precisaremos ter uma descrição matemática rigorosa da reta.

Uma das principais propriedades da reta euclidiana é a sua continuidade topológica . Com efeito: a reta euclidiana é o mais importante e conhecido exemplo de contínuo topológico. [1] O propósito maior deste capítulo é explicar o significado disso.

[1] Também se diz que a reta é um continuum

Em cursos de Geometria Superior, o leitor estudará outras propriedades da reta euclidiana e será apresentado a diversos tipos de reta, como a reta projetiva. Também ficará para outras matérias o estudo dos demais exemplos de *contínuos*.

5.1 Segmentos de reta: comparação

– Notação e terminologia inicial

Trabalhando na reta euclidiana, denotaremos seus pontos por letras latinas maiúsculas e usaremos a notação AB para denotar o segmento de reta que tem os pontos A e B como extremidades.

– Comparação de segmentos de reta

Queremos definir o que entenderemos ao dizer que um segmento de reta AB é congruente, menor ou maior do que um outro segmento CD. Esta comparação pode ser feita por meio de um compasso, conforme passaremos a explicar.

Definição 5.1 -

Na reta euclidiana, diremos que dois segmentos de reta são congruentes *se for possível superpô-los exatamente.*

Essa operação de "superposição" deve ser vista como a idealização da seguinte construção geométrica, realizada com um compasso: fazendo as pontas do compasso coincidirem com as extremidades do primeiro segmento e, mantendo esta abertura fixa, verificamos se é possível fazer o mesmo com as extremidades do segundo segmento.

Que basta preocupar-nos com as extremidades é consequência do axioma da Geometria Euclidiana que diz que por dois pontos passa exatamente uma reta. Com efeito, segundo tal axioma, todo segmento de reta fica univocamente determinado por suas extremidades.

Notação

Dados dois segmentos de reta quaisquer, AB e CD, se ocorrer de eles serem congruentes, escreveremos $AB = CD$; caso contrário, escreveremos $AB \neq CD$.
(Nos livros de Geometria, podem ser usadas outras notações, tais como $AB \equiv CD$ e $AB \cong CD$. O importante é o leitor ter bem claro que congruência não é o mesmo que igualdade de conjunto de pontos.)

Definição 5.2 -

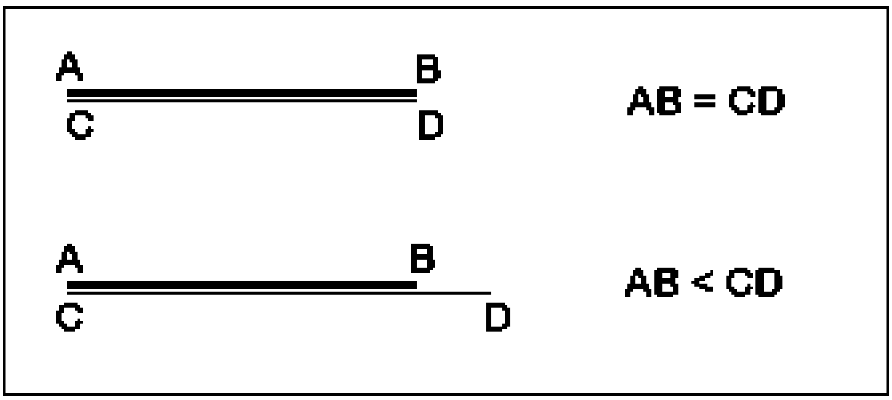
Na reta euclidiana, dado um segmento de reta AB, diremos que:

- *AB será* menor *do que um segmento CD, se for possível deslocar/transladar AB com o compasso de modo a ficar estritamente contido em CD;*
- *AB será* maior *do que um segmento CD, se CD for menor do que AB.*

Notação:

$AB = CD$ significará que os segmentos AB e CD são congruentes
$AB < CD$ significará que AB é menor do que CD
$AB > CD$ significará que AB é maior do que CD
$AB \leqslant CD$ significará que ou $AB = CD$ ou $AB < CD$
$AB \geqslant CD$ significará que ou $AB = CD$ ou $AB > CD$.

Confira na figura a seguir:



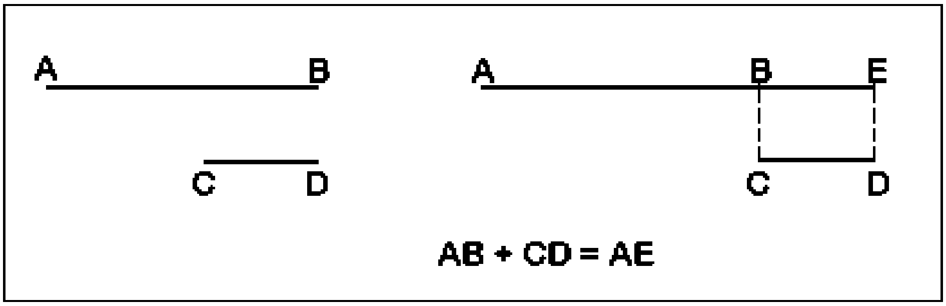
5.2 Segmentos de reta: operações

– Adição de segmentos de reta

Dados dois segmentos AB e CD sobre uma mesma reta, sua soma é o segmento AE que se constrói prolongando AB, a partir de B, até um ponto E, tal que BE seja congruente a CD.
Notação:

$$AB + CD = AE\,.$$

Confira na figura a seguir:



– Múltiplo de um segmento de reta

Notação.
Para cada n número natural positivo e cada segmento de reta AB, por $n \cdot AB$ denotaremos o segmento CD obtido somando n cópias de AB :

$$n \cdot AB = AB + AB + \overbrace{\cdots}^{n} + AB\,.$$

– Divisão de um segmento dado em partes iguais (ou alíquotas)

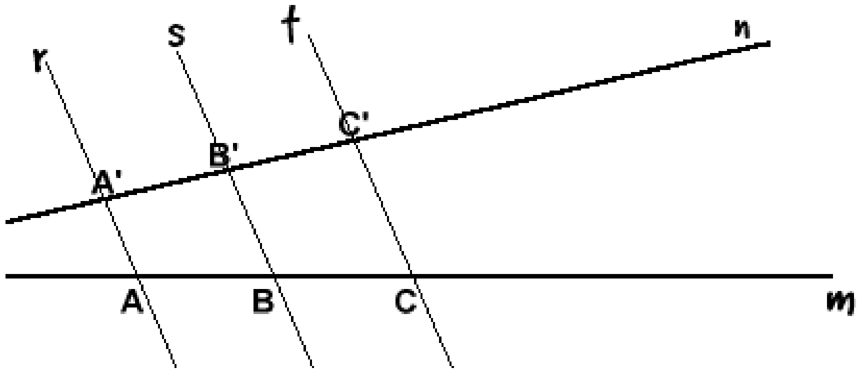
Definição 5.3 -

Se dividirmos um dado segmento de reta em partes iguais, chamaremos cada uma delas de parte **alíquota** *do segmento.*

Passemos a mostrar que, usando apenas compasso e régua, podemos dividir qualquer segmento de reta em 2, 3, ou quantas alíquotas desejarmos. Este processo de divisão baseia-se no Teorema de Thales, que recordamos a seguir.

Teorema 5.4 (Teorema de Thales) (*versão simplificada*) -

Suponhamos que três retas paralelas r, s, t cortam as retas m, n nos pontos A, B, C e A', B', C', respectivamente. Se AB e BC são congruentes, então também serão congruentes os segmentos $A'B'$ e $B'C'$ (veja Figura).



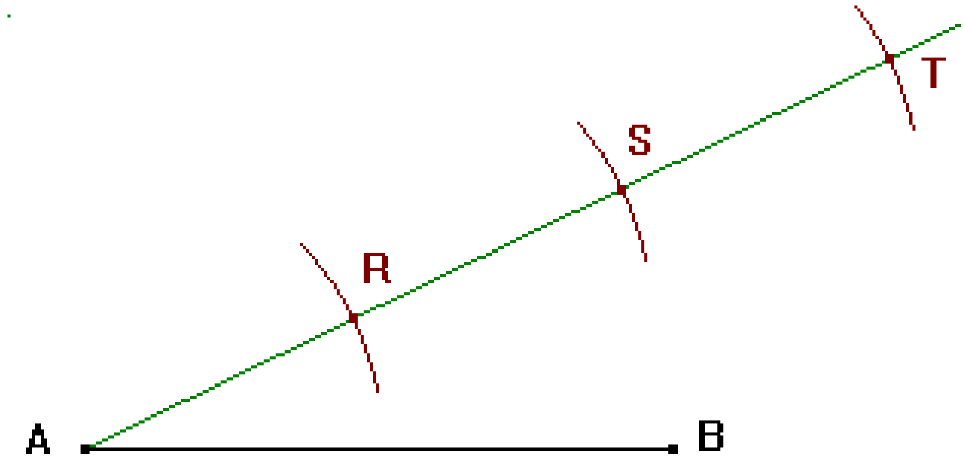
Teorema 5.5 -

Cada segmento de reta pode ser dividido em quantas alíquotas quisermos.

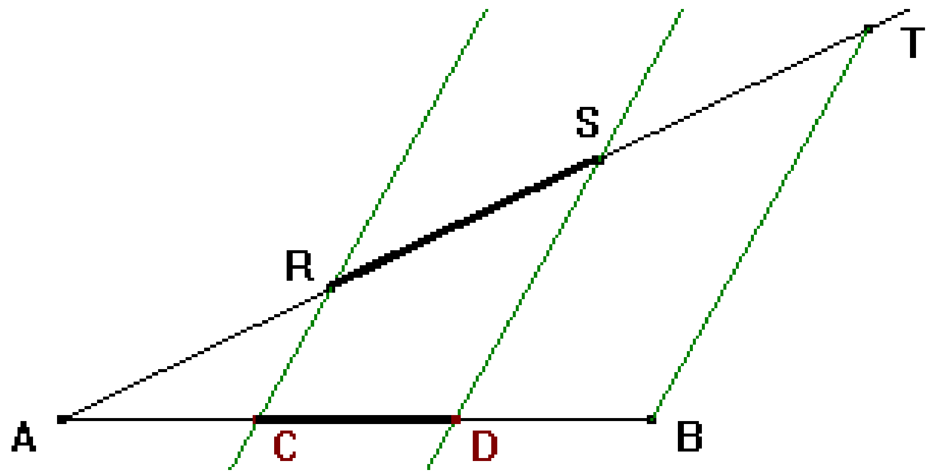
Prova:

Para que o raciocínio fique bem claro, iniciemos com um caso particular: mostremos como dividir um segmento qualquer AB dado em três partes iguais, ou três alíquotas.

Iniciemos com o traçado de uma semi-reta de origem A (acompanhe na figura que segue), cuja direção não coincida com a direção de AB. A seguir, marcamos sobre tal reta, a partir do ponto A e com o compasso, três segmentos congruentes quaisquer: AR, RS e ST.

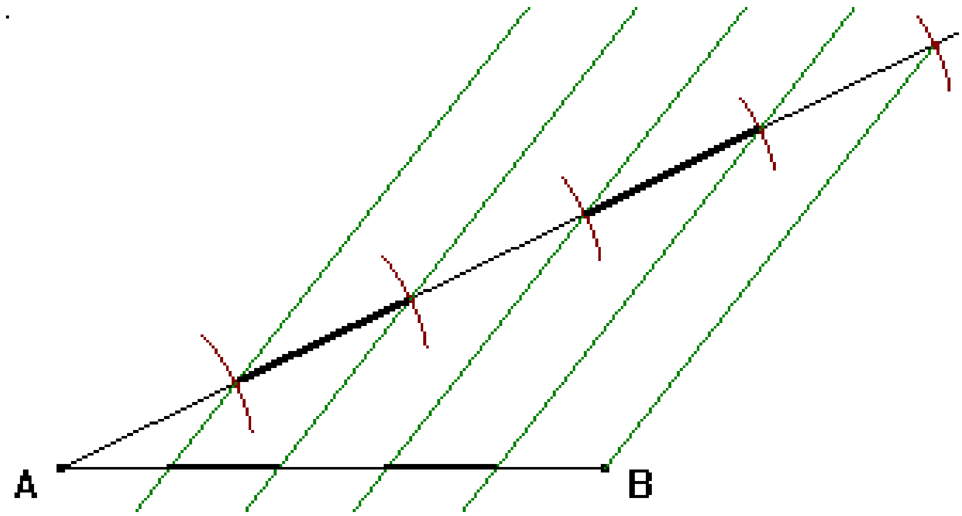


Traçando paralelas, obtemos o ponto D (que é a intersecção entre AB e a paralela a BT, passando por S) e o ponto C (que é a intersecção entre AB e a paralela a BT, passando por R), conforme mostra a seguinte figura:



Pelo Teorema de Thales, é imediato vermos que: AC, CD e DB são congruentes. Assim, acabamos de dividir AB em três partes iguais.

Um outro caso particular: divisão de AB em cinco partes iguais. Fazemos raciocínio análogo: sobre uma semi-reta de origem A e direção diferente de AB, marcamos com o compasso cinco segmentos congruentes e traçamos paralelas de modo semelhante ao já feito. A figura a seguir e o Teorema de Thales nos mostram que dividimos o segmento AB em cinco partes iguais.



Certamente, o leitor não terá a menor dificuldade em ver que os procedimentos que foram descritos são fáceis de modificar para o caso de querermos dividir AB em qualquer outro número de partes iguais, tais como dez, cem etc.

CQD.

Notação.

Por $\frac{1}{m} \cdot AB$ denotaremos qualquer um dos segmentos obtidos dividindo-se o segmento de reta AB em m partes iguais (onde m é um inteiro $\geqslant 1$).
Podemos combinar as notações anteriores, escrevendo:

$$\frac{n}{m} \cdot AB = n \cdot \left(\frac{1}{m} \cdot AB \right),$$

isto é, $\frac{m}{n} \cdot AB$ indica n cópias do segmento $\frac{1}{m} \cdot AB$.

5.3 Propriedade arquimediana da reta

A propriedade da reta euclidiana que a seguir enunciaremos é fundamental para que possamos medir qualquer segmento de reta, conforme veremos no próximo capítulo.

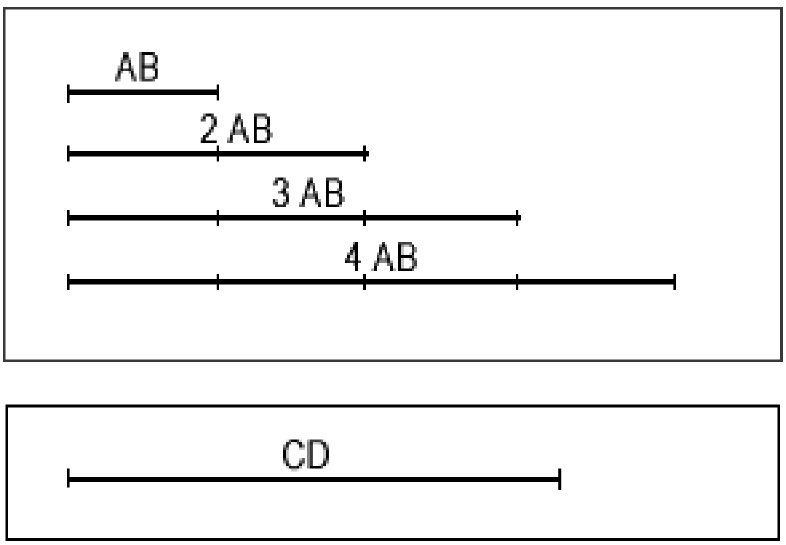
É importante salientarmos que a mesma *não é um teorema e sim um axioma ou postulado*. Embora não fosse explicitamente formulada como axioma nos Elementos de Euclides (300 AC), seu uso intuitivo era bem aparente quando da aplicação do método da exaustão ao cálculo de áreas e volumes, o que já tinha sido notado por Eudoxos (375 AC). A atribuição deste postulado a Archimedes (200 AC) deve-se ao fato de ter sido ele o primeiro a reconhecer sua "indemonstratibilidade".

Também é importante enfatizarmos que já encontramos essa "propriedade arquimediana" no contexto dos números inteiros e racionais. Com efeito, ela se aplica a muitos tipos de grandezas, embora existam o que se chama de "grandezas não-arquimedianas".

– Postulado de Archimedes/propriedade arquimediana

Na reta euclidiana, dado um segmento de reta AB (não reduzido a um único ponto), para cada segmento CD que escolhermos, sempre se acha um número natural n tal que o segmento formado pela soma de n cópias de AB é maior do que CD:

$$CD < n \cdot AB.$$



AB e' menor do que CD, mas
4AB e' MAIOR do que CD

5.4 Postulado do Contínuo

A continuidade da reta é uma ideia que tem fascinado e intrigado a Humanidade por muitos séculos. Em essência, deseja-se dizer que a reta não tem "furos" ou interrupcões. Euclides, em seu Elementos, considerou esta ideia como intuitiva, não explicitando-a como axioma ou postulado. Isso somente acabou ocorrendo mais de dois mil anos depois, após os trabalhos de Dedekind e George Cantor.

Para caracterizar matematicamente a continuidade da reta euclidiana, será importante considerarmos dois tipos muito especiais de sequências de segmentos de reta:

Definição 5.6 -

Uma sequência de segmentos de reta P_1Q_1, P_2Q_2, ... é dita encaixante *se estes segmentos, vistos como conjuntos de pontos, verificarem as inclusões:*

$$P_1Q_1 \supseteq P_2Q_2 \supseteq P_3Q_3 \supseteq \cdots \supseteq P_nQ_n \supseteq P_{n+1}Q_{n+1} \supseteq \cdots .$$

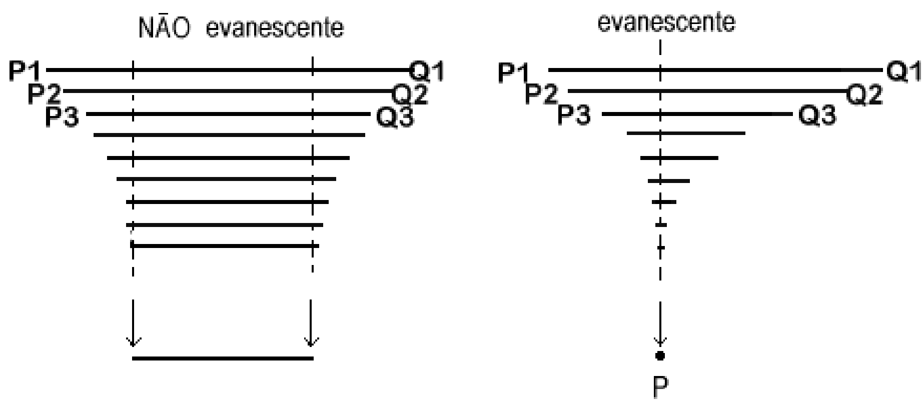
Definição 5.7 -

Uma sequência (infinita) de segmentos reta P_1Q_1, P_2Q_2, ... é dita evanescente *se:*

- *for encaixante;*
- *e, ademais, para cada segmento de reta AB (não reduzido a um único ponto) que escolhermos, sempre pudermos encontrar um n tal que o n-ésimo segmento da sequência satisfaça:*

$$P_nQ_n < AB .$$

As figuras a seguir ilustram exemplos de duas sequências de segmentos encaixantes, uma evanescente e a outra não.



Podemos, finalmente, caracterizar a continuidade da reta euclidiana:

– Postulado do Contínuo/Princípio dos Segmentos Evanescentes

Sempre que P_1Q_1, P_2Q_2, P_3Q_3, $\ldots$ *for uma sequência evanescente de segmentos de reta, podemos afirmar que existe exatamente um ponto comum a todos os segmentos da sequência.*

Intuitivamente, esse postulado ou axioma diz que a reta euclidiana é "contínua", isto é, não tem "buracos". Isso pode ser interpretado mais concretamente dos seguintes modos:

1) Se numa posição qualquer da reta Euclidiana colocássemos as pontas de uma pinça e, depois, começássemos a fechá-la, fazendo-a ficar com abertura sucessivamente 1/10, 1/100 etc. da abertura inicial, e se continuássemos com este processo eternamente, então teríamos um único ponto que ficou "prensado" pela pinça em todas as etapas.

2) Se focássemos um microscópio sobre a reta e sucessivamente aumentarmos a resolução do microscópio em 10 vezes, 100 vezes etc., então, "no infinito" veríamos exatamente um ponto, qualquer que tenha sido a posição inicial do microscópio. Em outras palavras, existirá apenas um ponto que permanecerá no campo de visão do microscópio em todas as etapas.

Resumindo

Não podemos deixar de enfatizar que as propriedades arquimediana e de continuidade da reta euclidiana *não são demonstráveis:* a Geometria Euclidiana exige, ou *postula,* que elas sejam verdadeiras.

Embora seja bastante seguro afirmar que – em seus estudos de Geometria nos Ensino Fundamental e Médio – o leitor nunca encontrou nenhuma menção dessas duas propriedades, é importante se observar que um exame minucioso das demonstrações geométricas que lá estudou mostra que elas, intuitiva e inconscientemente, foram usadas muito frequentemente.

Uma das razões pelas quais, hoje em dia, usamos a denominação "reta euclidiana" é o desejo de enfatizar que estamos tratando de uma reta que é arquimediana e contínua. Em cursos avançados, o aluno poderá ter a oportunidade de estudar geometrias que não verificam alguma dessas duas propriedades. O exemplo mais simples é o das *geometrias finitas*, cujo espaço é formado de um número finito de pontos.

5.5 Algumas palavras sobre Construções com Régua e Compasso

Praticamente a totalidade dos textos atuais dá como evidente que podemos dividir qualquer segmento de reta dado em tantas partes iguais quantas desejarmos. Tradicionalmente falando, isto seria considerado como heresia. O objetivo desta seção é explicarmos o que há por trás disto e justificar nosso ponto de vista.

O estudo dos objetos geométricos planos envolve a construção de linhas retas e curvas. Para isso, se usam instrumentos de vários tipos. Estes instrumentos variaram bastante ao longo dos tempos e das civilizações. Por exemplo, os geômetras e agrimensores da civilização egípcia tinham como instrumento de trabalho uma corda na qual tinham sido feitos nós uniformemente espaçados.

Quando, por volta de 500 AC, os gregos iniciaram o estudo científico da Geometria, como sua cultura tinha em alta estima a simplicidade, elegeram como instrumentos geométricos preferidos a régua e o compasso, pois estes são os instrumentos que nos permitem construir as linhas mais simples possíveis: retas e círculos. Alguns gregos, entre os quais Archimedes, aceitavam usar outros instrumentos.

Euclides – em seu livro *Elementos*, escrito por volta de 300 AC, e que por quase 2000 anos foi o mais importante livro de Matemática em boa parte do Mundo Cristão – adotou o costume já tradicional de permitir apenas o uso de régua e compasso. Dada a sua significativa autoridade, esses instrumentos (na verdade, suas "traduções matemáticas") passaram a ter um caráter oficial, e as correspondentes construções passaram a ser chamadas de "construções euclidianas", hoje mais conhecidas como "construções com régua e compasso".

Assim, de um modo inicial e grosseiro, as construções euclidianas são as construções geométricas que podemos fazer com uma régua e um compasso. A função maior da régua é estabelecer colinearidade, e a do compasso é estabelecer equidistância.

O compasso não serve apenas para desenhar círculos. Por exemplo, podemos usar suas pontas para transportar distâncias e, com um pouco de criatividade, pode-se inventar inúmeros outros usos geométricos para o mesmo. Isto levou os próprios gregos a delimitarem esses usos. Por exemplo, quanto ao compasso, os gregos não permitiam que o mesmo fosse levantado do plano onde estava sendo feita a construção.

A régua euclidiana também tem restrições: ela não pode ser graduada, ou seja, a régua euclidiana não pode ter marcas, como as réguas graduadas em centímetros e milímetros que estamos acostumados a usar. Semelhante ao que foi feito com o compasso, o uso dessa régua não graduada também deve obedecer restrições. Por exemplo, não podemos "arrastá-la".

É perfeitamente possível darmos uma caracterização formal e rigorosa do que são as "construções euclidianas", mas o esforço e grau de abstração para tal é excessivamente grande para os propósitos deste texto. Além disso, as construções que aqui consideraremos serão bastante simples e intuitivas, não deixando margem para que se duvide da possibilidade de serem matematicamente validadas. No entanto, não podemos deixar de ressaltar que existem muitas questões delicadas e sutis, algumas das quais constituiram desafios matemáticos por mais de 2.000 anos, cujo enfrentamento exige uma formulação matematicamente precisa dessas construções, acompanhada de uma rigorosa teoria.

Um desses famosos desafios foi posto já pelos gregos da Antiguidade e pedia a trisseção de um ângulo, ou seja, a divisão de um ângulo qualquer em três partes iguais. Os próprios gregos resolveram esse problema fazendo uso de outros instrumentos além da régua e do compasso. Contudo, a resolução euclidiana – no sentido tradicional: somente régua não graduada e compasso – resistiu por muitos séculos, até que, em torno de 1840, Pierre L. Wantzel (depois de muitas noites passadas à base de café e ópio!) mostrou que existem ângulos que *não* podem ser trisseccionados euclidianamente.

Que fique bem claro ao leitor que o costume de se considerar um problema geométrico como resolvido somente quando sua solução for passível de ser obtida através de uma construção euclidiana, é apenas uma tradição, e que esta tradição está obsoleta. A nossa posição neste texto será a de adotar soluções euclidianas quando as mesmas existirem e forem simples (já encontramos um exemplo destas situações quando tratamos da divisão de um segmento qualquer de reta em um número dado qualquer de partes iguais), caso contrário, não hesitaremos em partir para construções não-euclidianas (como, por exemplo, ocorrerá ao termos de dividir um ângulo qualquer em um número dado qualquer de partes iguais).

CAPÍTULO 6

NÚMEROS REAIS ABSOLUTOS

Neste capítulo introduziremos a noção de número real absoluto, associando-a à ideia de medida (comprimento) de segmentos da reta euclidiana. Isto será feito após mostrarmos que os números racionais, embora capazes de medir *aproximadamente* qualquer segmento de reta, são insuficientes para fazer o mesmo *exatamente*.

Com o propósito de resolver esse impasse, apresentaremos uma maneira de medir (exatamente) qualquer segmento de reta através de um processo que denominaremos de "medição iterativa". O conceito de número real absoluto surgirá naturalmente como o recurso necessário para expressar o resultado dessa medição.

6.1 Medida dos segmentos da reta euclidiana: generalidades

Todo processo de medição envolve, antes de mais nada, convencionar uma *unidade de medida*: uma unidade de peso, uma unidade de tempo, uma unidade de volume, etc. No caso especial que nos interessa, o da medida do comprimento dos segmentos da reta, convencionar uma unidade de comprimento significa escolher e fixar um segmento da reta euclidiana não reduzido a um único ponto.

Chamaremos tal segmento de segmento unitário *e o denotaremos por* OU.

Feita essa escolha, o processo de medição propriamente dito, de qualquer segmento de reta, consiste em determinar o número de vezes que o segmento unitário cabe no segmento dado.

Passaremos a discutir matematicamente o que está envolvido em tal "determinação", e o que deveremos entender por tal "número de vezes". Com tal objetivo em mente, a primeira coisa que temos de ressaltar é que, nas medições do dia-a-dia, usamos algumas propriedades básicas que, embora intuitivas, não podem ser matematicamente demonstradas e, assim, têm de ser vistas como postulados (ou axiomas) do processo de medição:

– Postulados que regem a medição de segmentos da reta euclidiana:

- Cada segmento de reta, AB, tem exatamente uma medida (comprimento), e ela será denotada por $|AB|$.
- Segmentos de reta congruentes têm a mesma medida.
  Simbolicamente: AB congruente a $CD \iff |AB| = |CD|$.
- A medida do todo é maior do que a da parte.
  Simbolicamente: $AB \geqslant CD \Rightarrow |AB| \geqslant |CD|$.
- A medida é aditiva, ou seja: a medida de um todo é a soma da medida das suas partes. Mais precisamente:
  se C é um ponto entre A e B, então

$$|AB| = |AC + CB| = |AC| + |CB|.$$

- Os segmentos triviais (ou seja, reduzidos a um único ponto), e só eles, têm medida nula.

– Convenção:
a medida do segmento unitário é $|OU| = 1$.

Da aditividade da medida, segue:

Proposição 6.1 -

A medida do múltiplo é o múltiplo da medida. Mais precisamente, para cada n inteiro positivo, temos que $|nAB| = n|AB|$.

Prova:

A prova é por indução em $n \geqslant 2$.
– Para $n = 2$, temos $2AB = AB + AB = AB + BC$, desde que $AB = BC$. Assim, a aditividade nos permite escrever:

$$|2AB| = |AB + BC| = |AB| + |BC| = |AB| + |AB| = 2|AB|.$$

– Valendo para $n \geqslant 2$, vale para $n + 1$.
Com efeito, como $(n + 1)AB = nAB + AB$, escrevendo $nAB = AC$ e tomando $CD = AB$, vemos que

$$|(n + 1)AB| = |nAB + CD| = |nAB| + |CD| = n|AB| + |AB| = (n + 1)|AB|.$$

CQD.

Com esses postulados e resultado, podemos calcular o comprimento de vários tipos de segmentos de reta:

Proposição 6.2 -

i). Se $AB = nOU$, então $|AB| = n$.
ii). Se $AB = \frac{1}{n}OU$, então $|AB| = 1/n$.
iii). Se $AB = m \cdot \frac{1}{n}OU$, então $|AB| = m/n$.

Prova:

– Para (i):
de $AB = nOU$ sai, pela proposição anterior, $|AB| = |nOU| = n|OU| = n \cdot 1 = n$.

– Para (ii):
escrever $AB = \frac{1}{n}OU$ é escrever $OU = nAB$, logo $1 = |OU| = |nAB| = n|AB|$.

– Para (iii):
usando a proposição anterior e o item (ii), temos que, se $AB = m \cdot \frac{1}{n}OU$, então $|AB| = |m\frac{1}{n}OU| = m|\frac{1}{n}OU| = m \cdot \frac{1}{n} = \frac{m}{n}$. CQD.

6.2 A insuficiência geométrica dos racionais

– Questão Fundamental: quais números expressam as medidas (exatas) de segmentos de reta?

Inicialmente, observemos que esses números têm de ser $\geqslant 0$. Com efeito, para qualquer segmento de reta AB, temos que $AB \geqslant AA$, logo $|AB| \geqslant |AA| = 0$.

A seguir, observemos que todas as medidas envolvidas na proposição anterior têm como resultado um número racional absoluto (ou seja: um racional $\geqslant 0$). Reciprocamente, todo número racional absoluto é a medida de algum segmento de reta. Com efeito, deixando de lado o caso trivial do número zero, dado um racional positivo, m/n, inicialmente construímos o segmento de reta $\frac{1}{n}OU$ e, a seguir, fazemos m cópias do mesmo. É imediato vermos que a medida deste último segmento é m/n.

Essas observações nos levam a reformular a questão fundamental acima:

– Questão Esperançosa: os racionais absolutos bastam para medir (exatamente) qualquer segmento de reta?

Infelizmente, a resposta é não! Para comprovarmos isso, é conveniente, ou ao menos tradicional, introduzirmos a seguinte terminologia:

Definição 6.3 -

Dois segmentos da reta euclidiana, AB e CD, são ditos comensuráveis *se, e só se, existirem números naturais m e n tais que vale a igualdade: $mAB = nCD$.*

Assim, podemos dividir os segmentos de reta em dois tipos;

- Segmentos comensuráveis com o segmento unitário.
  São os segmentos AB, tais que um múltiplo de AB é congruente a um múltiplo do segmento unitário:

$$mAB = nOU\,.$$

- Segmentos incomensuráveis com o segmento unitário.
  Nenhum múltiplo de um tal segmento é congruente a um múltiplo do segmento unitário.
  (Vide abaixo a prova da existência deste tipo de segmento.)

Teorema 6.4 -

Todo segmento de reta comensurável com a unidade tem como medida um número racional absoluto. Reciprocamente, se a medida de um segmento de reta for um número racional absoluto, este segmento é comensurável com o segmento unitário.

Prova:

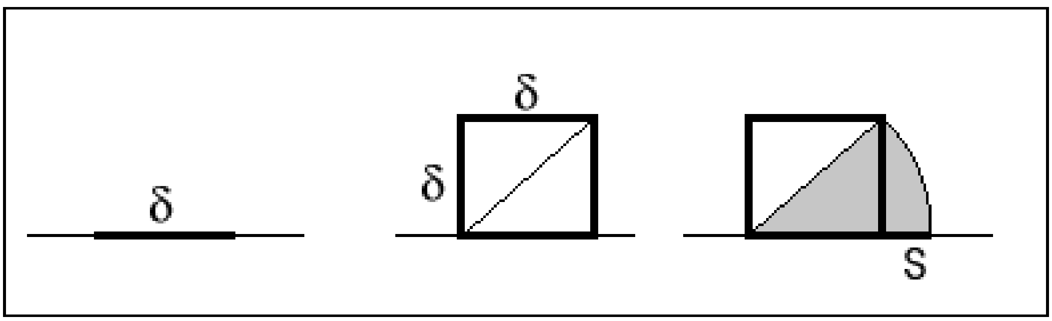
Imediata, a partir da relação $mAB = nOU$ e dos resultados anteriores. CQD.

Teorema 6.5 -

Existem segmentos de reta incomensuráveis com a unidade. Nenhum deles tem como medida um número racional.

Prova:

Evidentemente, basta exibirmos um exemplo de segmento incomensurável com o segmento unitário OU. Para tal, iniciamos construindo um quadrado de lado OU. Feito isso, com um compasso, construímos um segmento de reta, S, congruente à diagonal deste quadrado, conforme a figura a seguir.



É impossível S ser comensurável com o segmento unitário (lado do quadrado), pois, se assim fosse, sua medida $|S|$ seria um número racional cujo quadrado, vale 2:

$$|S|^2 = |OU|^2 + |OU|^2 = 1 + 1 = 2 \quad \text{(por Pythagoras)},$$

o que já sabemos ser impossível. (Essa impossibilidade já foi provada como uma aplicação do Teorema Fundamental da Aritmética – vide Capítulo 2 –, mas confira a seguir uma prova que usa apenas argumentos de paridade.) CQD.

Prova: (alternativa)
Vamos raciocinar por absurdo, supondo que exista um racional $x = m/n$, tal que $x^2 = 2$. Sem perda de generalidade, podemos supor que a fração m/n já está na forma irredutível. Teremos:

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

Assim, o inteiro m^2 é par, e portanto m também será par. Ou seja, m é um inteiro da forma $m = 2k$, com k inteiro. De modo que:

$$\begin{aligned} 2n^2 &= m^2 = (2k)^2 = 4k^2 \Rightarrow \\ n^2 &= 2k^2, \end{aligned}$$

de onde concluímos que n^2 é par. Mas então n também será par, o que é um absurdo! Com efeito, são contraditórias as conclusões que m e n são pares com a hipótese de que a fração m/n seja irredutível. CQD.

Veredito –

A resposta da Questão Esperançosa é negativa! Os números racionais *são insuficientes* para expressarem a *medida* (*exata*) de todos os tipos de segmentos da reta euclidiana.

Com esse veredito, ficamos com duas alternativas:

- continuar com os números racionais e "remediar" o caso dos segmentos incomensuráveis com a unidade, mostrando que podemos obter para eles medidas racionais tão aproximadas quanto desejarmos, ou
- construir um tipo de número mais geral do que os racionais, e mostrar que com eles podemos medir exatamente qualquer segmento de reta.

No que segue, adotaremos a segunda opção, pois é mais elegante e mais poderosa: além de poder expressar a medida exata de qualquer segmento reta, *também* permitirá obtermos aproximações tão boas quanto desejarmos. Esta opção envolverá a construção do que chamaremos de Régua Infinita, com a qual poderemos introduzir os números reais absolutos e, assim, resolver definitivamente o problema da medição.

– Breves considerações históricas

A descoberta das grandezas incomensuráveis ocorreu entre os matemáticos gregos, muito provavelmente por cerca de 450 AC. Ela produziu a primeira grande crise na Matemática, a chamada *Crise dos Incomensuráveis*. Em verdade, essa crise consistiu de dois impactos no já sofisticado pensamento grego.

- Crise matemática:
  os gregos reduziam a medida de todas as grandezas contínuas – geométricas (segmentos de reta, superfícies e sólidos) e físicas (peso, tempo etc.) – à medida dos segmentos de reta; ora, como achavam que todos os segmentos eram comensuráveis com a unidade, deduziam que toda medida poderia ser expressa por meio de razão entre números naturais (diríamos nós: em termos de números racionais absolutos).
- Crise filosófica:
  veio por terra a doutrina filosófica da muito importante Escola Pitágorica, a qual pregava que a harmonia do universo era regida por leis matemáticas expressas em termos de razões entre números naturais.

Quem descobriu o primeiro par de grandezas incomensuráveis ?

Apenas fragmentos dos documentos matemáticos anteriores a Euclides (300 AC) chegaram aos tempos modernos, isso torna impossível termos certeza do autor e data exata da descoberta. Contudo, pode-se afirmar que foi por algum membro da Escola Pitagórica, provavelmente Hippassos de Metapontion.

Qual o primeiro par de grandezas incomensuráveis descoberto ?

Essa pergunta é igualmente difícil de ser respondida. A leitura atenta dos famosos Diálogos de Platon (c. 350 AC), e textos posteriores, nos faz pensar em vários candidatos: a diagonal e lado do quadrado, a diagonal e lado de pentágono, os dois segmentos obtidos pela divisão de um segmento dado em razão média e extrema (seção áurea) etc. Também é de se acrescentar que, por cerca de 400 AC, já eram conhecidos resultados sobre incomensurabilidade que em muito ultrapassam o que veremos neste livro. Exemplos desses resultados são um livro, há séculos perdido, de Demokritos e os estudos de Theaitetos, boa parte dos quais foram incorporados por Euclides nos livros X e XIII de seu *Elementos*.

Como se chegou até tal descoberta ?

O importante é atinarmos que a descoberta dos incomensuráveis só pode ter sido feita por via estritamente dedutiva: não poderia ter sido feita por experimentação! Ademais, certamente não foi por meio de provas como as dadas acima, embora a segunda delas já fosse conhecida de Aristóteles. A argumentação grega original, muito provavelmente, era baseada na noção de *anthyphairesis* e é melhor revista em livros de História da Matemática.

Soluções para a crise.

Os próprios gregos, por cerca de 400 AC, com Theaitetos e Eudoxos, escreveram uma teoria das grandezas contínuas, e que envolvia os incomensuráveis. No século XIX, outras soluções surgiram, variando em naturalidade e grau de rigor, as principais sendo as de Ch. Méray, G. Cantor, K. Weierstrass e R. Dedekind. Como veremos, o trabalho que desenvolvemos até agora nos permitirá apresentar uma outra solução para o problema da medida das grandezas contínuas, solução esta natural e simples, mas também rigorosa. É o que será feito em detalhes nas próximas seções.

Exercício 123 -

Mostre que, para cada segmento de reta, AB, vale:

$$|AB| \geqslant |\frac{1}{2}AB| \geqslant |\frac{1}{3}AB| \geqslant \cdots$$

Exercício 124 -

Mostre que os segmentos da reta euclidiana podem ser divididos em três categorias:
– segmentos que são múltiplos do segmento unitário
– segmentos que são múltiplos de uma alíquota do segmento unitário
– segmentos que não são iguais a nenhum múltiplo de alíquota do segmento unitário.

Exercício 125 -

Construamos recursivamente uma sequência de quadrados, Q_n, do seguinte modo:
– Q_1 é o quadrado de lado unitário;
– Q_2 é o quadrado cujo lado é a diagonal de Q_1 ;
– para $n \geqslant 2$, o quadrado Q_{n+1} é o quadrado cujo lado é a diagonal de Q_n .
Assim, indicando por δ_n a medida da diagonal do quadrado Q_n, pede-se:

i). fazer desenho ilustrando geometricamente a construção dos Q_n ;

ii). pensando em áreas, mostrar que $\delta_{n+1}^2 = 2\delta_n^2$;

iii). mostrar que δ_n é comensurável com o segmento unitário $\iff$ n é par.

Exercício 126 -

Se um segmento de reta AB for incomensurável com um segmento CD, será que AB é incomensurável com o segmento unitário? Justifique sua resposta.

6.3 Construção da régua infinita sobre a reta euclidiana

Nosso propósito maior, qual seja, o de *medir exatamente qualquer segmento de reta*, necessita dispor de uma régua que permita realizar medidas arbitrariamente pequenas, diferentemente das réguas escolares, que permitem medidas com no máximo milímetros de precisão. Isto implica em precisarmos de uma régua idealizada, uma régua matemática, a qual terá infinitas subdivisões: unidades, décimos, centésimos, milésimos, décimos de milésimos da unidade, e assim por diante, ad infinitum. Por isso, ela será chamada de régua infinita.

Ressaltamos que a diferença fundamental entre a régua comum e a régua infinita é que, num pedaço qualquer de régua, a primeira tem apenas um número finito de marcações (normalmente, até os milímetros ou milésimos do metro) enquanto que a segunda tem um número infinito de marcações.

Obviamente, o que faremos a seguir é uma idealização matemática; no mundo material, jamais conseguiremos construir uma régua com *infinitas* marcações. Isto só é possível em uma "reta abstrata", como a reta euclidiana, apresentada no capítulo anterior.

Nesta seção trataremos da construção de nossa régua matemática, e nas próximas veremos como utilizá-la para medir de maneira exata qualquer segmento de reta.

Para facilitar o entendimento da nossa construção, faremos duas convenções:

- nossa régua será construída sobre uma reta euclidiana, r, que visualizaremos na posição horizontal;
- sobre r, escolheremos uma origem O e para unidade de medida um segmento OU, cujo extremo esquerdo coincidirá com O.

A construção de nossa régua matemática será feita por meio de uma sequência infinita de etapas, em cada uma das quais "marcaremos" em r uma rede de pontos com "graduação" (espaçamento) constante.

– Primeira etapa: rede de graduação unitária.
O primeiro ponto dessa rede é simplesmente o ponto U de OU. Denotamos esse ponto por $P(1)$. Para marcarmos o segundo ponto, tomamos um compasso com a abertura do segmento OU (ou seja, tal que suas duas pontas coincidam com os pontos extremos de OU). A seguir, colocamos a ponta seca do compasso em $P(1)$ e marcamos com a outra ponta um ponto de r à direita de $P(1)$.Denotamos esse novo ponto por $P(2)$. Continuamos, colocando a ponta seca do compasso em $P(2)$ e marcamos com a outra ponta um novo ponto de r, que denotaremos por $P(3)$, à direita de $P(2)$. Repetindo esse processo indefinidamente, obtemos um conjunto de

infinitos pontos sobre a semi-reta de r com origem em O:

$$O,\ P(1),\ P(2),\ P(3),\ P(4),\dots,\ P(n),\dots$$

os quais constituem a rede de graduação unitária da régua infinita.

– Segunda etapa: rede de graduação decimal.
Iniciamos dividindo o segmento unitário em dez alíquotas, ou dez partes iguais (para isso, podemos usar o Teorema de Thales, conforme explicado detalhadamente no capítulo anterior). A seguir, prosseguimos de modo semelhante ao da primeira etapa, só que tomando como abertura do compasso a abertura da alíquota que obtivemos com a divisão feita. Ou seja: usamos como abertura o décimo da abertura de OU. Deste modo, iremos marcar, sucessivamente e à direita de O, os pontos:

$$\begin{aligned}
O, P\left(\frac{1}{10}\right),\ P\left(\frac{2}{10}\right),\dots,P\left(\frac{10}{10}\right) &= P(1),\\
P\left(\frac{11}{10}\right),\ P\left(\frac{12}{10}\right),\dots,P\left(\frac{20}{10}\right) &= P(2),\\
P\left(\frac{21}{10}\right),\ P\left(\frac{22}{10}\right),\dots,P\left(\frac{30}{10}\right) &= P(3),\\
\dots &
\end{aligned}$$

o conjunto dos quais chamaremos de *rede de graduação decimal* da régua infinita.

Note que a rede de graduação decimal também pode ser representada usando expansão decimal dos racionais associados:

$$\begin{aligned}
O,\ & P(0,1),\ P(0,2),\ P(0,3),\ P(0,4),\dots,P(1,0) = P(1),\\
& P(1,1),\ P(1,2),\ P(1,3),\ P(1,4),\dots,P(2,0) = P(2),\\
& P(2,1),\ P(2,2),\ P(2,3),\ P(2,4),\dots,P(3,0) = P(3),\\
& P(3,1),\ P(3,2),\ P(3,3),\ P(3,4),\dots,P(4,0) = P(4),\\
& \dots
\end{aligned}$$

– Terceira etapa: rede de graduação centesimal.
Prosseguimos de modo semelhante, só que tomando como abertura do compasso um centésimo da abertura de OU. Deste modo, iremos marcar, sucessivamente e à

direita de O, os pontos:

$$
\begin{aligned}
&O, P\left(\frac{1}{100}\right),\ P\left(\frac{2}{100}\right), \ldots, P\left(\frac{100}{100}\right) = P(1),\\
&P\left(\frac{101}{10}\right),\ P\left(\frac{102}{10}\right), \ldots, P\left(\frac{200}{10}\right) = P(2),\\
&P\left(\frac{201}{10}\right),\ P\left(\frac{202}{10}\right), \ldots, P\left(\frac{300}{10}\right) = P(3),\\
&\ldots
\end{aligned}
$$

o conjunto dos quais chamaremos de *rede de graduação centesimal* da régua infinita.

Novamente, notemos que a rede de graduação centesimal também pode ser representada usando expansão decimal dos racionais associados:

$$
\begin{aligned}
O,\ &P(0,01),\ P(0,02),\ P(0,03),\ P(0,04), \ldots, P(1,00) = P(1),\\
&P(1,01),\ P(1,02),\ P(1,03),\ P(1,04), \ldots, P(2,00) = P(2),\\
&P(2,01),\ P(2,02),\ P(2,03),\ P(2,04), \ldots, P(3,00) = P(3),\\
&P(3,01),\ P(3,02),\ P(3,03),\ P(3,04), \ldots, P(4,00) = P(4),\\
&\ldots
\end{aligned}
$$

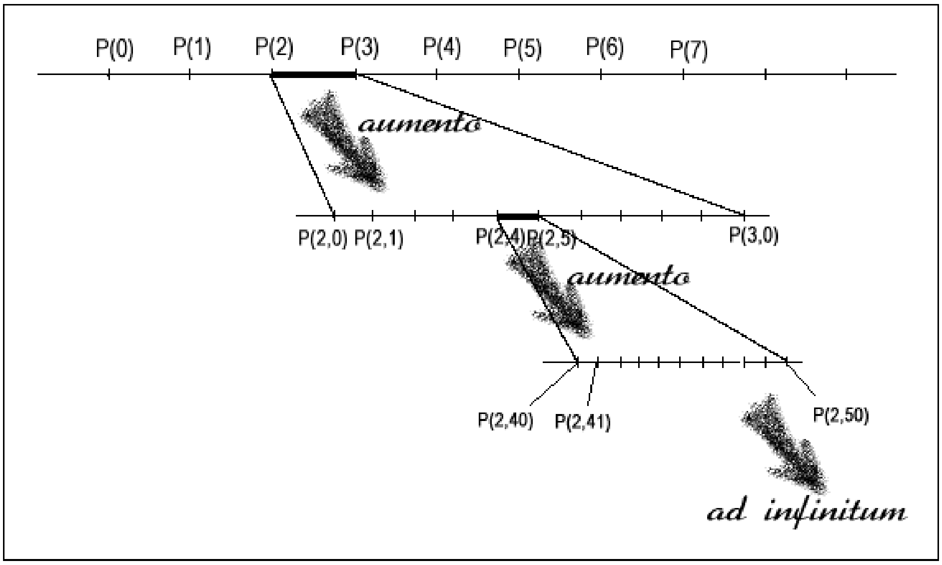
– n-ésima etapa: rede de graduação $1/10^n$.
Prosseguimos de modo semelhante, só que tomando como abertura do compasso $1/10^n$ da abertura de OU. Deste modo, iremos marcar, sucessivamente e à direita de O, os pontos:

$$
\begin{aligned}
&O, P\left(\frac{1}{10^n}\right),\ P\left(\frac{2}{10^n}\right), \ldots,\ P\left(\frac{10^n}{10^n}\right) = P(1)\\
&P\left(\frac{1+10^n}{10^n}\right),\ P\left(\frac{2+10^n}{10^n}\right), \ldots,\ P\left(\frac{10^n+10^n}{10^n}\right) = P(2)\\
&P\left(\frac{1+2\times 10^n}{10^n}\right),\ P\left(\frac{2+2\times 10^n}{10^n}\right), \ldots,\ P\left(\frac{10^n+2\times 10^n}{10^n}\right) = P(3)\\
&\ldots
\end{aligned}
$$

o conjunto dos quais chamaremos de *rede de graduação* $1/10^n$ da régua infinita.

> O conjunto de todos os pontos *de todas essas redes* é o que chamaremos de régua infinita de unidade de medida OU.

Note que esse conjunto consta de todos os pontos (à direita de O) da forma $P(m/10^n)$. Eles serão denominados simplesmente de *pontos graduados da reta* quando não for necessário fazer referência à rede que os originou. O ponto O poderá, eventualmente, ser indicado por $P(0)$.



> Resumindo –
>
> Uma régua infinita é *determinada* escolhendo, sobre uma reta euclidiana, um ponto "origem", O, e um segmento unitário, OU. Essa régua é *construída* com a marcação de infinitas redes de pontos à direita de O e com graduação (espaçamento) sucessivamente menor: $1,\ 1/10,\ 1/10^2,\ 1/10^3, \ldots$.
>
> Com a notação que introduzimos no texto, podemos dizer que essa régua pode ser vista tendo como pontos graduados o seguinte conjunto infinito da reta euclidiana:
>
> $$\{P\left(\frac{m}{10^n}\right) \mid m, n \text{ inteiros} \geqslant 0\},$$
>
> desde que convencionemos que $O = P(0)$.

Exercício 127 -

Usando representação em expansão decimal, escreva os pontos da rede de graduação milesimal.

Exercício 128 -

i). Um ponto da rede de graduação unitária também é um ponto da rede de graduação decimal? Justifique.

ii). Um ponto da rede de graduação decimal também é um ponto da rede de graduação centesimal? Justifique.

iii). Em geral: todo ponto da rede de graduação $1/10^n$ da régua infinita também é um ponto da rede de graduação $1/10^{n+1}$? Justifique.

iv). Dados dois pontos consecutivos da rede de graduação $1/10^n$, digamos, $P\left(m/10^n\right)$ e $P\left((m+1)/10^n\right)$, entre eles existem quantos pontos da rede de graduação $1/10^{n+1}$? Justifique.

Exercício 129 -

V ou F? Justifique.
Cada rede de graduação dada é um subconjunto de todas as redes de graduação "mais

fina" que a dada. Mais precisamente: a rede de graduação $1/10^n$ é um subconjunto da rede de graduação $1/10^{n+k}$, para qualquer k inteiro positivo.

Exercício 130 -

Trabalhando na rede de graduação $1/10^{n+1}$, encontre o segmento cujos extremos são pontos consecutivos desta rede e, ademais, está contido no segmento $P(\frac{m}{10^n})P(\frac{m+1}{10^n})$, e possui o ponto $P(\frac{m+1}{10^n})$. Determine os extremos de tal segmento.

Exercício 131 -

Trabalhando na rede de graduação $1/10^{n+1}$, encontre o segmento cujos extremos são pontos consecutivos desta rede e, ademais, está contido no segmento $P(\frac{m}{10^n})P(\frac{m+1}{10^n})$, e possui o ponto $P(\frac{m}{10^n})$. Determine os extremos de tal segmento.

Exercício 132 -

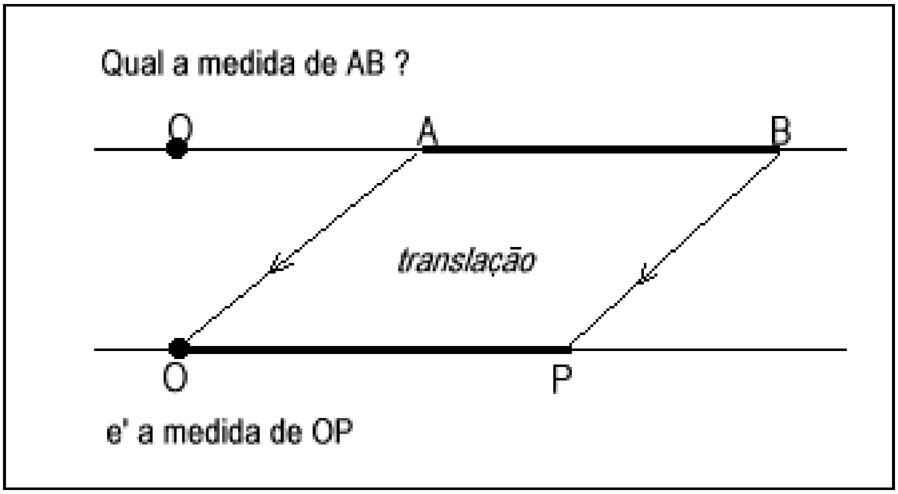
Mostre que a régua infinita é um conjunto denso, ou seja, que entre cada par de pontos graduados, digamos $P(\frac{m}{10^n})$ e $P(\frac{p}{10^q})$, existem infinitas marcações, isto é, infinitos pontos graduados.

6.4 Usando a régua infinita para medições diretas.

Como sempre, indiquemos por O a origem da régua infinita construída sobre uma reta euclidiana r. Temos, então, que medir um segmento de reta AB qualquer equivale a medir o segmento de reta OP, o qual é a translação de AB que leva a extremidade A para cima de O e a extremidade B para um ponto P de r, à direita de O. Pela congruência desses segmentos:

$$|AB| = |OP|.$$

Confira na figura a seguir.



Método da medição direta.

Dado qualquer segmento de reta AB, para determinarmos sua medida exata por meio da régua infinita, iniciamos achando o correspondente segmento congruente OP (conforme mostrado acima). Então, ocorrendo de P ser um ponto graduado da reta, digamos $P = P(m/10^n)$, teremos:

$$|AB| = |OP| = |OP\left(\frac{m}{10^n}\right)| = \frac{m}{10^n}\,.$$

Podemos dar utilidade muito maior a esse método se o combinarmos com a propriedade aditiva da medida, como mostram os seguintes exemplos.

Exemplo 6.6 -

Como $AB = P(4)P(6)$ *implica que* $OP(6) = OP(4) + AB$*, segue que* $|OP(6)| = |OP(4)| + |AB|$*, e assim:*

$$|AB| = |OP(6)| - |OP(4)| = 6 - 4 = 2.$$

Exemplo 6.7 -

Como temos:

$$AB = P\left(\frac{3}{100}\right)P\left(\frac{2}{10}\right) = P\left(\frac{3}{100}\right)P\left(\frac{20}{100}\right),$$

segue que:

$$OP\left(\frac{20}{100}\right) = OP\left(\frac{3}{100}\right) + AB \Rightarrow |AB| = \frac{20}{100} - \frac{3}{100} = \frac{17}{100}.$$

Vale a pena generalizarmos.

Teorema 6.8 -

Se um segmento de reta AB for congruente a um segmento da forma $P'P''$, onde tanto P' como P'' são pontos graduados da régua infinita, e onde o primeiro deles está à esquerda do segundo, então:

$$|AB| = |P'P''| = |OP''| - |OP'| = \frac{m}{10^n} - \frac{r}{10^s}, \text{ sendo } P' = P\left(\frac{m}{10^n}\right), P'' = P\left(\frac{r}{10^s}\right).$$

Prova:

Temos $OP'' = OP' + AB$, de modo que $|OP''| = |OP'| + |AB|$ e, assim:

$$|AB| = |OP''| - |OP'|.$$

CQD.

Teorema 6.9 (insuficiência do método direto de medição) -

Os números que expressam medidas exatas obtidas por medição direta com a régua infinita sempre são números racionais expressos por fração decimal. Como consequência, existem segmentos de reta cuja medida exata não pode ser obtida pelo método direto por meio da régua infinita. Com efeito, estes segmentos são:

- *todos os segmentos comensuráveis com a unidade, mas cuja medida é um número racional não representável por fração decimal;*
- *todos os segmentos de reta incomensuráveis com o segmento unitário.*

Prova:

É imediato percebermos que os resultados das medições, via método direto com a régua infinita, sempre serão racionais dados por frações decimais. Tendo-se isso em mente, fica imediato ver a validade do que é afirmado no teorema.

CQD.

Exemplo 6.10 -

O mais simples exemplo de segmento que não pode ser medido exatamente com a régua infinita é a terça parte do segmento unitário. Com efeito, esse é um segmento OP *tal que* $3OP = OU$*, de modo que* $|3OP| = 3|OP| = |OU| = 1$*, e então sua medida vale* $|OP| = 1/3$*. Contudo, esse valor não pode ser obtido com a régua, pois na fração* $1/3$*, o denominador não é fatorável apenas com potências de* 2 *e/ou* 5*, o que implica que* $1/3$ *não tem representação por fração decimal.*

Exercício 133 -

Determine as medidas $|OP(m/10)|$*,* $|OP(m/100)|, \dots, |OP(m/10^n)|$*, justificando sua resposta.*

Exercício 134 -

V ou F? Justifique.
Para qualquer $m \in \mathbb{N}$*,* $|P(m)P(m+1)| = 1$ *.*

Exercício 135 -

V ou F? Justifique.
Para qualquer $m \in \mathbb{N}$*,* $|P(\frac{m}{10})P(\frac{m+1}{10})| = 1$*.*

Exercício 136 -

Determine, justificando cuidadosamente, o valor da medida:

$$|P(\frac{m}{10^n})P(\frac{r}{10^s})|\,,$$

onde $m, n, r, s \in \mathbb{N}$*.*

Exercício 137 -

i). *Usando régua e compasso, como V. construiria um segmento* OP*, tal que* $3\,OP = 2\,OU$*?*
ii). *Mostre que tal segmento não pode ser medido exatamente pelo método direto.*

Exercício 138 -

i). Construa um segmento da forma OP, tal que $|OP| = 11/35$.

ii). Mostre que o ponto P construído em (i) não é um ponto graduado e que, consequentemente, o segmento OP não pode ser medido exatamente pelo método direto.

6.5 Usando a régua infinita para medições aproximadas.

Dado um segmento de reta, AB, diremos que

- todo segmento CD verificando $CD \subseteq AB$ é uma aproximação por falta de AB, e também que a medida $|CD|$ de CD é uma aproximação por falta da medida $|AB|$ de AB, pois teremos $|CD| \leqslant |AB|$;
- todo segmento CD verificando $AB \subseteq CD$ é uma aproximação por excesso de AB, e também que a medida $|CD|$ de CD é uma aproximação por excesso da medida $|AB|$ de AB, pois $|AB| \leqslant |CD|$.

  Sendo CD uma aproximação, por falta ou excesso, do segmento de reta AB, escreveremos:
$$|AB| \simeq |CD|\,.$$

A noção de aproximação é indissociável da de erro. Assim, na notacão acima, diremos que o erro de uma aproximação por falta (resp. por excesso) CD de AB é o segmento que precisamos acrescentar a CD (resp. retirar de CD) para obtermos AB. Também se costuma dizer que o erro de uma tal aproximação é a medida do respectivo segmento de falta ou excesso.

Na prática, o usual é ser impossível calcularmos o erro, e assim temos de nos contentar com uma cota ou estimativa da medida do erro.

Exemplo 6.11 -

Dizer "achar uma aproximação do segmento de reta AB com erro de cota *$0,01$" significa que queremos determinar uma aproximação (por falta ou por excesso) CD de AB, cujo erro tem medida $\leqslant 0,01$.*

Note que aí está incluída a possibilidade de acharmos um $CD = AB$, pois toda medida exata sempre é uma aproximada para qualquer cota que se escolha. Contudo, o usual é conseguirmos ou um $CD < AB$, ou um $CD > AB$.

Método da medição aproximada.

Dado qualquer segmento de reta AB, para encontrarmos sua medida com erro de cota $1/10^n$, inicialmente determinaremos o correspondente segmento congruente OP (conforme mostrado acima), de modo que $|AB| = |OP|$. A seguir, encontraremos os dois pontos graduados consecutivos – na rede de graduação $1/10^n$ – envolvendo o ponto P, de modo a termos:

$$OP\left(\frac{m}{10^n}\right) \subseteq OP \subseteq OP\left(\frac{m+1}{10^n}\right).$$

Feito isso, como vale:

$$\frac{m}{10^n} \leqslant |OP| \leqslant \frac{m+1}{10^n} = \frac{m}{10^n} + \frac{1}{10^n},$$

teremos que

- *uma aproximação por falta da medida de* AB será:

$$|AB| \simeq \frac{m}{10^n}, \text{ com erro } \leqslant \frac{1}{10^n};$$

- *uma aproximação por excesso da medida de* AB será:

$$|AB| \simeq \frac{m+1}{10^n}, \text{ com erro } \leqslant \frac{1}{10^n}.$$

Exemplo 6.12 -

Sendo AB a terça parte do segmento unitário, determinemos sua medida aproximada, com erro $\leqslant 0,001$.

Usando que $3|AB| = 1$, podemos escrever $0,999 \leqslant 3|AB| \leqslant 1,002$, de modo que $0,333 \leqslant |AB| \leqslant 0,334$, e então veremos que

$$|AB| \simeq 0,333\,, \textit{ com erro } \leqslant 0,001\,.$$

Uma vez fixada uma rede de graduação, deixando de lado as situações *excepcionais* em que P é um ponto graduado de tal rede, o usual é termos uma única medida por falta, e também uma única por excesso. No caso excepcional dos pontos graduados, teremos duas por falta e duas por excesso. Exemplifiquemos.

Na rede de graduação $1/10^2$, seja o segmento OP, onde $P = P(5/100)$. A relação

$$OP(4/100) \subseteq OP(5/100) \subseteq OP(5/100)$$

é interpretada como dizendo que $|OP| \simeq 0,04$ é uma aproximação por falta, com erro de cota $0,01$, e que $|OP| \simeq 0,05$ é uma aproximação por excesso, com erro de cota $0,01$.

Por outro lado, a relação:

$$OP(5/100) \subseteq OP(5/100) \subseteq OP(6/100)$$

diz que $|OP| \simeq 0,05$ é uma aproximação por falta, com erro de cota $0,01$, e que $|OP| \simeq 0,06$ é uma aproximação por excesso, com erro de cota $0,01$.

A não ser nos casos excepcionais em que o ponto P é um ponto graduado da rede de graduação $1/10^n$, a relação

$$OP\left(\frac{m}{10^n}\right) \subseteq OP \subseteq OP\left(\frac{m+1}{10^n}\right),$$

fica escrita como:

$$OP\left(\frac{m}{10^n}\right) \subset OP \subset OP\left(\frac{m+1}{10^n}\right),$$

o que implicará:

$$\left|OP\left(\frac{m}{10^n}\right)\right| < |OP| < \left|OP\left(\frac{m+1}{10^n}\right)\right|.$$

Observação 6.13 -

O fato de o método direto aproximado envolver o enquadramento

$$OP\left(\frac{m}{10^n}\right) \subseteq OP \subseteq OP\left(\frac{m+1}{10^n}\right)$$

e, assim

$$\left|OP\left(\frac{m}{10^n}\right)\right| \leqslant |OP| \leqslant \left|OP\left(\frac{m+1}{10^n}\right)\right|$$

deixa em aberto a possibilidade de uma dessas $\leqslant$ tornar-se uma $=$. Isso significa que o método direto aproximado generaliza o método direto exato.

Contudo, embora o método direto exato só possa produzir um resultado para cada segmento de reta medido, essa unicidade não ocorre com o método aproximado. Com efeito, sempre que P não for ponto graduado, teremos infinitos resultados para $|OP|$. Expliquemo-nos por meio de um exemplo, o do segmento AB que é um terço do segmento unitário, dando as seguintes aproximações (por falta):

$$
\begin{aligned}
&|AB| \simeq 0,333, \ \textit{com erro} \ \leqslant 0,001 \\
&|AB| \simeq 0,3333, \ \textit{com erro} \ \leqslant 0,0001\,; \ \textit{logo, também com erro} \leqslant 0,001 \\
&|AB| \simeq 0,33333, \ \textit{com erro} \ \leqslant 0,00001\,; \ \textit{logo, também com erro} \leqslant 0,001 \\
&\qquad \textit{etc., etc.}
\end{aligned}
$$

Teorema 6.14 -

O método da medição aproximada com a régua infinita é capaz de medir qualquer segmento de reta, qualquer que seja a cota de erro exigida.

Prova:

Dado AB, seja seu congruente da forma OP. Sendo a cota de erro dada correspondente à graduação $1/10^n$, basta observarmos que, pela propriedade arquimediana, terá de existir um número natural m, tal que:

$$OP\left(\frac{m}{10^n}\right) \subseteq OP \subset OP\left(\frac{m+1}{10^n}\right),$$

pois $OP(m/10^n) = m \cdot OP(1/10^n)$. CQD.

Exercício 139 -

i). Qual a menor cota de erro que podemos exigir na régua escolar? (Dizendo de outra maneira: como formular o teorema anterior para a régua escolar?)

ii). No Mundo Moderno usamos muitos mecanismos com peças que envolvem medidas que precisam ser obtidas com cota de erro bem menor do que 1 mm. Uma maneira de se conseguir isso envolve o uso de escalas auxiliares, como o nônio utilizado em paquímetros e outros instrumentos de medida. Pesquise sobre isso.

Exercício 140 -

Mostre que $0,3331$ *e* $0,3332$ *também são aproximações por falta da medida do segmento* $AB = 1/3\,OU$, *e que têm erro* $\leqslant 0,001$.

Exercício 141 -

Consideremos o segmento OP, *tal que* $3OP = 2OU$. *Pede-se determinar sua medida aproximada, com erro* $\leqslant 0,01$.

Exercício 142 -

Já foi pedido mostrar que é impossível que o método direto seja capaz de medir exatamente um segmento da forma OP *e tal que* $|OP| = 11/35$. *Contudo, mostre que podemos usar esse método para determinar sua medida aproximada, com erro* $\leqslant\ 0,001$.

Exercício 143 -

Denotemos por AB *a diagonal do quadrado de lado unitário.*

i). Explique detalhadamente por que esse segmento não pode ser medido exatamente pelo método direto via régua infinita.

ii). Determine uma medida aproximada dessa diagonal, com erro $\leqslant 0,1$.

iii). Determine uma medida aproximada dessa diagonal, com erro $\leqslant 0,01$.

6.6 Usando a régua infinita para medições iterativas.

O método direto é exato, mas tem o inconveniente de ser não ser capaz de produzir um resultado para a maioria dos segmentos de reta. Por outro lado, o método aproximado é capaz de medir qualquer segmento de reta, mas seu resultado não é, em geral, exato.

O método que passaremos a estudar, o método iterativo, é *exato e capaz de medir qualquer segmento de reta.* Ela baseia-se no fato que, com a aplicação repetida ou iterada do método direto aproximado, escolhendo redes de graduação cada vez mais finas, somos capazes de produzir medidas tão aproximadas quanto desejarmos de qualquer segmento dado. Com efeito, a essência do método iterativo é levar ao extremo, ao infinito, a repetição dessas medidas aproximadas. De uma maneira intuitiva e metafórica, o método iterativo pode ser visto como associando a cada medida um resultado "infinitamente aproximado".

Método da medição iterativa.

Dado qualquer segmento de reta AB:

α). Inicialmente, escolhendo uma régua infinita de origem O, encontramos sobre ela o segmento OP congruente a AB, de modo que $|AB| = |OP|$.

β). Em cada uma das redes de graduação da régua, determinamos dois pontos *consecutivos*, P' e P'', envolvendo P, obtendo assim:

$$OP' \subseteq OP \subseteq OP''.$$

Desse modo, obtemos uma sequência de infinitos pares constituídos por medidas aproximadas de OP, uma por falta e a outra por excesso, de cotas de erro sucessivamente $\leqslant 1,\ 1/10,$ $1/10^2, 1/10^3, \ldots$, e que podem ser escritos como:

$$\begin{gathered}
m \leqslant |OP| \leqslant m+1 \\
m, a_1 \leqslant |OP| \leqslant m, a_1\ + 1/10 \\
m, a_1 a_2 \leqslant |OP| \leqslant m, a_1 a_2\ + 1/10^2 \\
m, a_1 a_2 a_3 \leqslant |OP| \leqslant m, a_1 a_2 a_3\ + 1/10^3 \\
\cdots\cdots\cdots\cdots\cdots\cdots
\end{gathered}$$

γ). Diremos, finalmente, que a medida iterativa do segmento AB é expressa ou representada por

$$|AB| = m, a_1 a_2 a_3 \ldots .$$

Observe que, conforme é óbvio geometricamente, o item β faz com que as aproximações por falta sejam, sucessivamente, do tipo:
$m \to m, a_1 \to m, a_1 a_2 \to m, a_1 a_2 a_3 \to \cdots$; ou seja, nunca poderemos ter uma passagem do tipo, por exemplo: $m, a_1 a_2 \to m, a_1 b_2 a_3$, com $a_2 \neq b_2$.

Exemplo 6.15 -

Tomemos o caso de um segmento de reta AB, tal que OP seja um terço do segmento unitário da régua infinita. Explorando que $3\,|OP| = 1$, obtemos então:

$$
\begin{gathered}
0 = |OP(0)| \leqslant |OP| \leqslant |OP(1)| = 1 \\
0,3 = |OP(0,3)| \leqslant |OP| \leqslant |OP(0,4)| = 0,4 \\
0,33 = |OP(0,33)| \leqslant |OP| \leqslant |OP(0,34)| = 0,34 \\
0,333 = |OP(0,333)| \leqslant |OP| \leqslant |OP(0,334)| = 0,334 \\
0,3333 = |OP(0,3333)| \leqslant |OP| \leqslant |OP(0,3334)| = 0,3334 \\
\cdots\cdots\cdots\cdots\cdots\cdots
\end{gathered}
$$

de modo que temos: $|AB| = |OP| = 0,333\,333\ \ldots$ *.*

Observação 6.16 -

Podemos ver o método da medição iterativa como uma generalização do da medida aproximada, na medida que basta "abortarmos" a iteração – quando se chega na rede de graduação $1/10^n$ *– para obtermos tanto uma aproximação por falta como uma por excesso, com erro* $\leqslant 1/10^n$*. Adiante, também investigaremos sua relação com o método direto.*

Teorema 6.17 -

Todo segmento de reta admite uma medida iterativa.

Prova:

Escolhendo uma régua infinita de origem O, dado um segmento de reta qualquer, AB, obviamente podemos determinar sobre ela um único segmento OP congruente a AB, de modo que $|AB| = |OP|$; ademais, obviamente, em cada uma das redes de graduação da régua, podemos determinar um par de pontos consecutivos, P' e P'', envolvendo P, obtendo assim:

$$OP' \subseteq OP \subseteq OP''.$$

Desse modo, é imediato que sempre são executáveis as etapas da definição da medida iterativa, qualquer que seja o segmento dado AB.

CQD.

Crucial, sob o ponto de vista de medidas, é garantirmos que somente segmentos de reta congruentes podem ter a mesma medida. Isso é confirmado pelo teorema seguinte.

Teorema 6.18 -

A medida iterativa somente repete resultado para segmentos congruentes. Ou seja, se dois segmentos de reta têm a mesma medida iterativa, então eles serão congruentes.

Prova:

Basta mostrarmos que se OP e OQ têm a mesma medida iterativa, então $P = Q$. Ora, sendo $m, a_1a_2a_3\ldots$ uma medida iterativa desses segmentos, teremos:

$$\begin{gathered}
OP(m) \subseteq OP\,,\; OQ \subseteq OP(m+1)\\
OP(m+\frac{a_1}{10}) \subseteq OP\,,\; OQ \subseteq OP(m+\frac{1+a_1}{10})\\
OP(m+\frac{a_1}{10}+\frac{a_2}{10^2}) \subseteq OP\,,\; OQ \subseteq OP(m+\frac{a_1}{10}+\frac{1+a_2}{10^2})\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{gathered}$$

de onde é fácil percebermos que teremos uma sequência de segmentos de reta

$$P(m)P(m+1) \supset P(m,a_1)P(m,a_1+\frac{1}{10}) \supset P(m,a_1a_2)P(m,a_1a_2+\frac{1}{10^2}) \supset \cdots$$

encaixante, evanescente e tal que os pontos P e Q estão em todos esses segmentos. Logo, pelo Postulado da Continuidade da Reta Euclidiana, segue que $P = Q$.

CQD.

Exercício 144 -

Prove detalhadamente as duas últimas frases da prova anterior.

Prosseguimos com mais exemplos de medidas iterativas, agora insistindo no caso dos segmentos OP, onde P é um ponto graduado da régua infinita.

Exemplo 6.19 -

Consideremos agora o caso em que o segmento OP tem como P o ponto graduado $P = P(0,75) = P(75/10^2)$. É fácil notarmos que podemos construir duas sequências de segmentos envolventes.

– *Primeira sequência:*

$$
\begin{gathered}
OP(0) \subseteq OP \subseteq OP(1) \\
OP(0,7) \subseteq OP \subseteq OP(0,8) \\
OP(0,74) \subseteq OP \subseteq OP(0,75) \\
OP(0,749) \subseteq OP \subseteq OP(0,750) \\
OP(0,7499) \subseteq OP \subseteq OP(0,7500) \\
OP(0,74999) \subseteq OP \subseteq OP(0,75000) \\
\dots\dots\dots\dots\dots\dots
\end{gathered}
$$

do que resulta a medida iterativa: $|OP(0,75)| = 0,749\,999\ldots$.

– *Segunda sequência:*

$$
\begin{gathered}
OP(0) \subseteq OP \subseteq OP(1) \\
OP(0,7) \subseteq OP \subseteq OP(0,8) \\
OP(0,75) \subseteq OP \subseteq OP(0,76) \\
OP(0,750) \subseteq OP \subseteq OP(0,751) \\
OP(0,7500) \subseteq OP \subseteq OP(0,7501) \\
OP(0,75000) \subseteq OP \subseteq OP(0,75001) \\
\dots\dots\dots\dots\dots
\end{gathered}
$$

do que resulta a medida iterativa: $|OP(0,75)| = 0,750\,000\ldots$.

Note que os segmentos envolventes eram os mesmos nos dois casos, até a primeira rede *em que uma das extremidades, P' ou P'', coincidiu com P.*

Exemplo 6.20 -

Consideremos agora o caso em que o segmento AB é o próprio segmento unitário da régua infinita, de modo que OP tem como P o ponto graduado $P = P(1)$. Neste caso, também podemos construir duas sequências de segmentos envolventes.

– *Primeira sequência:*

$$
\begin{gathered}
OP(0) \subseteq OP \subseteq OP(1) \\
OP(0,9) \subseteq OP \subseteq OP(1,0) \\
OP(0,99) \subseteq OP \subseteq OP(1,00) \\
OP(0,999) \subseteq OP \subseteq OP(1,000) \\
OP(0,9999) \subseteq OP \subseteq OP(1,0000) \\
OP(0,99999) \subseteq OP \subseteq OP(1,00000) \\
\dots\dots\dots\dots\dots\dots
\end{gathered}
$$

do que resulta a medida iterativa: $|OP(1)| = 0,999\,999\ \ldots$.

– *Segunda sequência:*

$$\begin{array}{c} OP(1) \subseteq OP \subseteq OP(2) \\ OP(1,0) \subseteq OP \subseteq OP(1,1) \\ OP(1,00) \subseteq OP \subseteq OP(1,01) \\ OP(1,000) \subseteq OP \subseteq OP(1,001) \\ OP(1,0000) \subseteq OP \subseteq OP(1,0001) \\ OP(1,00000) \subseteq OP \subseteq OP(1,00001) \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

do que resulta a medida iterativa: $|OP(1)| = 1,000\,000\ \ldots$.

Exemplo 6.21 -

Consideremos agora o caso excepcionalíssimo onde o segmento AB *se reduz a um único ponto, de modo que* OP *tem* $P = O$*. Nesse caso, podemos construir somente uma sequência de segmentos envolventes:*

$$\begin{array}{c} OP(0) \subseteq OP \subseteq OP(1) \\ OP(0,0) \subseteq OP \subseteq OP(0,1) \\ OP(0,00) \subseteq OP \subseteq OP(0,01) \\ OP(0,000) \subseteq OP \subseteq OP(0,001) \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

do que resulta a medida iterativa: $|OO| = 0,000\,000\ \ldots$.

Exercício 145 -

Determine todas as medidas iterativas possíveis para o caso do segmento de reta: $OP = OP(5,43)$.

Exercício 146 -

Escreva todas as possíveis sequências de intervalos envolventes, e deduza a respectiva medida iterativa, para o caso dos segmentos de reta:

i). $OP = OP(3,95)$;

ii). $OP = OP(3,59)$.

Observação 6.22 -

O resultado de toda medição direta ou aproximada é um número racional, enquanto que o de uma medida iterativa é uma lista da forma

$$m, a_1 a_2 a_3 \ldots \,,$$

onde m é um inteiro $\geqslant 0$, e os a_n são dígitos.

Passaremos a chamar toda lista deste tipo de lista de dígitos*, embora m não seja necessariamente um dígito. Faremos este abuso de linguagem para tornar a leitura mais leve e porque toda lista desse tipo pode ser transformada numa legítima lista de dígitos, $b_M \ldots b_1 b_0, a_1 a_2 \ldots$, onde $m = b_M \ldots b_1 b_0$ é a expansão decimal do inteiro m.*

Uma das tarefas que teremos pela frente é elucidar a natureza de tais listas de dígitos, mostrar que elas têm um carácter numérico legítimo e que englobam as expansões decimais dos números racionais.

Definição 6.23 -

Chamaremos de lista 9-terminante *a toda lista de dígitos da forma $m, 999\,999\ldots$ ou da forma $m, a_1 a_2 a_3 \ldots a_n 999\ldots$, onde $a_n \neq 9$. Por sua vez, lista* 0-terminante *é toda lista da forma $m, 000\,000\ldots$ ou da forma $m, a_1 a_2 a_3 \ldots a_n 000\ldots$, onde $a_n \neq 0$.*

Uma medida iterativa será dita 9-terminante (resp. 0-terminante) se a lista que expressa essa medida for 9-terminante (resp. 0-terminante).

Exemplo 6.24 -

Para a adequada compreensão do que se segue, é essencial sempre termos em vista o caso do segmento unitário, o qual tem medida iterativa 9-terminante dada por $|OU| = 0,999\,999\ldots$ e medida 0-terminante de valor $|OU| = 1,000\,000\ldots$

Por sua vez, um protótipo de segmento de reta que só tem medida não 9-terminante é um terço do segmento unitário, cuja medida iterativa é $0,333\,333\ldots$.

> Temos como tarefas imediatas: caracterizar os segmentos que têm mais de uma medida iterativa, e descrever/relacionar os respectivos resultados.

O teorema a seguir mostra que os exemplos acima são representativos de todas as possibilidades de medidas iterativas:

Teorema 6.25 -

Todo segmento de reta OP, onde P é um ponto à direita da origem da régua infinita, tem medida iterativa. Mais detalhadamente, temos as seguintes alternativas para essa medida:

a). se P não for ponto graduado da régua, só haverá um resultado para a medida iterativa de OP e ele é uma lista que não é 0-terminante e nem 9-terminante;

b). se P for ponto graduado da régua, teremos exatamente dois resultados para a medida iterativa de OP: um é uma medida 0-terminante, e o outro uma medida 9-terminante.

Prova:

Para (a):

basta observarmos que o fato de P não ser ponto graduado implica termos, para cada uma das redes de graduação, que só existem dois pontos consecutivos, P' e P'', envolvendo P, e que valem as desigualdades estritas:

$$|OP'| < |OP| < |OP''| .$$

Para (b):

agora, existe um menor k e um menor m tal que $P = P(m/10^k)$. A partir desse ponto (ou seja, para $n \geqslant k$), e de modo totalmente semelhante ao que ocorreu no Exemplo 6.19, podemos escolher continuarmos ou com intervalos envolventes da forma

$$OP' < OP = OP'',$$

que darão uma medida iterativa da forma 9-terminante, ou com intervalos da forma

$$OP' = OP < OP'',$$

que darão uma medida iterativa da forma 0-terminante. Observado isso, fica imediato concluirmos. CQD.

Ao leitor que estranhou o fato de eventualmente ocorrer que um mesmo segmento "tenha" (seja representado por) duas medidas iterativas, adiantamos que este fato deve ser visto como análogo ao de um mesmo número racional poder ser representado por mais de uma – na verdade, infinitas – frações ordinárias. Coloquemos isso numa definição:

Definição 6.26 -

Dizemos que duas medidas iterativas são equivalentes se elas expressarem (representarem) a medida de um mesmo segmento de reta.

Exemplo 6.27 -

Pelo que vimos acima, as medidas $0,999\,999\ldots$ *e* $1,000\,000\ldots$ *são equivalentes. Isto também é o caso de* $0,749\,999\ldots$ *e* $0,750\,000\ldots$ *.*

Passemos a elucidar a relação entre as medidas iterativas que constituem um par equivalente.

Teorema 6.28 -

Quando a medida iterativa de um segmento de reta AB resultar em duas listas, estas terão ou a forma:

$$\begin{aligned} |AB| &= m,000\,000\ldots \\ |AB| &= M,999\,999\ldots \\ &\quad (\textit{onde o inteiro } M = m-1)\,, \end{aligned}$$

ou a forma:

$$\begin{aligned} |AB| &= m,a_1a_2a_3\ldots a_n000\ldots \\ |AB| &= m,a_1a_2a_3\ldots a_n'999\ldots \\ &\quad (\textit{onde os dígitos } a_n \neq 0,\ a_n' = a_n - 1 \leqslant 8)\,. \end{aligned}$$

Prova:

Pelo Teorema 6.25, já sabemos que a ocorrência de par de listas como resultado de uma medição iterativa ocorre quando, e somente quando, o segmento de reta for congruente a um OP com P ponto graduado da régua infinita e distinto da origem. Assim, tudo o que resta fazer é mostrar que, em tais casos, o par de listas tem a forma explicitada no enunciado do presente teorema. Dividiremos a prova em dois casos: P é ponto da rede unitária, e P não é ponto da rede unitária.

– Caso em que P é ponto da rede unitária.

Temos que $P = P(m)$, onde m é um inteiro $\geqslant 1$. Assim sendo, de modo absolutamente análogo ao que ocorreu no caso da medida iterativa do segmento unitário (vide Exemplo 6.20), temos duas famílias de segmentos envolventes.

– Primeira sequência:

$$\begin{aligned}
OP(m) &\subseteq OP \subseteq OP(m+1)\\
OP(m,0) &\subseteq OP \subseteq OP(m,1)\\
OP(m,00) &\subseteq OP \subseteq OP(m,01)\\
OP(m,000) &\subseteq OP \subseteq OP(m,001)\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

do que resulta a medida iterativa: $|OP(m)| = m{,}000\,000\ \ldots$.

– Segunda sequência:

$$\begin{aligned}
OP(m-1) &\subseteq OP \subseteq OP(m)\\
OP(m-1,9) &\subseteq OP \subseteq OP(m,0)\\
OP(m-1,99) &\subseteq OP \subseteq OP(m,00)\\
OP(m-1,999) &\subseteq OP \subseteq OP(m,000)\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

do que resulta a medida iterativa: $|OP(m)| = m-1{,}999\,999\ \ldots$.

– Caso em que P é ponto graduado, mas não da rede unitária.

Agora, estamos num caso análogo ao do Exemplo 6.19. Nosso ponto P é graduado e está estritamente entre dois pontos da rede unitária da régua infinita, digamos $P(m)$ e $P(m+1)$. Isto significa que podemos escrevê-lo como: $P = P(m, a_1a_2a_3\ldots a_n)$, onde os a_k são dígitos e o $a_n \neq 0$. Assim sendo, e tendo em vista o que foi feito naquele exemplo, bem como no Exercício 146, notamos que temos duas possibilidades para o par de sequências envolventes, dependendo de termos $a_n \neq 9$ ou $a_n = 9$.

Inicialmente, vejamos o caso mais fácil, aquele em que $a_n \neq 9$.

– Primeira sequência:

$$\begin{aligned}
OP(m) &\subseteq OP \subseteq OP(m+1)\\
&\cdots\cdots\cdots\\
OP(m, a_1a_2\ldots a_n') &\subseteq OP \subseteq OP(m, a_1a_2\ldots a_n)\\
OP(m, a_1a_2\ldots a_n'9) &\subseteq OP \subseteq OP(m, a_1a_2\ldots a_n0)\\
OP(m, a_1a_2\ldots a_n'99) &\subseteq OP \subseteq OP(m, a_1a_2\ldots a_n00)\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

onde $a_n' = a_n - 1$, do que resulta a medida iterativa: $|OP(m)| = m, a_1a_2\ldots a_n'\,999\ldots$.

– Segunda sequência:

$$
\begin{gathered}
OP(m) \subseteq OP \subseteq OP(m+1) \\
\cdots\cdots\cdots\cdots\cdot \\
OP(m, a_1a_2 \ldots a_n) \subseteq OP \subseteq OP(m, a_1a_2 \ldots a_n'') \\
OP(m, a_1a_2 \ldots a_n0) \subseteq OP \subseteq OP(m, a_1a_2 \ldots a_n1) \\
OP(m, a_1a_2 \ldots a_n00) \subseteq OP \subseteq OP(m, a_1a_2 \ldots a_n01) \\
OP(m, a_1a_2 \ldots a_n000) \subseteq OP \subseteq OP(m, a_1a_2 \ldots a_n001) \\
\cdots\cdots\cdots\cdots\cdots\cdot
\end{gathered}
$$

onde $a_n'' = 1+a_n$, do que resulta a medida iterativa: $|OP(m)| = m, a_1a_2 \ldots a_n\,000\ldots$.

Finalmente, vejamos o caso em que $a_n = 9$.

– Primeira sequência:

é igual aos casos $a_n \neq 9$, e como tal, obtemos a medida iterativa: $|OP(m)| = m, a_1a_2 \ldots a_n'\,999\ldots$.

– Segunda sequência:

$$
\begin{gathered}
OP(m) \subseteq OP \subseteq OP(m+1) \\
\cdots\cdots\cdots\cdots\cdot \\
OP(m, a_1a_2 \ldots a_n) \subseteq OP \subseteq OP(m, b_1b_2 \ldots b_n) \\
OP(m, a_1a_2 \ldots a_n0) \subseteq OP \subseteq OP(m, a_1a_2 \ldots a_n1) \\
OP(m, a_1a_2 \ldots a_n00) \subseteq OP \subseteq OP(m, a_1a_2 \ldots a_n01) \\
OP(m, a_1a_2 \ldots a_n000) \subseteq OP \subseteq OP(m, a_1a_2 \ldots a_n001) \\
\cdots\cdots\cdots\cdots\cdots\cdot
\end{gathered}
$$

onde $b_1b_2 \ldots b_n = 1 + a_1a_2 \ldots a_n$ (note que $a_1a_2 \ldots a_n \neq 99\ldots9$), do que resulta a medida iterativa: $|OP(m)| = m, a_1a_2 \ldots a_n\,000\ldots$.

CQD.

Exercício 147 -

Determine a medida iterativa do segmento de reta $OP = OP(3, 599)$, e use seus resultados numéricos para conferir a notação usada na prova do teorema anterior.

Resumo.

- Existem três categorias disjuntas de segmentos de reta: ordinários, excepcionais e excepcionalíssimos.
- Os segmentos ordinários são os AB congruentes a um segmento OP, com P ponto não graduado da régua infinita.
  O método iterativo expressa sua medida como uma única lista, e ela não é nem 9-terminante e nem 0-terminante.
- Os segmentos excepcionais são os AB não reduzidos a um único ponto e congruentes a um segmento OP, com P ponto graduado.
  O método iterativo expressa a medida desses segmentos por um par de listas: uma 9-terminante e a outra 0-terminante.
- Os segmentos excepcionalíssimos são os AB reduzidos a um único ponto, ou seja, congruentes a OO. Sua medida iterativa é a lista 0-terminante: $0,000\,000\ldots$.

Em particular:

- todo segmento de reta tem uma medida iterativa não 9-terminante.

Exercício 148 -

Suponhamos que a lista $13,01\,001\,0001\,00001\ldots$ *seja o resultado da medida iterativa de um certo segmento de reta. Pede-se obter números racionais que aproximem essa medida com erro:*

i). $\leqslant 1,\ 1/10,\ 1/100,\ 1/1000$

ii). $< 1,\ 1/10,\ 1/100,\ 1/1000$

iii). $\leqslant 1/25$

iv). $< 1/25$

Exercício 149 -

Sejam AB *e* CD *segmentos tais que* $|AB| = 2,43\ldots$ *e* $|CD| = 2,44\ldots$. *Prove que*

$$|AB| = |CD| \iff |AB| = 2,439\,999\ldots \ \textit{e}\ |CD| = 2,440\,000\ldots .$$

Resumo desta seção.

Apresentamos um terceiro método de medida de segmentos de reta, AB, que denominamos *método iterativo*.

- O mesmo pode ser visto como uma aplicação repetida ad infinitum do método aproximado. Dessa forma, *ele é capaz de medir exatamente qualquer segmento de reta*.
- *A unicidade* da representação da medida ocorre quando, e somente quando, ou o segmento de reta AB é congruente a um OP cuja extremidade P não seja ponto graduado da régua decimal, ou AB se reduz a um único ponto.
- A medida obtida pelo método iterativo é *expressa* por:
  - ◇ ou uma única lista de dígitos, a qual sempre é não 9- terminante
    (isso é o resultado usual, e ocorre nos casos em que o segmento a medir não é congruente a um segmento OP, com P ponto graduado e à direita da origem da régua infinita);
  - ◇ ou um par de listas de dígitos, uma das quais é 9-terminante e a outra é 0-terminante
    (isso ocorre só excepcionalmente).

6.7 Os números reais absolutos

Teorema 6.29 -

Toda medida de segmento de reta é uma lista de dígitos e, reciprocamente, toda lista de dígitos é a medida de algum segmento de reta.

Prova:

Pelo fato que todo segmento de reta tem medida iterativa, segue-se a primeira parte do enunciado. Resta provar a recíproca. Para tal, dada qualquer lista de dígitos, $m, a_1a_2a_3\ldots$, iniciamos observando que a mesma define a seguinte sequência de segmentos sobre a régua infinita:

$$P(m)P(m+1) \supset P(m,a_1)P(m,a_1+\frac{1}{10}) \supset P(m,a_1a_2)P(m,a_1a_2+\frac{1}{10^2}) \supset \cdots,$$

a qual é imediato se constatar que é encaixante e evanescente. Logo, pelo Postulado da Continuidade da Reta Euclidiana, segue que existe exatamente um ponto P da reta comum a todos eles. É igualmente imediato constatarmos que a medida iterativa do segmento de reta OP, assim determinado, é precisamente a lista dada.

CQD.

Com esse teorema, chegamos a um ponto crítico da caminhada que viemos percorrendo neste texto. Estamos para introduzir uma das noções mais importantes e básicas da Matemática: a de número real absoluto.

Definição 6.30 . -

O conjunto dos números reais absolutos é o conjunto de todas as listas de dígitos, ou equivalentemente:
é o conjunto de todas as medidas de segmentos de reta.

Isso desde que seja convencionado que essas listas estão submetidas ao seguinte critério de igualdade numérica: duas listas serão consideradas como iguais quando, e somente quando, elas forem a medida iterativa de um mesmo segmento de reta.

Essa definição deve ser entendida como dizendo que os números reais absolutos são *representados* por listas de dígitos, e também dizendo quando duas dessas representações serão consideradas como iguais (ou equivalentes). Não deixe de notar, ademais, que é o Teorema 6.29 que nos permite verificar a igualdade ou não, passando de listas para medidas.

Exemplo 6.31 -

O segmento de reta que é um terço do segmento unitário tem como medida iterativa o número real absoluto de representação única: $0,333\,333\ldots$.
Por sua vez, a medida iterativa do segmento unitário é o número real absoluto que tem as representações $0,999\,999\ldots$ *e* $1,000\,000\ldots$, *o que nos permite escrever:*

$$1,000\,000\ldots = 0,999\,999\ldots = |OU|\,.$$

Observação 6.32 -

Tendo em vista os Teoremas 6.25 e 6.28, podemos dividir os números reais absolutos em três tipos:

- *o número representado por* $0,\,000\ldots$ *;*
- *os números reais absolutos representados por exatamente uma dentre as infinitas possíveis listas de dígitos que não são nem 9-terminantes e nem 0-terminantes;*
- *os números reais absolutos que têm exatamente duas representações, as quais constituem qualquer um dos possíveis pares de listas que tem a forma*

$$m,000\,000\ldots = M,999\,999\ldots\ (\textit{onde } M = m-1)\,,$$

ou a forma

$$m,a_1a_2a_3\ldots a_n000\ldots = m,a_1a_2a_3\ldots a_n'999\ldots\ (\textit{onde } a_n \neq 0,\ a_n' = a_n - 1 \leqslant 8)\,.$$

Teorema 6.33 (solução do problema da medida) -

Fixada uma régua infinita:

i). a todo segmento da reta euclidiana, o método de medida iterativa associa exatamente um número real absoluto como medida exata de seu comprimento;

ii). reciprocamente, para cada número real absoluto, pode-se determinar um segmento de reta cujo comprimento é esse número; além disso, todos os segmentos de reta que admitem esse número como medida são congruentes.

Prova:

Para (i):

a afirmação (i) é uma mera transcrição da definição de real absoluto e de seu critério de igualdade.

Para (ii):

todo número real absoluto, pela definição, é a medida iterativa – ou seja, uma representação – do comprimento de um segmento de reta. Por outro lado, se dois segmentos de reta tiverem a mesma medida, eles têm de ser congruentes, como decorre do Postulado do Contínuo, por meio do do Teorema 6.18. CQD.

É possível atribuirmos um significado numérico aos reais absolutos?

Sim, pois:

i). estão associados diretamente a quantidades: as medidas iterativas de segmentos de reta;
ii). podem ser somados e multiplicados, bem como estão submetidos a uma relação de ordem, conforme veremos no próximo capítulo.

Para reforçar a atribuição de carácter numérico aos reais absolutos, mostremos que eles incluem ou generalizam os números racionais absolutos.

Teorema 6.34 -

Todo número racional absoluto pode ser identificado naturalmente com exatamente um número real absoluto. Essa associação deve ser entendida do seguinte modo:

> *fixada uma régua infinita, dado um número racional representado pela fração a/b, a ele associamos o segmento de reta $OP = \frac{a}{b}OU$ e determinemos sua medida iterativa, não 9-terminante; então, a_n é o $n-$ésimo dígito dessa medida iterativa de OP, se e só se a_n é o $n-$ésimo dígito da expansão decimal do número racional a/b.*

Portanto, podemos escrever, sem ambiguidade de interpretação:

$$\frac{a}{b} = |OP| = m, a_1a_2a_3 \ldots a_n \ldots \ .$$

Prova:

(Para o rápido entendimento do raciocínio envolvido nesta demonstração, recomendamos que o leitor revise os Exemplos 6.19 e 6.15).

Se a expansão decimal de a/b é $0, a_1a_2a_3\ldots$, isto significa que a mesma foi produzida pela seguinte sequência de divisões euclidianas:

$$
\begin{aligned}
10a =& ba_1 + r_1\,, \text{ com } 0 \leqslant r_1 < b\\
10r_1 =& ba_2 + r_2\,, \text{ com } 0 \leqslant r_2 < b\\
10r_2 =& ba_3 + r_3\,, \text{ com } 0 \leqslant r_3 < b\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

de onde saem:

$$
\begin{aligned}
\frac{a}{b} =& \frac{a_1}{10} + \frac{r_1}{10b}\\
\frac{r_1}{10b} =& \frac{a_2}{100} + \frac{r_2}{100b}\\
\frac{r_2}{100b} =& \frac{a_3}{1000} + \frac{r_3}{1000b}\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

Ora, usando que $0 \leqslant r_1, r_2, \ldots < b$, podemos reescrever isso como:

$$
\begin{aligned}
0 \leqslant& \frac{a}{b} < 1\\
\frac{a_1}{10} \leqslant& \frac{a}{b} < \frac{a_1}{10} + \frac{1}{10}\\
\frac{a_1}{10} + \frac{a_2}{100} \leqslant& \frac{a}{b} < \frac{a_1}{10} + \frac{a_2}{100} + \frac{1}{100}\\
\frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} \leqslant& \frac{a}{b} < \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \frac{1}{1000}\\
&\ldots\ldots\ldots\ldots
\end{aligned}
$$

Em termos de segmentos envolventes de $OP = \frac{a}{b}\,OU$, estas desigualdades são expressas como:

$$OP(0) \subseteq OP \subset OP(1)$$

$$OP(\frac{a_1}{10}) \subseteq OP \subset OP(\frac{a_1}{10} + \frac{1}{10})$$

$$OP(\frac{a_1}{10} + \frac{a_2}{10^2}) \subseteq OP \subset OP(\frac{a_1}{10} + \frac{a_2}{10^2} + \frac{1}{10^2})$$
$$\dots\dots\dots\dots\dots$$

Assim, vemos que a expansão decimal de a/b determina uma sequência de intervalos envolventes de $OP = \frac{a}{b}OU$, do tipo

$$OP' \leqslant OP < OP''$$

e tais que – em cada rede de graduação – os pontos P' e P'' são consecutivos e à distância, respectivamente, 1, $1/10$, $1/10^2$, $\dots$. Disso, e do enunciado e demonstração do Teorema 6.25, segue que a medida iterativa não 9-terminante do segmento $OP(a/b)$ é precisamente tal expansão decimal.

CQD.

Exemplo 6.35 -

No caso do segmento de reta OP que é a terça parte do segmento unitário, $OP = \frac{1}{3}OU$, temos:

$$\frac{1}{3} = |OP| = 0,\, 333\,333\dots\ ,$$

sendo que a primeira igualdade expressa a medida de OP, obtida pela Proposição 6.2, enquanto que podemos ver a segunda como expressando a medida iterativa de OP. O teorema acima está dizendo que $0,\, 333\,333\dots$ também tem de ser a expansão decimal de $1/3$, o que já sabemos ser realmente verdadeiro do capítulo anterior.

Exemplo 6.36 -

No caso do segmento de reta OP, onde P é o ponto graduado $P(0,75)$, podemos confirmar diretamente o teorema, pois valem as igualdades:

$$0,75 = 0,750 = 0,7500 = \dots = |OP(0,75)| = 0,\, 750\,000\dots\ ,$$

sendo que a última igualdade é dada pela medida iterativa.

Exemplo 6.37 -

No caso do segmento unitário, temos:

$$1 = |OU| = 1,\, 000\,000\ldots = 0,\, 999\,999\ldots\,,$$

onde as duas primeiras igualdades referem-se à igualdade da medida direta e da medida iterativa 0-terminante do segmento OU, enquanto que a terceira refere-se à equivalência dos resultados da medição iterativa.

Exercício 150 -

Seja OP o segmento de reta cuja medida iterativa é a lista

$$3,2245245245245\ldots. \tag{6.1}$$

Prove que

$$9990\, OP = 32213\, OU\,.$$

Exercício 151 -

Considere o segmento OQ obtido pela divisão de $7\,OP(23/10)$ em oito partes iguais, ou seja: $8\,OQ = 7\,OP(2,3)$. Determine a medida iterativa de OQ.

Exercício 152 -

A rigor, a prova do teorema anterior tratou apenas dos racionais absolutos de expansão decimal do tipo $a/b = 0,\, a_1a_2a_3\ldots$. Pede-se fazer a prova para o caso geral $a/b = m,\, a_1a_2a_3\ldots$, onde m é um inteiro positivo.

Exercício 153 -

Fixada uma régua infinita de origem O e segmento unitário OU, podemos dizer que –se a medida iterativa de um segmento de reta OP for uma lista não 9-terminante– teremos $OP = \frac{a}{b}\,OU$, onde a/b é o número racional que tem como expansão decimal a lista dada.

Observação 6.38 -

Podemos ver o exercício anterior e o Teorema 6.34 como dizendo que podemos ver o método iterativo como uma generalização do método direto, e o sentido exato com que isto deve ser visto.

É conveniente resumirmos os pontos chaves do que foi feito:

- O conjunto dos números reais absolutos é o conjunto das listas do tipo $m, a_1a_2...$, onde m é um inteiro não negativo e os a_n são dígitos, para $n = 1, 2, ...$.
  É essencial que sempre tenhamos em mente que:
  - esses números estão associados ao processo de medição iterativa dos segmentos da reta euclidiana
  - dois números reais absolutos são considerados iguais se estiverem medindo segmentos de reta congruentes (representam medidas iterativas de segmentos congruentes). É devido a isso que escrevemos coisas como: $1,0000\ldots = 0,9999\ldots$.
- Todo número racional absoluto pode ser visto como um número real absoluto (vide Teorema 6.34).

Como existem listas de dígitos que não são periódicas, pelo Teorema 6.29 elas representam números reais absolutos e estes não podem ser números racionais. A definição a seguir dá uma denominação para os mesmos:

Definição 6.39 -

Número irracional absoluto é todo número real absoluto que pode ser representado por uma lista de dígitos não periódica.

Exemplo 6.40 -

Explicitando listas de dígitos que garantidamente não são periódicas, mostremos que efetivamente existem números irracionais:

$$0,10\,100\,1000\,10000\,100000\ldots$$
$$0,012\,01212\,0121212\ \ldots$$
$$0,1010010000001000000000000010\ldots \qquad (\textit{ note que envolve fatorial }).$$

Teorema 6.41 -

Todo número irracional absoluto é representado por apenas uma lista de dígitos (e a mesma não é periódica).

Prova:

Pela Observação 6.28, das três possibilidades para o resultado de medida de segmentos de reta, a única compatível com lista não periódica é a de lista única.

CQD.

Corolário 6.42 -

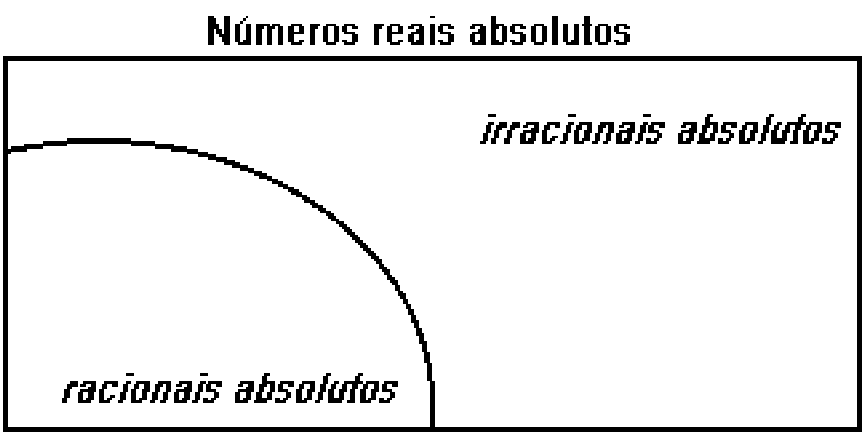
Todo número real absoluto ou é irracional, ou é racional.

Prova:

Já sabemos que existem tanto números racionais, como irracionais absolutos. Logo, tudo o que resta fazer é provar que é impossível um número real absoluto ser tanto racional, como irracional.

Ora, pelo teorema, todo irracional é representado por apenas uma lista e ela não é periódica; como tal, não havendo nenhuma possibilidade de esse número ter uma representação por lista periódica, ele não pode ser racional.

CQD.



Exemplo 6.43 -

Fixada uma régua infinita,

> *um segmento de reta é incomensurável com a unidade se, e só se, ele tiver como medida iterativa um número real absoluto irracional.*

Tendo em vista o teorema anterior, isso equivale a afirmar que um segmento de reta é comensurável com a unidade se, e só, se ele tiver como medida um número racional absoluto.

Com efeito, denotando o segmento unitário da régua por OU *:*

– sendo AB *um segmento comensurável com a unidade, temos que existem inteiros* m *e* n*, tais que* $m\,AB = n\,OU$*; disso segue que*

$$|AB| = |\frac{m}{n}\,OU| = \frac{m}{n} = \textit{ racional absoluto}\,;$$

– sendo $|AB| = m/n$*, como* $|m/n\,OU| = m/n$*, segue que* AB *é congruente a* $m/n\,OU$*, ou seja,* $m\,AB = n\,OU$*.*

Exemplo 6.44 -

Dado um quadrado de lado qualquer, tomemos uma régua infinita que tem como segmento unitário o lado deste quadrado. Da prova do Teorema 6.5, sabemos que a respectiva diagonal é incomensurável com o lado; de modo que, medindo tal diagonal com essa régua, obteremos como resultado um número irracional absoluto.

Exercício 154 -

Como fica a medida da diagonal do quadrado do exemplo anterior se tomarmos uma régua qualquer?

Observação 6.45 -

Quando tivermos definido operações aritméticas e algébricas (extração de raízes quadradas, cúbicas, etc.) de números reais absolutos, poderemos dar muitos exemplos de irracionais expressos por fórmula, em vez de diretamente por sua lista de dígitos.

Nesse sentido, recorde que já provamos que não existe nenhum número racional x *tal que* $x^2 = 2$*. Contudo, isso não é suficiente para nos permitir dizer que* $\sqrt{2}$ *é irracional, pois ainda não definimos multiplicação para reais absolutos.*

Note que para todo número irracional (em verdade, a todo número real absoluto), dado por sua representação em lista de dígitos, $x = m,\ a_1a_2a_3\ldots$, está associado um esquema de aproximações sucessivas:

$$\begin{gathered} m \leqslant x \leqslant m+1 \\ m, a_1 \leqslant x \leqslant m, a_1 \ + 1/10 \\ m, a_1a_2 \leqslant x \leqslant m, a_1a_2 \ + 1/10^2 \\ m, a_1a_2a_3 \leqslant x \leqslant m, a_1a_2a_3 \ + 1/10^3 \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{gathered}$$

Por isso, muitas pessoas, sem negar que os números reais são imprescindíveis em assuntos teóricos, costumam afirmar que os números racionais bastam para as aplicações práticas. Com efeito, nas desigualdades acima, tanto as aproximações por falta (as do tipo $m, a_1a_2a_3\ldots a_n$) como as aproximações por excesso (as do tipo $m, a_1a_2a_3\ldots a_n + 1/10^n$) são números racionais, e podemos tornar o erro $1/10^n$ tão pequeno quanto desejarmos.

Essa posição é um tanto polêmica, pois que a possibilidade de chegarmos a um racional aproximante $m,\ a_1a_2a_3\ldots a_n$, com n suficientemente grande, pode ser muito trabalhosa de ser efetivada –ou, até mesmo, apenas potencial. Vejamos um exemplo.

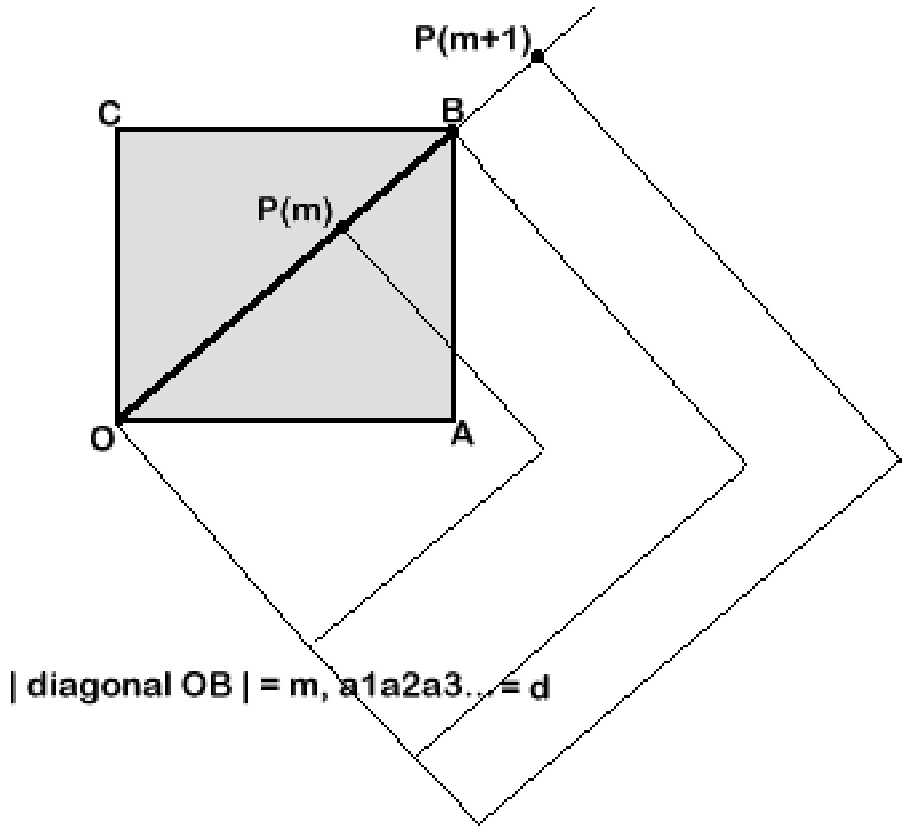
Exemplo 6.46 (*Estimando a diagonal do quadrado de lado unitário*) -

Retomemos a discussão de medida da diagonal OB de um quadrado de lado unitário (confira na figura seguinte). Como essa diagonal é um segmento de reta, sabemos que existe um real absoluto, digamos d, que mede seu comprimento: $d = |OB|$. Ora, sendo d um real absoluto, ele é uma lista infinita de dígitos, digamos:

$$d = m,\ a_1a_2a_3\ldots\ ,$$

e, pelo Teorema 6.5, sabemos que tal lista não é periódica. O problema que surge agora é: como determinar explicitamente os valores de m, a_1, a_2, a_3, etc.?

Iniciamos observando que o natural m mede um segmento menor do que OB, enquanto $m+1$ mede um segmento maior do que OB. Construindo quadrados de diagonais medindo m e $m+1$, obtemos, respectivamente, um quadrado menor e um quadrado maior do que o quadrado de diagonal OB.



Daí, por Pythagoras[1]*, obtemos*

$$m^2 \leqslant 2 \leqslant (m+1)^2. \tag{6.2}$$

Ora, sendo m um número natural, a única possibilidade para ele satisfazer (6.2) é com $m = 1$.

Da mesma forma, a_1 deve ser um dígito tal que

$$(1, a_1)^2 \leqslant 2 \leqslant (1, a_1 + \frac{1}{10})^2. \tag{6.3}$$

[1]Aqui estamos utilizando a versão geométrica original desse teorema. Essa diz que se, a partir de um dado quadrado, construírmos um segundo quadrado cujo lado é a diagonal do primeiro, a área desse segundo quadrado será o dobro da do primeiro. Consequentemente, tomando como unidade de área a área de um quadrado de lado unitário, segue que o quadrado que tem como lado a diagonal do quadrado unitário terá como área o dobro da unidade de área.

Como existem no máximo 10 *possibilidades para o valor de* $a_1 \in \{0,..,9\}$, *depois de no máximo dez tentativas testando (6.3), iremos descobrir que* $a_1 = 4$ *(pois* $(1,4)^2 = 1,96$, *enquanto* $(1,5)^2 = 2,25$*). Concluímos assim que*

$$d = 1,4\ldots .$$

Para determinarmos a_2, *notemos que*

$$(1,4a_2)^2 \leqslant 2 \leqslant (1,4a_2 + \frac{1}{100})^2\,,$$

de modo que, após no máximo 10 *tentativas, encontraremos* $a_2 = 1$. *Assim,*

$$d = 1,41\ldots .$$

Continuando dessa forma, podemos obter aproximações racionais de $d = |OB|$ *tão acuradas quanto quisermos; dito de forma precisa, podemos determinar o dígito* a_n, *seja qual for o* n *dado. De fato, convidamos o leitor a provar, usando indução matemática, que o processo descrito neste exemplo pode ser generalizado para provar que, dado* $n \geqslant 2$, *o dígito* a_n *fica bem determinado a partir do conhecimento de* $a_1, \ldots, a_{n-1}$.

Exercício 155 -

Usando o raciocínio do exemplo anterior, determine os três primeiros elementos da lista que representa o número real absoluto que mede a diagonal de um retângulo cujos lados medem 1 *e* 2.

Exercício 156 -

Dado um número real absoluto x, *suponhamos que vamos obtendo, sucessivamente, as seguintes desigualdades, onde* m *é inteiro* $m \geqslant 0$ *e os* a_n *são dígitos:*

$$\begin{gathered}
m \leqslant x < m+1 \\
m,a_1 \leqslant x < m,a_1 + 1/10 \\
m,a_1a_2 \leqslant x < m,a_1a_2 + 1/10^2 \\
m,a_1a_2a_3 \leqslant x < m,a_1a_2a_3 + 1/10^3 \\
\cdots\cdots\cdots\cdots\cdots\cdots
\end{gathered}$$

Pede-se mostrar que a seguinte afirmação é falsa:

> *se alguma das* $\leqslant$ *for, em verdade, uma igualdade, então* x *será racional; caso contrário, ele será irracional.*

Dependendo de como um número real absoluto – racional ou irracional – for dado, ou caracterizado, pode ser bastante difícil conseguirmos informação sobre os dígitos constituindo sua expansão decimal. Ainda hoje, existem várias áreas de pesquisa envolvidas com esta questão. No Capítulo 8 discutiremos, com algum detalhe, esse assunto.

Algumas simplificações de terminologia e notação.

Para que a leitura dos próximos capítulos fique mais leve e envolva terminologias e notações mais próximas da usada na Escola:

- Passaremos a usar a expressão expansão decimal de um número real absoluto para qualquer uma das medidas iterativas que o representam. Faremos isso, mesmo no caso das medidas iterativas 9-terminantes de segmentos de reta tipo OP, com P ponto graduado da régua infinita.

  Ou seja, por exemplo, chamaremos a medida iterativa $0,999\ldots$ (do segmento unitário) de expansão decimal, embora $0,999\ldots$ não seja uma expansão decimal obtenível pelo método da divisão euclidiana.
- No caso de números racionais que têm expansão decimal 0- terminante, como ocorre com, por exemplo,

  $$0,8 = 0,80 = 0,800 = \cdots,$$

  também escreveremos:

  $$0,8 = 0,80 = 0,800 = \cdots = 0,800\,000\,000\ldots = 0,8\overline{0} = 0,7\overline{9}.$$

  O mesmo faremos com qualquer outra expansão 0-terminante.

- Consideraremos a medida direta como caso particular da medida iterativa, e procuraremos usar apenas a palavra "medida", no lugar de "medida iterativa".

- Note que é comum se dizer "seja o número dado por $1,234\ldots$", mas isso é ambíguo, pois poderíamos (a menos que seja dada mais informação) estar falando de $1,2345$, $1,2346$, $1,23444\ldots$ e infinitas outras possibilidades, tanto racionais como irracionais.

CAPÍTULO 7

NÚMEROS REAIS

No capítulo anterior, resolvemos a *insuficiência geométrica* dos números racionais (qual seja: sua incapacidade de atribuir uma medida a todos os segmentos da reta euclidiana) introduzindo o conjunto $\mathbb{A}$ dos números reais absolutos.

O primeiro grande objetivo do presente capítulo é fazer a *capacitação numérica dos reais*. Com isso, queremos dizer que precisamos poder somar, multiplicar e ordenar os números reais absolutos. Mais do que isso: a partir de $\mathbb{A}$, queremos construir um campo numérico que deverá ter uma adição e uma multiplicação, bem como uma relação de ordem, que sejam uma extensão das do campo dos números racionais –obedecendo-se assim ao chamado Princípio da Permanência de Hankel. Em particular, na medida do possível, essa extensão deverá imitar a passagem do campo $[\mathbb{Z}, +, \cdot, <]$ para o campo $[\mathbb{Q}, +, \cdot, <]$.

Com vistas a esse objetivo, a primeira coisa a observar é que, como a todo número racional está associado um outro que lhe é simétrico na adição, o conjunto $\mathbb{A}$ é insuficiente para a extensão pretendida. Será preciso construir um conjunto ainda maior do que $\mathbb{A}$, formado justamente pelos números reais absolutos e seus "negativos"; conjunto esse que passaremos a chamar de conjunto dos números reais[1] e que será denotado por $\mathbb{R}$. Essa tarefa será bastante semelhante, embora muito mais complexa, da que encontramos quando passamos do conjunto dos números naturais para o campo dos inteiros:

$$\mathbb{N} \to [\mathbb{Z}, +, \cdot, <] \quad \text{versus} \quad \mathbb{A} \to [\mathbb{R}, +, \cdot, <]\,.$$

A seguir, *qualificaremos* essa capacitação numérica, demonstrando que os números reais resolvem parcialmente a *insuficiência aritmética* dos racionais. Ou seja: com os números reais seremos, finalmente, capazes de atribuir um resultado exato para a raiz quadrada de 2, bem como para a raiz quadrada de qualquer inteiro positivo que não seja um quadrado.

Concretizada a capacitação numérica dos reais, bem como a sua qualificação, passaremos à segunda grande tarefa deste capítulo, qual seja: a *elucidação da estrutura* do campo $[\mathbb{R}, +, \cdot, <]$ dos números reais. Isso resultará na demonstração de que esse campo tem duas propriedades importantes:

- é um corpo ordenado;
  (o campo dos racionais também tem essa propriedade estrutural)
- tem a Propriedade do Contínuo
  (o campo dos racionais não tem essa propriedade).

[1] Esta denominação é devida a George Cantor, c. 1875, e a escolha da palavra "real" foi feita para diferenciá-los de um campo numérico ainda mais geral, o dos números imaginários (ou complexos), que estudaremos num capítulo mais adiante.

Como $[\mathbb{R}, +, \cdot, <]$ é um corpo ordenado, temos à nossa disposição um poderoso, mas simples, algebrismo. Este, aliado à Propriedade do Contínuo, nos permite muito cômoda e mecanicamente abordar os problemas envolvendo grandezas contínuas, sejam eles problemas matemáticos (como os problemas geométricos) ou problemas físicos (como a mecânica dos sólidos e fluídos, as transformações de energia e assim por diante). Com efeito, a última grande tarefa deste capítulo será *exemplificar o poder da algebrização dos problemas de grandezas contínuas* por meio de uma rápida abordagem das ideias centrais da Geometria Analítica.

Historicamente falando, essa mistura de um algebrismo simples com um campo que tem a Propriedade do Contínuo ocorreu basicamente entre 1600 e 1700, e resultou das contribuições de muitos matemáticos, entre os quais: Viète (cálculo literal ou cálculo algébrico com letras), Fermat e Descartes (tradução algébrica dos problemas geométricos). Essa foi, em verdade, uma "mistura explosiva" que propiciou o desenvolvimento da ciência e tecnologia modernas, a partir de Newton e Euler.

Passando ao desenvolvimento deste capítulo, iniciaremos com a construção de $\mathbb{R}$ a partir de $\mathbb{A}$. Para tal, usaremos um procedimento bastante concreto que chamaremos de "etiquetagem dos pontos da reta euclidiana", o qual nos permitirá localizar sem ambiguidade os pontos da reta euclidiana, e dar um significado bem concreto para o que chamaremos de "números reais negativos".

7.1 Localização geométrica dos pontos da reta

Suponha o leitor que alguém lhe pare para perguntar onde fica uma determinada loja que ele apenas sabe que está na rua em que ambos se encontram. Duas maneiras de responder seriam dizer "O Sr. encontrará tal loja andando 100 metros adiante", ou "O Sr. passou tal loja 50 metros atrás".

Se examinarmos cuidadosamente essas respostas, veremos que ela têm três ingredientes básicos:

- um ponto de referência
  (no caso, o ponto de encontro das duas pessoas);
- uma unidade de medida de distâncias
  (no caso, o metro);
- um sentido de percurso da rua
  (o sentido em que vinha andando o cidadão que nos parou, e o sentido inverso deste; por exemplo, um sentido podia ser o de subida da rua e o outro o de descida da rua).

No caso abstrato da localização dos pontos de uma reta qualquer, podemos proceder de modo análogo. Assim, começamos selecionando um ponto da reta – que servirá como *ponto de referência*, ou *origem* –, o qual denotaremos por O.

Dado agora um ponto P da reta, é natural considerarmos como "localizador" de P a distância de P a O, ou seja, o comprimento ou medida do segmento OP. Sabemos do capítulo sobre medição de segmentos que, desde que tenhamos escolhido uma unidade de medida de comprimentos, essa distância está bem definida, e é dada por um número real absoluto, digamos x; ou seja, $x = |OP|$.

Entretanto, é claro que esse número x ainda não determina o ponto P de maneira unívoca, uma vez que sabemos que seu simétrico P' em relação à origem também satisfaz $|OP'| = x$. Contudo, o impasse é imediato de ser resolvido: de modo semelhante ao que fizemos na localização da loja, basta escolhermos um sentido de percurso dos pontos da reta. Equivalentemente, basta acrescentarmos a informação acerca do "lado" da origem em que está o ponto P.

Uma reta onde uma tal distinção está bem determinada é denominada de *eixo cartesiano,* conceito que a seguir definiremos com precisão.

Definição 7.1 -

Um eixo cartesiano *é uma reta euclidiana na qual foram escolhidos uma orientação e uma unidade de medida. Mais precisamente:*
um eixo cartesiano *é formado por uma reta euclidiana r, e pela escolha de dois pontos distintos sobre a mesma, denotados por O e U. O ponto O é chamado de* origem *do eixo. O ponto U é chamado de* ponto unitário *do eixo, e tem dupla serventia: determina uma* unidade de medida*, OU, para os segmentos de reta do eixo, e determina um* sentido *de percurso, ou* orientação*, para o mesmo.*

O sentido de percurso do eixo que vai de O para U é chamado de sentido positivo*, enquanto que o sentido de percurso oposto (que vai de U para O) é chamado de* sentido negativo*.*

> Notação: denotaremos por (r, O, U) o eixo determinado pela reta r, pela origem O e pelo ponto unitário U, ficando subentendido que isto determina OU como unidade de medida.

Observação 7.2 -

Alguns autores preferem ver a orientação do eixo como consistindo em dividir os *pontos da reta r (distintos da origem) em duas classes exclusivas: os* pontos positivos *e os* pontos negativos. *Os pontos positivos são os pontos distintos da origem e que estão na semi-reta que inicia em O, e passa por U; os pontos negativos são os pontos distintos da origem e que estão sobre a outra semi-reta que inicia em O.*

Também se costuma chamar essas duas semi-retas de, respectivamente, semi-eixo positivo *e* semi-eixo negativo.

Observação 7.3 -

Quando pudermos supor o eixo (r, O, U) (a rigor, a reta r do eixo) colocado na posição horizontal, costuma-se usar a seguinte terminologia mais intuitiva:
sendo P ponto do eixo, dizemos que "P está à direita da origem" se o segmento de reta que inicia em O, e termina em P, for percorrido no sentido positivo do eixo. Semelhantemente, dizemos que "P está à esquerda da origem" se o segmento de reta que inicia em O, e termina em P, for percorrido no sentido negativo do eixo.

Exemplo 7.4 -

O ponto U está à direita e à distância um da origem, enquanto que seu simétrico em relação a esta origem está à esquerda dela e à distância também um.

Exemplo 7.5 -

Mais geralmente, dado um eixo (r, O, U), "caminhando" no sentido positivo, marquemos sucessivamente os pontos $U_1, U_2, U_3, \ldots$ tais que $|OU_n| = n$. Note que $U_1 = U$. A seguir, denotemos por U'_n o simétrico de U_n em relação à origem.

Os pontos da "rede" $\ldots, U'_2, U'_1, O, U_1, U_2, \ldots$, assim construída, podem ser localizados do seguinte modo:

- *cada U_n está à direita da origem e à distância de n unidades da mesma;*
- *cada U'_n está à esquerda da origem e à distância de n unidades da mesma.*

Exemplo 7.6 -

A partir de todo eixo, (r, O, U), podemos construir uma régua infinita sobre o mesmo. Basta tomar como suporte da régua o semi-eixo positivo, e como unidade de medida da régua, a mesma unidade do eixo, OU.

Feito isso, podemos localizar cada ponto graduado da régua, $P(m/10^n)$, como sendo o ponto à direita da origem que está à distância $m/10^n$ da mesma.

Resumindo:

combinando *números absolutos* com a ideia de orientação (*sentido* de percurso), podemos "etiquetar" todos os pontos da reta euclidiana (a rigor, de um eixo cartesiano):

$$\text{reta euclidiana} \longleftrightarrow \mathbb{A} + \text{sentido.}$$

7.2 Localização algébrica dos pontos da reta: números reais

A ideia que estamos para introduzir é fundamental na Matemática. É uma ideia bastante simples, mas não é trivial apresentá-la de uma maneira sistemática. Para uma visão preliminar da mesma, retomemos o caso da rede de pontos construída no Exemplo 7.5.

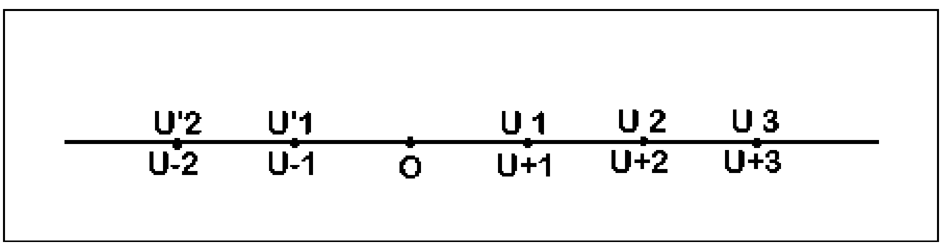
Podemos localizar os pontos daquela rede de uma maneira mais rápida, substituindo a expressão "à direita" por um sinal + e a expressão "à esquerda" por um sinal -. Ou seja, podemos usar o seguinte sistema alternativo de etiquetagem:

- o ponto U_n está à distância $+n$ da origem (por exemplo: U_2 está à distância $+2$ da origem);
- o ponto U'_n está à distância $-n$ da origem (por exemplo: U'_2 está à distância -2 da origem).

Além de estarmos economizando palavras, também poderemos usar uma notação ainda mais simples para tal rede:

$$\dots, U_{-2}, U_{-1}, O, U_{+1}, U_{+2}, \dots,$$

e agora fica natural a denominarmos "rede dos números inteiros".



Nossa intenção é fazermos algo semelhante para todos os pontos da reta euclidiana. Contudo, temos uma dificuldade imediata a enfrentar:

> enquanto que, no caso da rede dos inteiros, para fazer a etiquetagem dos pontos à esquerda da origem, *já dispunhamos* dos inteiros negativos $(-1, -2, \dots)$, no caso da etiquetagem de pontos quaisquer da reta, precisaremos dar significado a "$-$número real absoluto".

Assim, precisaremos *criar um conjunto numérico* que consista do conjunto dos reais absolutos e seus "negativos". No que segue, passaremos a definir tal conjunto; o mesmo será denominado conjunto dos *números reais* [2], e o denotaremos por $\mathbb{R}$.

Note que nossa tarefa não é total novidade, pois podemos dizer:

$$\mathbb{N} \to \mathbb{Z} \to \text{etiquetagem da rede dos inteiros}$$
$$\mathbb{A} \to \mathbb{R} \to \text{etiquetagem da reta euclidiana.}$$

Definição 7.7 -

A cada número real absoluto não nulo, x, associaremos dois novos objetos matemáticos: $+x$ e $-x$; sendo que denominaremos

- $+x$ *de número real positivo;*
- $-x$ *de número real negativo.*

(Note que o zero dos reais absolutos não é nem real positivo, e nem real negativo.)

O número real absoluto x envolvido passará a ser denominado valor absoluto de $+x$ e de $-x$, e costuma-se escrever: $|+x| = |-x| = x$.

[2] Conforme já dito, esta denominação é recente, e devida a George Cantor, c. 1875. Outras denominações, mas que sairam de uso, são: números reais relativos, ou meramente números relativos. Alguns autores antigos também usavam a terminologia números algébricos, a qual hoje é empregada com outro sentido.

Notação:

$$\begin{aligned}\mathbb{R}_+ &= \text{conjunto dos números reais positivos}\\ &= \text{conjunto dos reais absolutos, não nulos, precedidos do sinal } +;\end{aligned}$$

$$\begin{aligned}\mathbb{R}_- &= \text{conjunto dos números reais negativos}\\ &= \text{conjunto dos reais absolutos, não nulos, precedidos do sinal } - .\end{aligned}$$

Definição 7.8 -

O conjunto dos números reais relativos, ou meramente conjunto dos números reais , é denotado por $\mathbb{R}$ e consiste no conjunto de todos os números reais positivos, bem como todos os negativos e o zero:

$$\mathbb{R} = \mathbb{R}_- \cup \{0\} \cup \mathbb{R}_+ .$$

Ademais, a igualdade em $\mathbb{R}$ é assim convencionada:
sendo a e b números reais, diremos que eles são iguais, e escreveremos $a = b$, se, e somente se:

- *ou ambos forem o zero;*
- *ou tiverem o mesmo sinal e o mesmo valor absoluto.*

Exemplo 7.9 -

Cada inteiro negativo está naturalmente associado a um real negativo. Por exemplo, $-1 = -1,000\ldots$, $-2 = -2,000\ldots$, etc. Por isso, diremos que todo inteiro negativo é (identificável a) um número real negativo.

Semelhantemente, todo racional negativo, por meio de sua expansão decimal, está naturalmente associado a um real negativo. Por exemplo, $-1/2 = -0,5000\ldots$, $-2/3 = -0,666\ldots$, etc. Por isso, também diremos que todo número racional negativo é (identificável a) um número real negativo.

Observação 7.10 -

Do exemplo anterior, surge a ideia de identificarmos os inteiros positivos e os racionais positivos com números reais. Para termos tal identificação, basta tratarmos o sinal + como "invisível". Com efeito, por que não tratarmos $2 = 2,000\ldots$ *como* $2 = +2,000\ldots$*? Analogamente, para racionais positivos, por que não tratarmos, por exemplo,* $1/4 = 0,25000\ldots$ *como* $1/4 = +0,25000\ldots$*?*

Assim, em termos mais gerais, na prática, costumamos identificar todo número real absoluto não nulo r *com o real positivo* $+r$*. Essa convenção, e o que já foi observado no exemplo anterior, nos permitem a seguinte sequência de inclusões:*

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}\,,}$$

as quais estão dizendo que o conjunto dos números reais inclui todos os conjuntos de números que já encontramos.

Com essas cruciais preliminares, estamos com recursos análogos aos que tínhamos quando usamos $\mathbb{Z}$ para etiquetar os pontos da rede dos inteiros. Com efeito, vamos mostrar como, agora, podemos facilmente etiquetar todos os pontos da reta.

Em verdade, faremos um pouco mais do que isso. Em vez de usarmos longas expressões como, por exemplo, "P está à distância $2,333\ldots$ da origem e à esquerda da mesma", passaremos a usar uma expressão equivalente, mas bem mais curta: "a coordenada de P é $-2,333\ldots$ ". Vejamos como.

Definição 7.11 -

Denominamos sistema de coordenadas cartesianas *de um eixo* (r, O, U) *a seguinte associação de pontos do eixo a números reais:*

> *a cada ponto* Q *do eixo associamos um número real* $x(Q)$ *(frequentemente denotado menos precisamente por* x*), dito* coordenada cartesiana *de* Q *e o qual é definido da seguinte forma:*

– *se* $Q = O$ *então* $x(Q) = 0$*;*
– *se* Q *é um ponto positivo do eixo então* $x(Q) = +|OQ|$*;*
– *se* Q *é um ponto negativo do eixo então* $x(Q) = -|OQ'|$
(onde Q' *denota o simétrico de* Q *em relação à origem* O*).*

Exemplo 7.12 -

Temos $x(U) = 1 = +1,000\ldots$, ou seja, o ponto unitário U tem coordenada um. Semelhantemente, $x(O) = 0$, ou seja, a origem do eixo tem coordenada zero.

Do mesmo modo, os pontos da rede dos inteiros, vide Exemplo 7.5, podem ser muito rapidamente localizados: $x(U_n) = +n$ e $x(U'_n) = -n$.

Teorema 7.13 -

O sistema de coordenadas cartesianas definido por cada eixo é uma associação que exaure todos os números reais, e faz isto sem repetir valores.

Prova:

As coordenadas exaurem $\mathbb{R}$.
Como $0 = x(O)$, resta mostrar que todo número real positvo ou negativo é a coordenada de algum ponto sobre a reta.
– Seja x real positivo, de modo que $x = +r$, com r real absoluto não nulo. Por definição de número absoluto, é imediato que tal r é a medida de um segmento de reta OP, com P ponto positivo: $|OP| = r$. Logo, $x(P) = +|OP| = +r = x$.
– Seja x real negativo, de modo que $x = -r$, com r real absoluto. Pela definição de número real absoluto, existe P tal que $|OP| = r$, e sendo P' o simétrico de P em relação à origem, temos $|OP'| = |OP| = r$ e então, como P positivo dá P' negativo, segue que $x(P') = -|OP'| = -r = x$.

As coordenadas não repetem valores.
Se tivermos $x(P_1) = x(P_2) = +r$, isto significa que $|OP_1| = |OP_2| = r$ e que P_1, P_2 são pontos positivos. Daí, pelo Teorema 6.33, segue que OP_1 e OP_2 são congruentes e, portanto, $P_1 = P_2$. Um raciocínio análogo trata da possibilidade $x(P_1) = x(P_2) = -r$, com r real absoluto.[3]

CQD.

É mais comum enunciarmos o resultado anterior usando a noção de associação biunívoca, ou correspondência biunívoca, definição essa que passaremos a recordar da Teoria dos Conjuntos:

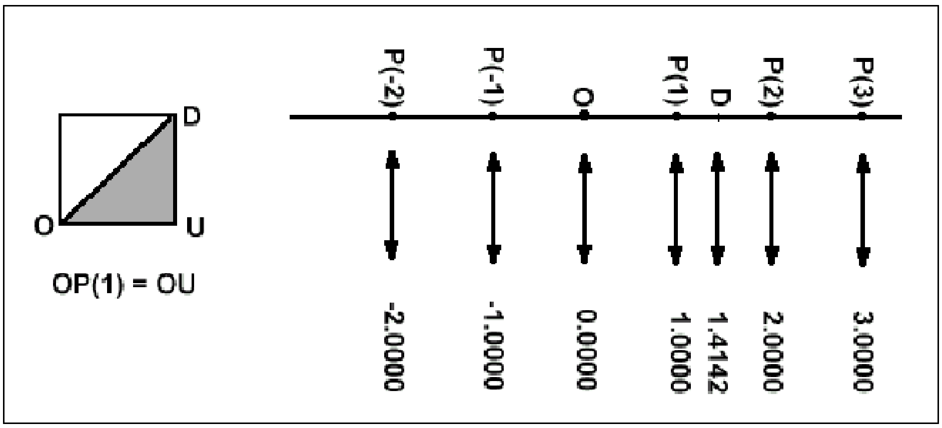
[3] É importante que o leitor recorde que o Teorema 6.33 é consequência do Postulado do Contínuo.

Definição 7.14 -

Sejam dois conjuntos não vazios, A e B. Dizemos que temos uma **correspondência biunívoca**[4] *entre A e B se existir uma associação tal que:*

- *cada elemento de A está associado a um único elemento de B;*
- *inversamente, cada elemento de B está associado a um único elemento de A.*

> **Teorema 7.15 (Teorema Fundamental da Geometria Analítica)**
> *A correspondência que associa a cada ponto de um eixo cartesiano (r, O, U) a coordenada cartesiana deste ponto é uma correspondência biunívoca entre a reta r e o conjunto $\mathbb{R}$ dos números reais.*



Prova:

Com efeito, pelo teorema anterior, cada ponto Q da reta tem uma única coordenada, $x(Q)$. E, reciprocamente, para cada número real x, existe um único ponto Q da reta, tal que a coordenada de Q seja x.

CQD.

Eventualmente, pode-se abreviar o enunciado desse resultado dizendo que há uma

[4] Outras denominações em uso: correspondência um a um e bijeção

correpondência biunívoca entre os pontos de cada reta euclidiana e os números reais.[5] Por essa razão, também se costuma chamar uma reta euclidiana de reta real.

A denominação desse teorema resulta do fato de que o mesmo é o ponto de partida para o tratamento estritamente algébrico dos problemas geométricos, assunto que compete à disciplina Geometria Analítica. Numa leitura complementar a este capítulo, faremos uma breve exposição dessa muito importante ideia matemática.

Notação.
Podemos dizer que o teorema anterior garante que, para cada número real x, existe sobre a reta euclidiana exatamente um ponto Q, tal que $x(Q) = x$. De modo que o teorema anterior garante que está bem feita a notação $P(x)$ para denotar o ponto Q do eixo que tenha como coordenada o número real x.

Por exemplo: $P(0) = O$, pois $x(O) = 0$; $P(1) = U$, pois $x(U) = 1$. Em termos mais gerais, se x é positivo, temos que $P(x)$ é o único ponto positivo Q do eixo, tal que $|OQ| = x$. Analogamente, se x é negativo, ele é da forma $x = -r$; daí, tomando um $x' = r$, temos que $P(x)$ é o único ponto negativo Q do eixo, tal que $|OQ| = r$.

Com essa notação, podemos escrever:

$$Q \to x(Q) \to P(x(Q)) = Q\,.$$

Exercício 157 -

Mostre que essa última notação generaliza a notação já utilizada no Capítulo 5: se $x = m/10^n$, com $m > 0$, então o ponto $P(x)$ à direita de O, que tem coordenada x é precisamente o ponto graduado $P(m/10^n)$.

7.3 Números reais como expansões decimais

– Expansão decimal de números reais quaisquer.

Podemos resumir o que foi feito anteriormente, observando que:

> intuitivamente, um número real é o resultado que se obtém "colando" um sinal ($+$, ou $-$) a um número real absoluto. Ora, como todo número

[5] É importante que o leitor tenha bem claro que trata-se de uma abreviação: em cada reta, podemos escolher infinitas unidades de medida e duas orientações; mas cada escolha determina um único eixo cartesiano.

real absoluto pode ser representado por expansão decimal, segue que os reais ficam naturalmente dotados de uma representação deste tipo.

– Significado da expansão decimal dos números reais.

Nas seções que se seguirão, muito exploraremos *o significado* da expansão decimal de um número real. Ele é semelhante ao da expansão de um número absoluto, diferenciando-se apenas pela necessidade de levar em conta o sinal. Exemplifiquemos.

Escolhido um eixo cartesiano, podemos interpretar o real positivo $+0,250\,000\ldots$ como sendo a coordenada de um ponto P sobre o eixo, que é localizado da seguinte maneira: para ir da origem do eixo até P, tenho de "caminhar" para a direita dois décimos da unidade, e mais cinco centésimos da unidade.

Semelhantemente, $-0,250\,000\ldots$ é a coordenada de um ponto P', que é localizado do seguinte modo: para ir da origem do eixo até P', tenho de "caminhar" para a esquerda dois décimos da unidade, e mais cinco centésimos da unidade. Os pontos P e P' são simétricos em relação à origem.

Em particular, devido a essa interpretação, vemos que pode-se fazer as seguintes identificações:

$$0 = 0,000\ldots = +0,000\ldots = -0,000\ldots\,.$$

Consequentemente, diremos que o valor absoluto do zero é zero, e escreveremos:

$$0 = |0,000\ldots| = |+0,000\ldots| = |-0,000\ldots|\,.$$

– A questão da eventual duplicidade da expansão.

Como certos números reais absolutos têm uma dupla representação decimal (uma expansão 0-terminante e outra expansão 9-terminante), segue que é útil explicitarmos a relação de igualdade entre números reais em termos de suas expansões. Vejamos.

Teorema 7.16 -

Sendo a e b números reais, temos que eles serão iguais (e escreveremos $a = b$) se, e somente se

- *ou $a = 0$ e $b = 0$;*
- *ou a e b são reais positivos e, assim, da forma*

$$a = +m, a_1 a_2 a_3 \ldots \quad e \quad b = +M, b_1 b_2 b_3 \ldots\ ,$$

ou, então, ambos são reais negativos e, assim, da forma

$$a = -m, a_1 a_2 a_3 \ldots \quad e \quad b = -M, b_1 b_2 b_3 \ldots$$

(onde $m, M \geqslant 0$ são inteiros; os a_k e os b_k são dígitos; ao menos um dentre m e os a_k é não nulo, e ao menos um dentre M e os b_k é não nulo) ,
sendo que, ademais – em qualquer uma dessas duas alternativas –, vale a seguinte igualdade entre números reais absolutos:

$$m, a_1 a_2 \ldots = M, b_1 b_2 \ldots .$$

Prova:

Imediata, pelos resultados e definições anteriores. CQD.

Exemplo 7.17 -

Temos: $+0,25000\ldots = +0,24999\ldots$, *bem como* $-1 = -1,000\ldots = -0,999\ldots$.

– A questão da periodicidade da expansão decimal.

Definição 7.18 -

Número irracional é todo número real que não é número racional. Denotaremos o conjunto dos irracionais por $\mathbb{I}$.

Com essa terminologia, dividimos o conjunto dos números reais em duas classes disjuntas, tendo-se:

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I} .$$

Exemplo 7.19 -

O Exemplo 6.40 nos mostra alguns irracionais positivos e, "colando" um sinal negativo no valor absoluto dos mesmos, a partir deles obtemos os seguintes exemplos de números irracionais negativos:

$-0,10\,100\,1000\,10000\,100000\ldots$
$-0,012\,01212\,0121212\ \ldots$
$-0,101001000000100000000000000010\ldots$ *(note que envolve fatorial).*

Teorema 7.20 -

Os números reais podem ser caracterizados em termos de suas expansões decimais, do seguinte modo:

- *os números racionais são os números reais que têm uma (ao menos) expansão decimal periódica (talvez 0-terminante);*
- *os números irracionais têm exatamente uma expansão decimal e ela é não periódica.*

Prova:

O resultado decorre do que já sabemos sobre expansões de números racionais e do Teorema 6.41, o qual garante que todo número irracional absoluto é representado por apenas uma lista de dígitos, e que a mesma não é periódica.

CQD.

Exercício 158 -

A partir de uma conferência do famoso físico Richard Feymann (Prêmio Nobel 1965, Eletrodinâmica Quântica), definiremos como casa de Feymann *de um número irracional a primeira casa – depois da vírgula, em sua expansão decimal – que é seguida pelo bloco cabalístico 666. Assim sendo, pede-se:*

i). mostrar que, para cada $n = 1, 2, 3 \ldots$, existe um número irracional cuja casa de Feymann é a n-ésima casa decimal;
ii). mostrar que existem números irracionais sem casa de Feymann.

Exercício 159 -

Chamaremos de "casa generalizada de Feymann" de um número irracional a primeira casa – depois da vírgula, em sua expansão decimal – que é seguida por um bloco de três dígitos repetidos. Assim sendo, pergunta-se: todo número irracional tem uma casa generalizada de Feymann? Justifique.

7.4 Ordenação dos números reais

Nas seções anteriores, introduzimos os números reais, vimos que os mesmos têm uma útil interpretação geométrica (são as coordenadas dos pontos da reta euclidiana) e incluem os números reais absolutos (os quais resolvem completamente o problema da medida de segmentos de reta). Eles têm um inegável carácter numérico: incluem as quantidades (os resultados das medidas) e incluem os demais conjuntos numéricos que já introduzimos: $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$.

No que segue, reforçaremos esse carácter numérico construindo um campo numérico com os números reais: mostraremos como ordená-los, como somá-los e multiplicá-los. Mais do que isso, faremos uma extensão, seguindo o Princípio da Permanência de H. Hankel [6]:

> definiremos uma ordem ($<$), uma adição ($+$) e uma multiplicação ($\cdot$) em $\mathbb{R}$, de modo a estender as correspondentes ordenação e operações aritméticas em $\mathbb{Z}$ e $\mathbb{Q}$, preservando ao máximo suas propriedades.

Podemos abreviar isso, dizendo que queremos construir um campo $[\mathbb{R}, <, +, \cdot\,]$ tal que:

$$[\mathbb{Z}, <, +, \cdot\,] \subset [\mathbb{Q}, <, +, \cdot\,] \subset [\mathbb{R}, <, +, \cdot\,].$$

Na presente seção, faremos a extensão da ordem, deixando para a seguinte a extensão das operações aritméticas.

A expansão decimal de um número real absoluto nos diz até quantas unidades, até quantos décimos, até quantos centésimos, etc. cabem no mesmo. Em particular, dado um real absoluto $x = m, a_1 a_2 a_3 \ldots$, podemos escrever:

$$m, a_1 a_2 a_3 \ldots a_n \leqslant x \leqslant m, a_1 a_2 a_3 \ldots a_n + \frac{1}{10^n}.$$

Assim, podemos dizer que a definição de expansão decimal já traz embutida uma relação de ordem entre o real absoluto x e os números racionais que se obtém truncando sua expansão decimal.

Isso nos permite estabelecer uma relação de ordem entre dois reais absolutos quaisquer, a partir da comparação entre as respectivas expansões decimais. Dados dois

[6] Hermann Hankel, matemático alemão que por cerca de 1860 introduziu a ideia de número formal.

números reais absolutos *distintos*, x e y, escrevamos suas expansões decimais:

$$x = m, a_1a_2a_3 \ldots$$
$$y = M, b_1b_2b_3 \ldots .$$

Com o intuito de dizermos *"quem é o maior"* entre x e y, o caminho natural é iniciarmos comparando m com M.
– Se $m < M$, então dizemos que x *é menor do que* y e escrevemos $x < y$.
– Se $M < m$, então invertemos a conclusão: dizemos que y *é menor do que* x e escrevemos $y < x$.
– Se $m = M$, então comparamos a_1 com b_1. Se tivermos $a_1 < b_1$, então $x < y$, e se $b_1 < a_1$, então $y < x$. Resta a possibilidade $a_1 = b_1$, ou seja: $m = l$ e $a_1 = b_1$. Nesse caso, comparamos a_2 com b_2, aplicando o mesmo critério. Se $a_2 = b_2$, então comparamos a_3 com b_3, e assim por diante. Pode acontecer de termos muitos dígitos da representação decimal de x iguais aos correspondentes dígitos da representação de y, mas como $x \neq y$, certamente ocorrerá um primeiro valor de n para o qual $a_n \neq b_n$. Nesse caso, teremos $a_i = b_i$, para $i = 0, 1, \ldots, n-1$. Escreveremos, então: $x < y$, se $a_n < b_n$, ou $y < x$, se $b_n < a_n$.

Examinemos mais cuidadosamente essa ideia, supondo, sem perda de generalidade, que $m \leqslant M$. Teremos exatamente dois casos a examinar.

$\boxed{1^\circ \text{ caso: } m < M}$

Observemos inicialmente que a hipótese $m \leqslant M$ nos permite escrever:

$$m \leqslant x \leqslant m + 1 \leqslant M \leqslant y \leqslant M + 1 .$$

Ademais, se supormos que estamos usando apenas expansões não 9-terminantes, podemos até garantir que:

$$m \leqslant x < m + 1 \leqslant M \leqslant y < M + 1 ,$$

o que torna natural estendermos a relação de ordem, escrevendo que $x < y$.

$\boxed{2^\circ \text{ caso: } m = M}$

Continuando a trabalhar apenas com expansões decimais que não sejam 9-terminantes, suponhamos que a primeira diferença entre os dígitos de x e y ocorra na terceira casa decimal, de modo que $a_1 = b_1$, $a_2 = b_2$ e $a_3 \neq b_3$.

Sem perda de generalidade, suponhamos que $a_3 < b_3$. Temos duas possibilidades para examinar: $1 + a_3 < b_3$ e $1 + a_3 = b_3$.

- Sendo $1 + a_3 < b_3$:

$$m, a_1a_2a_3 \leqslant x \leqslant m, a_1a_2a_3 + \frac{1}{10^3} = m, a_1a_2 + \frac{1 + a_3}{10^3}$$

$$< m, a_1a_2 + \frac{b_3}{10^3} = m, a_1a_2b_3 = M, b_1b_2b_3 \leqslant y\,,$$

de modo que $x < y$.

- Sendo $1 + a_3 = b_3$,
usando a hipótese de expansões não 9-terminantes, tomemos, digamos, $a_5 \neq 9$, de modo que $a_5 < 9$. Assim, temos $x = m, a_1a_2a_3a_4a_5 \ldots = M, b_1b_2b_3a_4a_5 \ldots$ e $y = M, b_1b_2b_3b_4b_5 \ldots$. Então:

$$x \leqslant m, a_1a_2a_3a_4a_5 + \frac{1}{10^5} = m, a_1a_2a_3 + \frac{a_4}{10^4} + \frac{a_5}{10^5} + \frac{1}{10^5}$$

$$< m, a_1a_2a_3 + \frac{9}{10^4} + \frac{9}{10^5} + \frac{1}{10^5} = m, a_1a_2a_3 + \frac{9}{10^4} + \frac{1}{10^4} = m, a_1a_2a_3 + \frac{1}{10^3}\,,$$

de modo que:

$$x < m, a_1a_2a_3 + \frac{1}{10^3} = m, a_1a_2 + \frac{1 + a_3}{10^3} = m, a_1a_2 + \frac{b_3}{10^3} = M, b_1b_2b_3 \leqslant y\,,$$

o que mostra que $x < y$.

Assim, somos levados a formalizar essas ideias na seguinte

Definição 7.21 (*Ordem entre reais absolutos*) -

Dados x e y números reais absolutos, escrevemos $x < y$, ou $y > x$, e dizemos que "x é menor do que y", ou que "y é maior do que x", quando, e só quando, valerem:

- $x \neq y$ *;*
- *e, ademais, sendo eles representados por*

$$x = m, a_1a_2 \ldots$$
$$y = M, b_1b_2 \ldots\ ,$$

tivermos: ou ($m < M$), ou ($m = M$, mas $a_n < b_n$, onde n é o primeiro índice i tal que $a_i \neq b_i$) .

Exemplo 7.22 -

Vale $2,444\,444\ldots < 2,5 = 2,500\,000\ldots$, *pois* $m = M = 2$, *mas* $a_1 = 4 < 5 = b_1$. *Note que a conclusão continua a mesma se escrevermos* $2,5$ *como* $2,499\,999\ldots$, *só que agora temos* $m = M$, $a_1 = b_1$ *e* $a_2 = 4 < 9 = b_2$. *A proposição seguinte garante que a conclusão nunca muda com a troca por eventuais expansões decimais equivalentes.*

Exemplo 7.23 -

Sendo x *um número real absoluto não nulo, então* $0 < x$.
Com efeito, sendo $x = M, b_1b_2b_3\ldots$ *uma expansão decimal de tal número, como ele não é nulo, temos:*

- *se* $M = 0$, *existe um primeiro* $b_n \neq 0$, *ou seja,* $0 = a_n < b_n \neq 0$; *logo,* $0 < x$;
- *se* $M \neq 0$, *temos diretamente:* $0 = m < M$; *logo,* $0 < x$.

Exemplificada a aplicação da definição, passemos a mostrar que a mesma está bem feita, examinando duas sutilezas envolvidas na mesma. A primeira trata da necessidade de garantirmos que os dois números a comparar são, antes de mais nada, distintos. O exercício a seguir faz o leitor pensar sobre isso.

Exercício 160 -

Por que a Definição 7.21

i). não permite afirmar que $0,999\ldots < 1,000\ldots$ *?*
ii). não permite afirmar que $1,2999\ldots < 1,3000\ldots$ *?*

A segunda sutileza na definição de ordem entre números reais está no fato de que a comparação entre dois reais (distintos) independe da escolha da expansão decimal usada. Em termos mais precisos, isso é o que garante a seguinte proposição.

Proposição 7.24 -

A definição de ordem entre os reais absolutos está bem feita, na medida em que a conclusão da ordem relativa entre dois números absolutos dados independe das expansões decimais usadas para representá-los.

Prova:

Usando um exemplo significativo, vejamos a ideia. Sendo $x = 1/4$, achemos quais y verificam $x < y$, observando que x tem duas representações: $0,250\ \ldots$ e $0,24999\ldots$. Aplicando a definição com a segunda expansão temos que é impossível termos algo do tipo $0,24999\ldots < y = 0,24abc\ldots$. Como $0,24999\ldots = 0,25000\ldots$, a próxima possibilidade a examinar é $0,24999\ldots < y = 0,25abc\ldots$, com ao menos um dígito não nulo entre $a, b, c\ldots$, possibilidade esta que é evidentemente sempre verdadeira.

Resumindo: de acordo com a segunda expansão de x, os $y > x$ são os da forma $y = 0,25abc\ldots$, onde algum dígito, entre $a, b, c, \ldots$, é não nulo. É mais fácil ainda ver que esta é a conclusão que chegaríamos usando a primeira expansão de x.

Fica para o leitor formalizar a prova para quaisquer x e y. Também fica para o leitor examinar o caso em que x tem apenas uma representação, mas y tem duas.

CQD.

Exercício 161 -

Decida qual entre os dois números reais absolutos dados é o maior:

i). $3,1415161711111\ldots$ *e* $3,14151617102122122212222122222\ldots$ *;*

ii). $1,33333$ *e* $1,333\ldots$ *.*

Nossa próxima etapa é estender a ordem dos reais absolutos para os números reais quaisquer.

Observação 7.25 -

Para o correto entendimento da definição que se segue, recordemos que convencionamos escrever

$$0 = 0,000\ldots = +0,000\ldots = -0,000\ldots$$

e, então, zero é o único número real que tem tanto o sinal $+$*, como o sinal* $-$*.*

Definição 7.26 *(ordem entre reais quaisquer) -*

Sendo x e y dois números reais distintos, escreveremos $x < y$ e diremos que "x é menor do que y" quando, e somente quando:

- *ou ambos tem o sinal $+$ e verificam $|x| < |y|$;*
- *ou ambos tem o sinal $-$ e verificam $|y| < |x|$;*
- *ou x é negativo e y positivo.*

Exemplo 7.27 -

i). $0 < x$ *para todo x número real positivo*
$($*Com efeito, como $0 = +0$, ambos têm o sinal $+$ e, como $|x|$ é um número absoluto não nulo, sabemos que $0 < |x|$.);*

ii). $x < 0$ *para todo x número real negativo;*

iii). $-2 < -1$, *ou seja* $-2,000\ldots < -1,000\ldots$, *pois que* $1,000\ldots < 2,000\ldots$ *;*

iv). $-5000,000\ldots < +0,0005000\ldots$.

Convenções e Notações.

- Como foi costume fazer nos campos numéricos já estudados, podemos usar $x > y$ para dizer $y < x$. Também usaremos $x \leqslant y$ para dizer que vale $x = y$, ou $x < y$. Semelhantemente para $x \geqslant y$.
- Se $x \geqslant 0$, diremos que x é não-negativo.
- Se $x \leqslant 0$, diremos que x é não-positivo.

Exemplo 7.28 -

Com $x \leqslant 1$ indicamos qualquer x real que, ou verifica $x < 1$, ou verifica $x = 1$.

Observação 7.29 -

Sendo x e y números reais absolutos, então é imediato verificarmos que $x \leqslant y$ (na ordem de reais absolutos) $\iff$ $+x \leqslant +y$ (na ordem de números reais). Como, na prática, identificamos $+r$ com r, podemos dizer que

$$x \leqslant y \text{ como reais absolutos} \iff x \leqslant y \text{ como números reais,}$$

ou seja: a ordem dos números reais estende a dos números reais absolutos!
Em particular, podemos dizer que os números absolutos são os números reais x *verificando* $x \geqslant 0$.

Exercício 162 -

Ache os menores a *e* b, *tais que* $0,\overline{5} < 0,ab$.

Exercício 163 -

Coloque em ordem $\leqslant$ *:*

$$2,55\,, \quad 2\,,\overline{54}\,, \quad \frac{9}{4}, \quad \frac{22}{9}\,.$$

Exercício 164 -

Verifique qual entre os dois números reais -10 *e* $-10,999\ldots$ *é o maior.*

Proposição 7.30 -

A ordem $\leqslant$ *entre números reais tem as seguintes propriedades:*

i). $x \leqslant x, \forall x \in \mathbb{R}$ *;*

ii). $x \leqslant y$ *e* $y \leqslant x \;\Rightarrow\; x = y, \forall x, y \in \mathbb{R}$ *;*

iii). $x \leqslant y$ *e* $y \leqslant z \Rightarrow x \leqslant z, \forall x, y, z \in \mathbb{R}$ *.*

Prova:

Essas afirmações são obviedades geométricas. A prova algébrica, apesar de ter de considerar os sinais dos números envolvidos, é direta e fica como exercício para o leitor. CQD.

Proposição 7.31 -

A ordem entre números reais verifica a chamada Lei da Tricotomia: para cada dois reais quaisquer, x *e* y, *vale uma, e somente uma, das seguintes possibilidades:*

$$ou\;\; x = y, \;\; ou\;\; x < y, \;\; ou\;\; y < x\,.$$

Prova:

Basta verificar que a Definição anterior cobre todas as possibilidades de sinal para x e y. Deixamos os detalhes para o leitor.

CQD.

Exercício 165 -

Convença-se que a definição de ordem podia ter sido enunciada da seguinte forma: dados dois reais distintos quaisquer x e y, então:

i). se ambos forem não-negativos, então ou $x < y$, ou $y < x$, de acordo com a definição de ordem entre reais absolutos;

ii). se um deles for não-negativo e o outro for negativo, então o negativo será menor do que o não-negativo;

iii). se ambos forem negativos, então decide-se se $x < y$, ou $y < x$, comparando $-x$ e $-y$.

Nossa proxima tarefa é mostrar que a definição de ordem entre reais absolutos, ou entre reais quaisquer, foi feita conforme o Princípio da Permanência de Hankel, ou seja: efetivamente, fizemos uma extensão da relação de ordem que existia entre os números racionais.

Bem entendido, temos de mostrar que comparar dois números racionais por meio das respectivas representações fracionárias, a/b e c/d, dá no mesmo que comparar as respectivas expansões decimais. A primeira dessas comparações envolve trabalhar com as frações equivalentes ad/bd e bc/bd, enquanto que a segunda envolve aplicação da definição de ordem de reais, conforme vimos neste capítulo.

O teorema seguinte confirma que realmente, no caso básico de números racionais positivos, a extensão foi feita de acordo com o Princípio da Permanência de Hankel.

Teorema 7.32 -

Consideremos dois racionais positivos, $r \neq s$, representados, respectivamente, pelas frações a/b e c/d, onde a, b, c, d são números inteiros positivos. Sejam, ademais, $r = m, a_1a_2a_3\dots$ e $s = M, b_1b_2b_3\dots$ as expansões decimais (não 9-terminantes) desses racionais. Assim, teremos que:
$a/b < c/d$ na ordem dos números racionais $\iff$
$m, a_1a_2a_3\dots < M, b_1b_2b_3\dots$ na ordem dos números reais.

Prova:

$\boxed{\Rightarrow}$

Fazendo divisão euclidiana, obtemos:

$$\frac{a}{b} = m + \frac{R_1}{b}, \quad \frac{c}{d} = M + \frac{R_2}{d}, \quad \text{com} \quad 0 \leqslant \frac{\mathrm{R}_1}{\mathrm{b}}, \frac{\mathrm{R}_2}{\mathrm{d}} < 1\,,$$

de modo que, na ordem dos racionais: $a/b < c/d \Rightarrow m \leqslant M$ (Por quê?), e teremos duas possibilidades a examinar:

• $m < M$
Neste caso, diretamente da definição de ordem entre reais, temos que
$r = m, a_1a_2a_3\dots < M, b_1b_2b_3\dots = s$.

• $m = M$
Neste caso, como os dois racionais são distintos, terá de existir uma primeira casa onde as expansões terão dígitos diferentes, digamos: $a_1 = b_1$, $a_2 = b_2$ e $a_3 \neq b_3$. Bastará, então, mostrar que a hipótese $a/b < c/d$ implica $a_3 < b_3$.

Ora, isso tem de ser verdade, pois a suposição $a_3 > b_3$ nos leva a uma impossibilidade. Com efeito, como a divisão euclidiana produz

$$\frac{a}{b} = m + \frac{a_1}{10} + \frac{a_2}{100} + A, \quad \frac{c}{d} = M + \frac{a_1}{10} + \frac{a_2}{100} + B,$$

teremos que, na ordem dos racionais, $a/b < c/d$ implica $A < B$, e daí a suposição $a_3 > b_3$, nos levaria (sempre na ordem dos racionais!) ao seguinte resultado absurdo:

$$A \geqslant \frac{a_3}{1000} \geqslant \frac{1 + b_3}{1000} > B \quad \therefore \quad A > B.$$

$\boxed{\Leftarrow}$

Agora, o objetivo é mostrar que $m, a_1a_2a_3 \dots < M, b_1b_2b_3\dots$ (na ordem dos reais) $\Rightarrow a/b < c/d$ (na ordem dos racionais) $\iff$ $ad < bc$.

• $m < M$

Temos $M = m + k$, com $k \geqslant 1$. Logo, a divisão euclidiana de a/b e c/d produz: $a = bm + R_1$ e $c = dM + R_2 = dm + dk + R_2$, de modo que: $ad = bdm + dR_1$ e $bc = bdm + bdk + bR_2$. Consequentemente, vemos que

$$ad < bc \iff dR_1 < bdk + bR_2 \,.$$

Assim, basta observar que $0 \leqslant R_1 < b$ implica

$$0 \leqslant dR_1 < bd \leqslant bdk \leqslant bdk + bR_2 \quad \therefore \quad dR_1 < bdk + bR_2 \,.$$

• $m = M$

Neste caso, $m, a_1a_2a_3 \ldots < m, b_1b_2b_3 \ldots$, logo, terá de existir uma primeira casa decimal, digamos a terceira, tal que: $a_1 = b_1$, $a_2 = b_2$ e $a_3 < b_3$. Bastará, então, mostrar que isso implica $a/b < c/d$ (na ordem dos racionais). Ora, como temos $1 + a_3 \leqslant b_3$, segue que (na ordem dos racionais):

$$\frac{a}{b} < m+\frac{a_1}{10}+\frac{a_2}{100}+\frac{a_3}{1000}+\frac{1}{1000} \leqslant m+\frac{a_1}{10}+\frac{a_2}{100}+\frac{b_3}{1000} = M+\frac{b_1}{10}+\frac{b_2}{100}+\frac{b_3}{1000} \leqslant \frac{c}{d}\,.$$

CQD.

7.5 O campo dos números reais tem a Propriedade do Contínuo

Nesta pequena, mas decisiva, seção combinaremos o Teorema Fundamental da Geometria Analítica com a ordem dos números reais, com o objetivo de produzir uma muito útil versão numérica do Postulado do Contínuo. Como a maioria dos resultados são basicamente “traduções” de resultados geométricos, deixaremos a prova dos mesmos como um fácil exercício para o leitor.

Iniciamos com a interpretação geométrica para a ordem dos reais:

Exercício 166 -

Prove a seguinte afirmação: dados números reais distintos x e y, tem-se $x < y$ se, e somente se, no eixo cartesiano, x for a coordenada de um ponto que está à esquerda do ponto que tenha y para coordenada. Ou seja,

$$\boxed{\textit{sendo } x = x(P) \textit{ e } y = x(Q)\,, \textit{ então}: x < y \iff P \textit{ à esquerda de } Q\,.}$$

A ordenação do conjunto $\mathbb{R}$ nos permite introduzir o conceito de intervalo, o qual é a versão numérica de segmento de reta do eixo euclidiano:

Definição 7.33 -

Por intervalo fechado *de extremos x e y (onde x e y são números reais, verificando $x \leqslant y$), entendemos o conjunto*

$$[x, y] = \{z \in \mathbb{R} | \, x \leqslant z \leqslant y\}.$$

Exercício 167 -

Conforme notação introduzida anteriormente, $P(x)$ denota o ponto da reta euclidiana que tem $x \in \mathbb{R}$ como coordenada. Assim, explique por que o intervalo $[x, y]$ pode ser interpretado como sendo o conjunto dos números reais z, tais que $P(z)$ seja um ponto do segmento de reta $P(x)P(y)$.

Definição 7.34 -

Uma sequência de intervalos fechados $[x_n, y_n]$ é dita encaixante *se, e só se, verificar que:*

$$\cdots \subseteq [x_n, y_n] \subseteq \cdots \subseteq [x_1, y_1] \subseteq [x_0, y_0] \, .$$

Exercício 168 -

Prove que uma sequência de intervalos fechados $[x_n, y_n]$ é encaixante se, e somente se, verificar que $x_{n+1} \geqslant x_n$ e $y_{n+1} \leqslant y_n$, para todos os $n \in \mathbb{N}$.

Exercício 169 -

Mostre que uma sequência de intervalos $[x_n, y_n]$ é encaixante se, e somente se, a sequência de segmentos de reta $P(x_n)P(y_n)$ for encaixante.

Definição 7.35 -

Uma sequência encaixante de intervalos fechados $[x_n, y_n]$ é dita ser evanescente *se, e só se, a correspondente sequência encaixante de segmentos de reta $P(x_n)P(y_n)$ for evanescente.*

Com essa definição, podemos agora traduzir numericamente o Postulado do Contínuo (veja Capítulo 5) ou Princípio dos Segmentos Evanescentes.

Teorema 7.36 (*Teorema dos Intervalos Evanescentes/Propriedade do Contínuo*)
Para cada sequência evanescente de intervalos, $[x_n, y_n]$, existe exatamente um número real x pertencente a cada um dos intervalos da sequência. Isso é, existe exatamente um $x \in \mathbb{R}$, tal que $x \in [x_n, y_n]$, para todo $n \in \mathbb{N}$.

Exercício 170 -

Prove o teorema anterior.

É muito importante o leitor se convencer que a Propriedade do Contínuo é uma propriedade "muito forte": corresponde a uma exigência muito grande que só pode ser satisfeita por um campo suficiente rico de números, como é o caso de $\mathbb{R}$. Vejamos. Antes de mais nada, iniciemos observando que a noção de intervalo fechado se aplica a qualquer campo ordenado $[\mathbb{X}, <,]$. Com efeito, são os conjuntos da forma:

$$[x, y]_{\mathbb{X}} = \{z \in \mathbb{X} \,|\, x \leqslant z \leqslant y\}, \text{com x, y} \in \mathbb{X}.$$

Exemplifiquemos. Sendo $\mathbb{X} = \mathbb{Z}$, $x = 1$ e $y = 5$, então

$$[x, y]_{\mathbb{Z}} = [1, 5]_{\mathbb{Z}} = \{1, 2, 3, 4, 5\}.$$

É imediato o leitor verificar que, sendo $\mathbb{X} \subset \mathbb{R}$, então

$$[x, y]_{\mathbb{X}} = [x, y] \cap \mathbb{X}.$$

Essa observação nos permite denotar o $\mathbb{Q}$-intervalo fechado $[1, 5]_{\mathbb{Q}}$, que consiste em todos os números racionais r verificando $1 \leqslant r \leqslant 5$, por:

$$[1, 5]_{\mathbb{Q}} = [1, 5] \cap \mathbb{Q}.$$

Exercício 171 -

Caracterizar as sequências encaixantes de $\mathbb{Z}$-intervalos fechados. No caso de uma tal sequência ser, ademais, evanescente, mostre que cedo ou tarde seus intervalos se reduzem a um único número e que, como tal, verificam trivialmente a Propriedade do Contínuo.

Exercício 172 -

Passemos a mostrar que o campo dos números racionais não tem a Propriedade do Contínuo. Para tal, consideremos o seguinte exemplo de sequência encaixante de

$\mathbb{Q}$-intervalos fechados, construída em torno do número real $0,505005000500005\ldots$*:*

$$\begin{aligned}
&I_1 = [0,5\,;\ 0,6] \cap \mathbb{Q}\\
&I_2 = [0,50\,;\ 0,51] \cap \mathbb{Q}\\
&I_3 = [0,505\,;\ 0,506] \cap \mathbb{Q}\\
&I_4 = [0,50500\,;\ 0,50501] \cap \mathbb{Q}\\
&I_5 = [0,505005\,;\ 0,505006] \cap \mathbb{Q}\\
&\ldots\ldots
\end{aligned}$$

Pede-se provar que a sequência dos $\mathbb{Q}$-intervalos I_n é evanescente, mas não tem ponto comum.

7.6 Adição de números reais

Nossa próxima tarefa é tratar das quatro operações aritméticas básicas entre números reais, a saber: adição, subtração, multiplicação e divisão. Como viemos fazendo, queremos fazer isso estendendo as correspondentes operações sobre os números racionais. [7]

Queremos estender a adição dos números racionais para os reais, e para isto, teremos de partir das expansões decimais correspondentes. Um exame superficial poderia nos levar a crer que nossa tarefa é simples. Por exemplo, é natural esperarmos que a soma dos reais

$$1,01001000100001\ldots$$
$$3,02002000200002\ldots\ ,$$

seja o real

$$4,030030003000003\ldots\ .$$

Contudo, um exame mais demorado mostra que a tentativa de *definição direta* da adição entre números reais quaisquer nos levaria a um emaranhado sem fim de casos particulares. Com efeito, procure o leitor descrever o resultado da adição de

$$1,01001000100001\ldots\ ,$$

com o real

$$3,09009000900009\ldots\ .$$

[7]Para não nos alongarmos, discutiremos em detalhe apenas os dois casos principais: a adição (nesta seção) e multiplicação (próxima seção).

Nesse caso, a tarefa já não é tão simples, e menos ainda é o caso da adição de

$$1,01001000100001\ldots$$

com

$$3,09009900099900009999\ldots\ .$$

Assim, para evitar uma tamanha complicação, *vamos proceder de uma maneira indireta*, usando as aproximações racionais dos reais a serem somados, e fazendo uso da fácil e familiar adição de racionais.

Feitos estes preliminares, passemos a definir a soma $x+y$ de dois números reais quaisquer, x e y. De saída, descartamos as possibilidades triviais em que ao menos uma dessas parcelas é nula, pois é óbvio que devemos ter $0+y=y$ e $x+0=x$. Assim, vamos nos concentrar nas possibilidades em que ambas as parcelas são não nulas, as quais dividiremos em três casos: x e y positivos, x e y negativos, e x e y de sinal contrário.

– Adição de dois reais positivos

Dados x e y reais positivos, com expansões decimais

$$\begin{aligned} x &= m, a_1 a_2 \ldots \\ y &= M, b_1 b_2 \ldots\ , \end{aligned}$$

sejam, para cada $n \geqslant 1$, os números racionais

$$x_n = m, a_1 a_2 \ldots a_n \quad \text{e} \quad y_n = M, b_1 b_2 \ldots b_n\,. \tag{7.1}$$

Da definição de expansão decimal, sabemos que valem:

$$x_n \leqslant x \leqslant x_n + \frac{1}{10^n}$$

$$y_n \leqslant y \leqslant y_n + \frac{1}{10^n}\,.$$

Ora, os x_n e y_n são números racionais e assim, *no caso particular em que x e y também são racionais*, das desigualdades acima tiramos[8], agora na ordem dos números racionais:

$$x_n + y_n \leqslant x + y \leqslant x_n + y_n + \frac{2}{10^n}\,. \tag{7.2}$$

[8] Lembre que, para a,b,c,d racionais, $a \leqslant b$ e $c \leqslant d$ implicam $a+c \leqslant b+d$.

Assim, *se x e y forem racionais*, a soma $x+y$ estará em cada elemento da sequência de intervalos $[x_n + y_n\, , \, x_n + y_n + 2/10^n]$, a qual é encaixante e evanescente, e, por isso – segundo a Propriedade do Contínuo –, só pode ter $x + y$ como elemento comum. Com efeito, o encaixante sai imediatamente das desigualdades a seguir, e a evanescência é imediata:

$$\begin{aligned} x_n \leqslant x_{n+1} \leqslant x \leqslant x_{n+1} + \frac{1}{10^{n+1}} \leqslant x_n + \frac{1}{10^n} \\ y_n \leqslant y_{n+1} \leqslant y \leqslant y_{n+1} + \frac{1}{10^{n+1}} \leqslant y_n + \frac{1}{10^n}\,. \end{aligned}$$

Consequentemente, como estamos procurando estender a adição de números racionais para números reais, fica natural *definirmos* a soma $x + y$, no caso de x e y reais positivos, como sendo o único número real comum à sequência de intervalos encaixante e evanescente que encontramos acima. (Não deixe o leitor de observar que o fato de essa sequência ser encaixante e evanescente independe de x e y serem racionais ou irracionais.)

Definição 7.37 (*adição de reais positivos*) -

Dados x e y números reais positivos, com expansões decimais

$$\begin{aligned} x &= m, a_1 a_2 \dots \\ y &= M, b_1 b_2 \dots\,, \end{aligned}$$

sejam, para cada $n \geqslant 1$, os números racionais

$$x_n = m, a_1 a_2 \dots a_n \quad e \quad y_n = M, b_1 b_2 \dots b_n\,.$$

Assim sendo, a **adição** *dos números reais positivos x e y produz um resultado chamado* **soma***, o qual é denotado por $x+y$, e é definido como sendo o único número real comum a todos os elementos da sequência de intervalos encaixantes e evanescentes:*

$$[x_n + y_n\, , \, x_n + y_n + \frac{2}{10^n}]\,.$$

Observe que a definição anterior envolve um procedimento, mas que ele não nos dá explicitamente a expansão decimal de $x+y$ em termos das expansões decimais de x e de y. Apesar disso, ela nos fornece aproximações racionais de $x + y$ tão boas quanto se queira. De fato, basta notar que $x_n + y_n$ e $x_n + y_n + 2/10^n$ são aproximações racionais, por falta e por excesso, para o número real $x + y$, e que o "erro" $2/10^n$ pode ser tornado tão pequeno quanto desejarmos.[9]

[9]Mas *atenção!* com erro menor ou igual a $2/10^n$, e não $1/10^n$.

A possibilidade de termos aproximações racionais tão boas quanto queiramos para a soma nos diz que, do ponto de vista das aplicações práticas, por exemplo, esse procedimento é satisfatório.

Exemplo 7.38 -

Seja somar $0,58000\ldots$ *e* $0,333000\ldots$ *. Aplicando o procedimento da definição, obtemos a sequência de intervalos evanescentes:*

$[0,8;1,0] \supset [0,91;0,93] \supset [0,913;0,915] \supset [0,9130;0,9132] \supset [0,91300;0,91302] \supset \cdots$

da qual fica fácil vermos que $0,58000\ldots + 0,333000\ldots = 0,913000\ldots = 0,913$ *.*

Exercício 173 -

Verifique que somando $0,58$ *e* $0,333$ *como números racionais (ou seja: por meio de suas representações fracionárias) obteremos o mesmo resultado do exemplo anterior.*

Exemplo 7.39 -

Vendo $1/3 + 2/3$ *como uma soma de números reais, obter o valor dessa soma com erro de no máximo uma unidade da terceira casa decimal.*

Aplicando a definição e ao mesmo tempo escrevendo as respectivas aproximações, teremos:
$x_1 + y_1 = 0,3 + 0,6 = 0,9 \ \rightarrow \ [0,9\,;\,1,1] \ \rightarrow \ 1/3 + 2/3 \simeq 1,0 \pm 0,1$
$x_2 + y_2 = 0,33 + 0,66 = 0,99 \ \rightarrow \ [0,99\,;\,1,01] \ \rightarrow \ 1/3 + 2/3 \simeq 1,00 \pm 0,01$
$x_3 + y_3 = 0,333 + 0,666 = 0,999 \ \rightarrow \ [0,999\,;\,1,001] \ \rightarrow \ 1/3 + 2/3 \simeq 1,000 \pm 0,001$.

Exemplo 7.40 -

Usemos nossa definição de adição para somar os números de um dos nossos exemplos iniciais:

$$1,01001000100001\ldots + 3,02002000200002\ldots \ = ?$$

Agora, a sequência de intervalos evanescentes fica:

$[4,0;4,2] \supset [4,03;4,05] \supset [4,030;4,032] \supset [4,0300;4,0302 \supset [4,03003;4,03005] \supset \cdots$

de modo que fica fácil concluirmos que

$$1,01001000100001\ldots + 3,02002000200002\ldots = 4,030030003000003\ldots \ .$$

(Exercício: redija o argumento da conclusão.)

Exercício 174 -

V ou F? Justifique.

i) $0,\overline{1}+0,\overline{3}=0,\overline{4}$ *ii)* $0,\overline{9}+0,\overline{1}=1,\overline{0}$.

Exercício 175 -

Determine uma aproximação racional, e com erro menor do que $1/10^5$*, para a soma dos reais positivos:* $x=2,79323189\ldots$ *e* $y=13,83452153\ldots$ *.*

Exercício 176 -

Some $0,32\overline{15}$ *e* $2,134\overline{120}$ *como números reais e conclua que o resultado é, de fato, o esperado: a expansão decimal do racional*

$$\left(\frac{3215-32}{9900}\right)+\left(2+\frac{134120-134}{999000}\right) .$$

Exercício 177 -

Seja M *um inteiro positivo, e* $x=m,a_1a_2\ldots$ *um real positivo. Usando soma de reais positivos, prove que* $x+M=N,a_1a_2\ldots$ *, onde* $N=m+M$ *.*

Exercício 178 -

Amplie a Definição 7.37, de modo a incluir os casos $x\geqslant 0$ *e* $y\geqslant 0$*. Com isso, teremos as seguintes novas possibilidades:* $x>0, y=0$*;* $x=0, y>0$ *e* $x=y=0$*, para as quais pede-se provar que teremos, respectivamente:* $x+0=x$*;* $0+y=y$ *e* $0+0=0$*. Em particular, note que – se* $x\geqslant 0$ *for racional – o resultado* $x+0=x$ *independe de a adição ser feita no sentido dos números racionais ou no dos reais.*

– Adição de dois reais negativos

A adição de dois reais negativos segue um caminho óbvio:

Definição 7.41 (*adição de reais negativos*) -

A adição *de dois números reais negativos, x e y, produz uma soma $x+y$ que é obtida por meio da adição dos reais positivos $|x|$ e $|y|$:*

$$x + y = -\big(|x| + |y|\big)\,.$$

Exemplo 7.42 -

Diretamente da definição:

$$(-1,25000\dots) + (-2,52000\dots) = -(1,25000\dots + 2,52000\dots) = -3,77000\dots\ .$$

Exercício 179 -

Determine uma aproximação racional, por excesso e com erro menor do que $1/10^3$, para a soma dos reais negativos: $x = -2,79323189\dots$ e $y = -13,83452153\dots$.

Exercício 180 -

Dados x e y dois reais negativos, $x = -m,a_1a_2\dots$ e $y = -M,b_1b_2\dots$, sejam $x_n = m,a_1a_2\dots a_n$ e $y_n = M,b_1b_2\dots b_n$ (note a ausência do sinal menos). Verifique que:

$$-x_n - \frac{1}{10^n} \leqslant x \leqslant -x_n, \quad -y_n - \frac{1}{10^n} \leqslant y \leqslant -y_n\,.$$

A partir disso e da definição acima, conclua que:

$$-x_n - y_n - \frac{2}{10^n} \leqslant x + y \leqslant -x_n - y_n\,.$$

Exercício 181 -

Ampliando a Definição 7.41, acrescentando os casos $(x<0, y=0)$ e $(x=0, y<0)$, verifique que teremos: $x+0=x$ e $0+y=y$, respectivamente.

– Adição de dois reais de sinais opostos

Nos casos em que os números reais x e y têm o mesmo sinal, é imediato da definição que a adição é uma operação comutativa: $x + y = y + x$. Tendo isso em vista, bem como o fato de que ela é comutativa no caso de números racionais quaisquer, é natural que, nos casos onde x e y tenham sinais opostos, também exijamos que essa propriedade continue valendo. É o que faremos e, por isso, na definição a seguir, tratamos apenas do caso em que x é positivo e y negativo.

Definição 7.43 -

Dados x número real positivo e y real negativo, com expansões decimais

$$\begin{aligned} x &= m, a_1 a_2 \ldots \\ y &= -M, b_1 b_2 \ldots \ , \end{aligned}$$

sejam – pelas expansões de x e $|y|$, e para cada $n \geqslant 1$ – os números racionais:

$$x_n = m, a_1 a_2 \ldots a_n \quad e \quad |y|_n = M, b_1 b_2 \ldots b_n \, .$$

Assim, a adição *do número real positivo x e o real negativo y produz um resultado chamado* soma*, o qual é denotado por $x + y$, e é definido como sendo o único número real comum a todos os elementos da sequência de intervalos encaixante e evanescente:*

$$\left[x_n - |y|_n - \frac{1}{10^n} \, , \, x_n - |y|_n + \frac{1}{10^n} \right] .$$

Precisamos mostrar que esta definição está bem feita. Isso envolve mostrar que a sequência de intervalos envolvida realmente é encaixante e evanescente e que, ademais, no caso particular em que x e y são racionais, ela coincide com a soma $x + y$ de racionais, de modo que estamos efetivamente estendendo a adição dos racionais para os reais.

Provaremos isso de modo bastante semelhante ao do caso de x e y positivos. Iniciamos observando que, das expansões decimais de x e $|y|$, valem as seguintes desigualdades na ordem dos reais:

$$\begin{aligned} x_n \leqslant x \leqslant x_n + \frac{1}{10^n} \\ |y|_n \leqslant |y| \leqslant |y|_n + \frac{1}{10^n} \ . \end{aligned}$$

No caso particular em que x e y são números racionais, a segunda desigualdade acima pode ser reescrita como:

$$-|y|_n - \frac{1}{10^n} \leqslant -|y| \leqslant -|y|_n \ ,$$

de modo que, pelas propriedades da ordem entre racionais, obteremos:

$$\big(x_n - |y|_n\big) - \frac{1}{10^n} \leqslant x - |y| \leqslant \big(x_n - |y|_n\big) + \frac{1}{10^n}\,.$$

Mas, $y = -|y|$, de modo que:

$$\big(x_n - |y|_n\big) - \frac{1}{10^n} \leqslant x + y \leqslant \big(x_n - |y|_n\big) + \frac{1}{10^n}\,,$$

e assim vemos que, se x e y fossem racionais, teríamos

$$x + y \in [x_n - |y|_n - \frac{1}{10^n}\,,\, x_n - |y|_n + \frac{1}{10^n}], \quad \forall n \geqslant 1\,.$$

Ora, a Propriedade do Contínuo –como essa sequência é encaixante e evanescente–, garante que somente $x + y$ pode ser elemento comum a todos os intervalos. Com efeito, o encaixante sai imediatamente das propriedades da ordem dos racionais e da soma das desigualdades (note que, agora, não aparecem nem x e nem $|y|$, elas envolvem apenas números racionais):

$$\begin{aligned} x_n \leqslant x_{n+1} \leqslant x_{n+1} + \frac{1}{10^{n+1}} \leqslant x_n + \frac{1}{10^n} \\ -|y|_n - \frac{1}{10^n} \leqslant -|y|_{n+1} - \frac{1}{10^{n+1}} \leqslant -|y|_{n+1} \leqslant -|y|_n\,, \end{aligned}$$

o que resulta em:

$$x_n - |y|_n - \frac{1}{10^n} \leqslant x_{n+1} - |y|_{n+1} - \frac{1}{10^{n+1}} \leqslant x_{n+1} - |y|_{n+1} + \frac{1}{10^{n+1}} \leqslant x_n - |y|_n + \frac{1}{10^n}\,,$$

e a evanescência é imediata.

Exemplo 7.44 -

Seja somar $1,222\ldots + (-2,111)$. *Procedendo como indicado, obteremos:*

$x_1 - |y|_1 = 1,2 - 2,1 = -0,9 \;\to\; [-1,0\,;\,-0,8]$
$x_2 - |y|_2 = 1,22 - 2,11 = -0,89 \;\to\; [-0,90\,;\,-0,88]$
$x_3 - |y|_3 = 1,222 - 2,111 = -0,889 \;\to\; [-0,890\,;\,-0,888]$
$x_4 - |y|_4 = 1,2222 - 2,1110 = -0,8888 \;\to\; [-0,8889\,;\,-0,8887]$
e prosseguindo semelhantemente, percebe-se que temos a sequência encaixante e evanescente:

$$\begin{aligned} [-1,0\,;-0,8] \supset [-0,90\,;-0,88] \supset [-0,890\,;-0,888] \supset [-0,8889\,;\,-0,8887] \supset \\ \supset [-0,88879\,;\,-0,88877] \supset [-0,888778\,;\,-0,888779] \supset \cdots\,, \end{aligned}$$

de onde pode-se ver facilmente que $1,222\ldots + (-2,111) = -0,888777\ldots$ *.*

Como uma confirmação, verifique o leitor que

$$-1,222222\ldots+(-0,888777\ldots) = -\big(1,222222\ldots+0,888777\ldots\big) = -2,111000\ldots \ .$$

Exemplo 7.45 -

Seja calcular o valor da soma $1,222\ldots + (-2,111)$ *, com um erro garantido de no máximo uma unidade da quinta casa decimal.*

Observemos que o intervalo $[-0,8889\,;\,-0,8887]$ *nos diz que a soma é aproximadamente* $-0,888$ *, e que o dígito da quarta casa é um dentre* $9,8,7$ *. Por sua vez, o próximo intervalo,* $[-0,88879\,;\,-0,88877]$*, nos diz que a soma é aproximadamente* $-0,8887$ *, e que o dígito da quinta casa é um dentre* $9,8,7$ *. Assim, podemos dizer que a soma vale* $-0,88878$ *, com um erro no máximo* $\pm 0,00001$ *.*

Exemplo 7.46 -

Usando que $(-0,333\ldots) + 0,58000\ldots = 0,58000\ldots + (-0,333\ldots)$*, vamos determinar esta soma usando que ela é o único número real comum a todos os elementos da sequência de intervalos:*

$$\begin{aligned}[0,1\,;0,3] \supset [0,24\,;0,26] \supset\ & [0,246\,;0,248] \\ & \supset [0,2466\,;\ 0,2468] \supset [0,24666\,;\ 0,24668] \supset \ldots\ ,\end{aligned}$$

de onde se vê facilmente (Exercício!) que $(-0,333\ldots)+0,58000\ldots = 0,24666\ldots$ *.*

Como uma confirmação, verifique o leitor que $0,24666\ldots + 0,333\ldots = 0,58$ *.*

Exercício 182 -

i). Calcule a soma $1,\overline{3} + (-2,5\overline{12})$ *como números reais.*

ii). Calcule a soma $1,\overline{3} + (-2,5\overline{12})$ *como números racionais.*

iii). Você obteve respostas iguais em (i) e (ii)?

– Compatibilidade da adição com a ordem de reais

O teorema a seguir generaliza, para os números reais, a imprescindível e já abordada compatibilidade da adição com a ordem no campo dos números racionais.

Teorema 7.47 -

A adição de números reais é compatível com a relação de ordem, ou seja, sendo $a, b, c \in \mathbb{R}$*:*

$$a < b \iff a + c < b + c, \ \forall c \in \mathbb{R} \ .$$

Prova:

Esse resultado é geometricamente óbvio. Contudo, sua prova algébrica requer um argumento elaborado e a deixaremos para a Leitura Complementar 7.11.

CQD.

7.7 Multiplicação de números reais

Queremos estender a multiplicação $x \cdot y$ de números racionais para o caso de x e y reais. De saída, descartamos as possibilidades triviais em que ao menos um dos fatores é nulo, pois é óbvio que continuamos querendo ter $0 \cdot x = x \cdot 0 = 0$. Assim, vamos nos concentrar nas possibilidades em que ambos os fatores são não nulos, as quais dividiremos em dois casos: x e y positivos, e o caso em que ao menos um dos fatores é negativo.

– Multiplicação de reais positivos

Iniciemos com o seguinte resultado sobre números racionais positivos:

Lema 7.48 -

Sendo x e y dois números racionais positivos, na notação habitual temos:

$$x_n y_n \leqslant xy \leqslant \big(x_n + \frac{1}{10^n}\big)\big(y_n + \frac{1}{10^n}\big), \tag{7.3}$$

de modo que o produto xy sempre está em cada elemento da sequência de intervalos $[x_n y_n \, , \, (x_n + 1/10^n)(y_n + 1/10^n)]$*, a qual é encaixante e evanescente.*

Prova:

Da definição de expansão decimal, sabemos que valem:

$$x_n \leqslant x \leqslant x_n + \frac{1}{10^n}\,, \quad y_n \leqslant y \leqslant y_n + \frac{1}{10^n}\,.$$

Como todos os números acima são racionais, multiplicando essas desigualdades, obtemos[10], na ordem dos números racionais:

$$x_n y_n \leqslant xy \leqslant (x_n + \frac{1}{10^n})(y_n + \frac{1}{10^n})\,, \tag{7.4}$$

de modo que $xy \in [x_n y_n\,,\,(x_n + 1/10^n)(y_n + 1/10^n)]$, $\forall n$. Resta provar que essa sequência é encaixante e evanescente.
O encaixante sai imediatamente pela multiplicação das desigualdades já nossas conhecidas:

$$\begin{gathered} x_n \leqslant x_{n+1} \leqslant x_{n+1} + \frac{1}{10^{n+1}} \leqslant x_n + \frac{1}{10^n} \\ y_n \leqslant y_{n+1} \leqslant y_{n+1} + \frac{1}{10^{n+1}} \leqslant y_n + \frac{1}{10^n}\,. \end{gathered}$$

Por sua vez, a evanescência sai de:

$$(x_n + \frac{1}{10^n})(y_n + \frac{1}{10^n}) - x_n y_n = (x_n + y_n)\frac{1}{10^n} + \frac{1}{10^{2n}} \leqslant (m + M + 2)\frac{1}{10^n} + \frac{1}{10^{2n}} =$$

$$= (m + M + 2 + \frac{1}{10^n})\frac{1}{10^n} \leqslant (m + M + 3)\frac{1}{10^n}\,.$$

CQD.

Consequentemente, como estamos procurando estender a multiplicação de números racionais para números reais, o Lema 7.48 nos mostra que fica natural *definirmos* o produto $x \cdot y$, no caso de x e y reais positivos, como sendo o único número real comum à sequência de intervalos encaixante e evanescente que encontramos nesse lema. (Não deixe o leitor de observar que o fato de essa sequência ser encaixante e evanescente independe de x e y serem racionais ou irracionais.)

Definição 7.49 (*multiplicação de reais positivos*) -

Dados x e y números reais positivos, com expansões decimais

$$\begin{aligned} x &= m, a_1 a_2 \ldots \\ y &= M, b_1 b_2 \ldots\ , \end{aligned}$$

[10] Lembre que, para a, b, c, d racionais positivos, $a \leqslant b$ e $c \leqslant d$ implicam $ac \leqslant bd$.

sejam, para cada $n \geqslant 1$*, os números racionais*

$$x_n = m, a_1 a_2 \ldots a_n \quad e \quad y_n = M, b_1 b_2 \ldots b_n\,.$$

Assim, a multiplicação *dos números reais positivos* x *e* y *produz um resultado chamado* produto*, o qual é denotado por* $x \cdot y$*, ou meramente* xy*, e é definido como sendo o único número real comum a todos os elementos da sequência de intervalos encaixante e evanescente:*

$$\left[x_n y_n, (x_n + \frac{1}{10^n})(y_n + \frac{1}{10^n}) \right].$$

Exemplo 7.50 -

Como um exemplo inicial, verifiquemos que multiplicando 3 *por* 2/3*, como números reais, obtemos o esperado produto* 2*. Com efeito:*

$x_1 y_1 = 3,0 \times 0,6 = 1,8$ *e* $3,1 \times 0,7 = 2,17 \ \rightarrow$ $[1,8\,;\,2,17]$
$x_2 y_2 = 3,00 \times 0,66 = 1,98$ *e* $3,01 \times 0,67 = 2,0167 \ \rightarrow$ $[1,98\,;\,2,0167]$
$x_3 y_3 = 3,000 \times 0,666 = 1,998$ *e* $3,001 \times 0,667 = 2,00167 \ \rightarrow$ $[1,998\,;\,2,00167]$
$x_4 y_4 = 3,0000 \times 0,6666 = 1,9998$ *e* $3,0001 \times 0,6667 = 2,000167 \rightarrow [1,9998; 2,000167]$.
Agora, fica fácil o leitor concluir (Exercício!).

Exemplo 7.51 -

Como um segundo exemplo, verifiquemos que o quadrado de 1/3*, interpretado como um produto de números reais, é o esperado* 1/9 *. Com efeito:*

$x_1^2 = 0,3^2 = 0,09$ *e* $0,4^2 = 0,16 \ \rightarrow$ $[0,09\,;\,0,16]$
$x_2^2 = 0,33^2 = 0,1089$ *e* $0,34^2 = 0,1156 \ \rightarrow$ $[0,1089\,;\,0,1156]$
$x_3^2 = 0,333^2 = 0,11089$ *e* $0,334^2 = 0,11156 \ \rightarrow$ $[0,11089\,;\,0,11156]$
$x_4^2 = 0,3333^2 = 0,111089$ *e* $0,3334^2 = 0,111156 \ \rightarrow$ $[0,111089\,;\,0,111156]$
e continua num padrão muito regular, o que nos permite afirmar que (Exercício!):

$$(\frac{1}{3})^2 = 0,111\ldots = \frac{1}{9}\,.$$

Exemplo 7.52 -

Sempre usando a Definição 7.49, tratemos de determinar o produto do número racional $1,\overline{414}$ *pelo irracional* $3,010010001\ldots$ *, com erro de, no máximo, uma unidade da terceira casa decimal.*

Aplicando a definição:
$n = 1 \to 1,4 \times 3,0 = 4,2$ *e* $1,5 \times 3,1 = 4,65 \ \to$ $[4,2\,;\ 4,65]$
$n = 2 \to 1,41 \times 3,01 = 4,2441$ *e* $1,42 \times 3,02 = 4,2884 \ \to$ $[4,2441\,;\ 4,2884]$
$n = 3 \to 1,414 \times 3,010 = 4,25614$ *e* $1,415 \times 3,011 = 4,26057 \ \to$ $[4,25614\,;\ 4,26057]$
$n = 4 \to 1,4141 \times 3,0100 = 4,25644\ldots$ *e* $1,4142 \times 3,0101 = 4,25688\ldots \ \to$
$[4,25644\ldots\,;\ 4,25688\ldots]$.
Consequentemente, o produto desejado é $xy = 4,256\ldots$, *com um erro certamente menor do que* $0,001$.

Exercício 183 -

Admitindo conhecida a Regra da Multiplicação de Racional r *por Potências de* 10, *estenda-a para o caso de multiplicação por* r *número real positivo de expansão decimal* $r = a_m \ldots a_1 a_0,\, b_1 b_2 b_3 \ldots$ *:*

$$\begin{aligned} 10 \times r &= a_m \ldots a_1 a_0 b_1\,,\, b_2 b_3 b_4 \ldots \\ 10^2 \times r &= a_m \ldots a_1 a_0 b_1 b_2\,,\, b_3 b_4 b_5 \ldots \\ &\ldots\ldots \\ 10^n \times r &= a_m \ldots a_1 a_0 b_1 b_2 \ldots b_n\,,\, b_{n+1} b_{n+2} b_{n+3} \ldots\,, \quad \forall n \geqslant 1\,. \end{aligned}$$

Exercício 184 -

Ampliando a Definição 7.49 – acrescentando os casos $(x > 0, y = 0)$, $(x = 0, y > 0)$ *e* $(x = y = 0)$ *–, verifique que teremos, para os mesmos:* $x \cdot 0 = 0$, $0 \cdot y = 0$ *e* $0 \cdot 0 = 0$, *respectivamente. Resumindo:* $x \cdot 0 = 0 \cdot x = 0$, *para todos os* $x \geqslant 0$ *reais.*

– Multiplicação por real negativo

Definição 7.53 *(multiplicação por real negativo)* -

Sejam x *e* y *dois números reais, tais que, ao menos um deles é negativo. O produto* $x \cdot y$ *é obtido usando a Definição 7.49 e o Exercício 184, segundo as seguintes possibilidades lógicas:*

– *se* $x \geqslant 0$ *e* $y < 0$, *temos:* $x \cdot y = -(x \cdot |y|)$.
– *se* $x < 0$ *e* $y \geqslant 0$, *temos:* $x \cdot y = -(|x| \cdot y)$.
– *se* $x < 0$ *e* $y < 0$, *temos:* $x \cdot y = |x| \cdot |y|$.

Exercício 185 -

Valendo-se do Exemplo 7.52, calcule $1,\overline{414} \cdot (-3,010010001\ldots)$.

– Compatibilidade da multiplicação com a ordem de reais

O teorema a seguir generaliza, para os números reais, a imprescindível e já abordada compatibilidade da multiplicação com a ordem no campo dos números racionais.

Teorema 7.54 -

A multiplicação de números reais é compatível com a relação de ordem, ou seja, sendo $a, b \in \mathbb{R}$*:*

$$a < b \iff a \cdot c < b \cdot c, \ \forall c \text{ real positivo.}$$

Prova:

Nos casos em que c é inteiro ou racional positivo, esse resultado é geometricamente óbvio. Infelizmente, uma prova que inclua o caso de c irracional positivo envolve um argumento mais técnico do que o usual, e assim preferimos deixá-la para a Leitura Complementar 7.11.

CQD.

Exercício 186 -

Verifique que a hipótese $c > 0$ *do teorema é essencial; isto é, se não soubermos que* $c > 0$*, então não poderemos garantir que* $ac < bc$*.*

– Aplicação: raiz quadrada de um real positivo

Definição 7.55 -

Por raiz quadrada *de um número* r*, entendemos qualquer número*[11] x *tal que* $x^2 = r$*.*

Exemplo 7.56 -

O número real $r = 4$ *admite duas raízes quadradas:* 2 *e* -2*, conforme se verifica imediatamente. Pelo Teorema Fundamental da Álgebra (vide, adiante, capítulo sobre números complexos) segue que ele não tem outras raízes quadradas.*

[11] Propositalmente, não explicitamos o campo numérico onde estão r e x. Normalmente esse campo é $\mathbb{R}$, ou o campo $\mathbb{C}$ dos números complexos, o qual será estudado num capítulo adiante.

Exemplo 7.57 -

O quadrado de zero (como número real) é zero, de modo que zero é uma raiz quadrada de zero. Por outro lado, como todo número real não nulo tem quadrado positivo (Exercício!), segue que o zero tem somente uma raiz quadrada no campo dos números reais.

Semelhantemente, se percebe que nenhum número real negativo pode ter raiz quadrada real (ou seja: no campo dos números reais).

Definição 7.58 -

Por raiz quadrada aritmética (ou principal) *de um número real* r *, entenderemos qualquer real* $x \geqslant 0$*, se existir, tal que* $x^2 = r$*.*
Notação: $\boxed{x = \sqrt{r}}$ *sempre indica a raiz quadrada aritmética de* r*.*

Exemplo 7.59 -

Pelo que vimos acima, zero tem uma única raiz quadrada aritmética: $\sqrt{0} = 0$*. Ademais, nenhum real negativo tem raiz quadrada aritmética; ou seja,* $\sqrt{x}$ *não está definida para* $x < 0$*. Ao contrário, o teorema seguinte diz que* $\sqrt{x}$ *sempre está definida para* $x > 0$*.*

Teorema 7.60 -

Todo número real positivo ou nulo tem uma, e somente uma, raiz quadrada aritmética.

Prova:

A prova formal do caso geral é bastante penosa, assim nos limitaremos a mostrar a ideia envolvida tratando do caso concreto e modelo da $\sqrt{2}$.

– Cálculo de um candidato a $\sqrt{2}$.

denotaremos por δ este candidato e, como ele tem de verificar $\delta^2 = 2$, o determinaremos como o único número real comum a uma sequência de intervalos encaixantes e evanescentes

$$[a_0\,,\, b_0] \supset [a_1\,,\, b_1] \supset \ldots [a_n\,,\, b_n] \supset \ldots\,,$$

a qual será obtida exigindo-se que os a_n e b_n sejam números racionais e que tenhamos $a_n^2 < 2 < b_n^2$.

• Tomamos $a_0 = 1$ e $b_0 = 2$, de modo que $1^2 < 2 < 2^2$.

• Determinaremos a_1 e b_1 procurando enquadrar 2 entre dois valores consecutivos do tipo $(1,d)^2$, com $d = 0, 1, 2, \ldots, 9$:

$$\begin{aligned}
&1,0^2 = 1\\
&1,1^2 = 1,21\\
&1,2^2 = 1,44\\
&1,3^2 = 1,69\\
&1,4^2 = 1,96\\
&1,5^2 = 2,25\,,
\end{aligned}$$

de modo que $a_1 = 1,4$ e $b_1 = 1,5$.

• Determinaremos a_2 e b_2 procurando enquadrar 2 entre dois valores consecutivos do tipo $(1,4d)^2$, com $d = 0, 1, 2, \ldots, 9$:

$$\begin{aligned}
&1,40^2 = 1,96\\
&1,41^2 = 1,9881\\
&1,42^2 = 2,0164\,,
\end{aligned}$$

de modo que $a_2 = 1,41$ e $b_2 = 1,42$.

• Determinaremos a_3 e b_3 procurando enquadrar 2 entre dois valores consecutivos do tipo $(1,41d)^2$, com $d = 0, 1, 2, \ldots, 9$:

$$\begin{aligned}
&1,410^2 = 1,96\\
&1,411^2 = 1,9909\\
&1,412^2 = 1,993\ldots\\
&1,413^2 = 1,996\ldots\\
&1,414^2 = 1,9993\ldots\\
&1,415^2 = 2,002\ldots\ ,
\end{aligned}$$

de modo que $a_3 = 1,414$ e $b_3 = 1,415$.

• Prosseguindo de modo semelhante, ficará bem claro que determinaremos um número real δ que é comum à sequência dos intervalos $[a_n\,, b_n]$ e o qual é tal que sua expansão decimal, até a n-ésima casa decimal, é $\delta = 1, a_1a_2a_3\ldots a_n\ldots$. Por exemplo, até a 40-ésima casa decimal, nosso candidato é:

$$\delta = 1,41421\,35623\,73095\,04880\,16887\,24209\,69807\,856967\ldots\,.$$

– Verifiquemos que $\delta^2 = 2$.

pela definição de multiplicação, o quadrado δ^2 é o ponto comum da sequência encaixante e evanescente dos intervalos $[x_n^2\,,\,(x_n+1/10^n)^2]$, onde x_n é a expansão decimal de δ truncada na n-ésima casa decimal. Ora, pela contrução feita na etapa inicial, temos que $x_n = 1, a_1a_2a_3\ldots a_n$ e que, por isso, $x_n^2 < 2 < (x_n+1/10^n)^2$. Assim, podemos afirmar que, realmente, $\delta^2 = 2$. Ou seja: $\delta = \sqrt{2}$.

– Unicidade da raiz quadrada aritmética.

temos de mostrar que não existem $x \neq y$ reais *positivos*, tais que $x^2 = y^2 = 2$. Com efeito, se existissem, teríamos, sem perda de generalidade, que $0 < x < y$. Então, das propriedades da ordem de números reais *positivos*, seguiria: $2 = x^2 = x \cdot x < x \cdot y < y \cdot y = y^2 = 2$, um absurdo.

CQD.

Corolário 7.61 -

i). Todo número real $r > 0$ tem exatamente duas raízes quadradas, e elas sempre podem ser escritas em termos de sua raiz quadrada aritmética: $+\sqrt{r}$ e $-\sqrt{r}$.

ii). O zero tem somente uma raiz quadrada: $\sqrt{0} = 0$.

iii). Nenhum número real $r < 0$ tem raiz quadrada em $\mathbb{R}$.

Exemplo 7.62 *(importante)* -

O quadrado r^2 de um número real r tem uma, e somente uma, raiz quadrada aritmética:

$$\sqrt{r^2} = |r|\,.$$

Por outro lado, $|r|$ e $-|r|$ são suas raízes quadradas.
(Obviamente, elas também podem ser escritas como r e $-r$, e sempre são duas, a menos que $r = 0$.)

Exemplo 7.63 -

Já encontramos a versão geométrica *do Teorema de Pythagoras, a qual diz que – num triângulo retângulo de lados a e b, e hipotenusa c – a área do quadrado de lado c é a soma das áreas dos quadrados de lado a e lado b. Agora, com a definição de multiplicação de reais, podemos escrever esse teorema como:*

$$c^2 = a^2 + b^2\,.$$

Usando raiz quadrada, também podemos escrever:

$$c = \sqrt{a^2 + b^2}\,.$$

Em particular, resulta disso que a diagonal d de um quadrado unitário vale:

$$d = \sqrt{1^2 + 1^2} = \sqrt{2}\,.$$

Mais geralmente, a diagonal de um quadrado de lado ℓ vale:

$$d = \sqrt{\ell^2 + \ell^2} = \sqrt{2 \cdot \ell^2} = \ell\sqrt{2}\,.$$

Fica para o exercício seguinte a prova da última igualdade.

Exercício 187 -

Usando que a raiz quadrada de todo número real positivo é única, mostre que, para todo número real $a > 0$:

$$\sqrt{2a^2} = a\sqrt{2}\,.$$

Mais geralmente, mostre que, para todos os reais $a, b > 0$, vale:

$$\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}\,.$$

Exercício 188 -

De modo semelhante ao que foi feito com $\sqrt{2}$, mostre que $\sqrt{3}$ está definida no campo dos números reais.

Exercício 189 -

Generalizando as construções e argumentos usados no estudo de $\sqrt{2}$ e $\sqrt{3}$, prove o caso geral do teorema anterior.
Sugestão:
sendo r um número real positivo, na sequência de quadrados inteiros consecutivos:

$$0^2 < 1^2 < 2^2 < 3^2 < \dots\,,$$

temos $m^2 \leqslant r < (m+1)^2$, para exatamente um m inteiro, o que já diz que, se $\sqrt{r}$ existir, ela é obrigatoriamente da forma $\sqrt{r} = m, \dots$. Para determinar o primeiro dígito da parte fracionária, enquadramos r entre dois valores sucessivos dos quadrados:

$$m^2 < (m + \frac{1}{10})^2 < (m + \frac{2}{10})^2 < \dots < (m + \frac{9}{10})^2 < (m+1)^2\,,$$

de modo que, para exatamente um $d_1 \in \{0,1,2,\dots,9\}$*, tenhamos*

$$\left(m+\frac{d_1}{10}\right)^2 \leqslant r < \left(m+\frac{1+d_1}{10}\right)^2,$$

o que já diz que, se $\sqrt{r}$ *existir, ela é obrigatoriamente da forma:*

$$\sqrt{r} = m, d_1 \dots ;$$

e assim por diante.

Fique o leitor alertado de que, na prática, poucas pessoas e poucos livros usam a denominação "raiz quadrada aritmética"; em particular, não a diferenciam de "raiz quadrada". Essa falta de cuidado, frequentemente, resulta em erros e confusões. Assim, vale a pena ressaltar alguns pontos:

- As raízes quadradas de 4 são $+\sqrt{4} = 2$ e $-\sqrt{4} = -2$.
  Podemos resumir isso escrevendo (cuidado!) que as raízes quadradas de 4 são $\pm\sqrt{4} = \pm 2$.
- É errado escrever $\sqrt{4} = \pm 2$!
- É correto escrever $\sqrt{4} = 2$.
- Para qualquer x número real, temos: $\sqrt{x^2} = |x|$.

7.8 O corpo ordenado dos números reais

Uma vez definidas as operações aritméticas e a relação de ordem sobre os números reais, precisamos estudar suas propriedades, inclusive sua compatibilidade. Esse estudo é o objetivo desta seção.

O fato de termos definido uma adição, uma multiplicação e uma ordem sobre os números reais, como extensão das correspondentes sobre os números racionais, faz com que o campo $[\mathbb{R}, +, \cdot, <]$ tenha tudo para "herdar" as propriedades de $[\mathbb{Q}, +, \cdot, <]$. Com efeito, conforme veremos a seguir, ambos têm a estrutura de corpo ordenado. Mas nem tudo fica igual, há uma grande diferença estrutural entre eles: o campos dos reais tem a Propriedade do Contínuo, o campo dos racionais não!

– Estrutura de corpo de $[\mathbb{R}, +, \cdot]$

Teorema 7.64 -

O campo dos números reais, $[\mathbb{R}, +, \cdot]$, tem o seguinte conjunto de propriedades básicas que lhe dão uma estrutura de corpo. *Para todos os a, b, $c \in \mathbb{R}$:*

i). as operações + (adição) e · (multiplicação) são fechadas em todo o $\mathbb{R}$:
$a + b \in \mathbb{R}$ [*a operação + é fechada*]
$a \cdot b \in \mathbb{R}$ [*a operação · é fechada*]

ii). associatividade das operações:
$a + (b + c) = (a + b) + c$ [*associatividade da +*]
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ [*associatividade da ·*]

iii). existência de elemento neutro:
$a + 0 = a$ [*0 é elemento neutro da +*]
$a \cdot 1 = a$ [*1 é elemento neutro da ·*]

iv). existência de inverso:
$\exists a' \in \mathbb{R}$ *tal que* $a + a' = 0$. *Com efeito:* $a' = -a$. [*$-a$ é o simétrico de a*]
sendo $a \neq 0$, $\exists a^{-1} \in \mathbb{R}$ *tal que* $a \cdot a^{-1} = 1$. [*a^{-1} é o recíproco de a*]

v). comutatividade das operações:
$a + b = a + b$ [*comutatividade da +*]
$a \cdot b = b \cdot a$ [*comutatividade da ·*]

vi). distributividade da multiplicação:
$a \cdot (b + c) = a \cdot b + a \cdot c$ [*distributividade da ·*]

Observação 7.65 -

Pela existência do simétrico, podemos definir a subtração *de dois reais quaisquer, x e y, por meio de*

$$x - y = x + (-y)\,.$$

Pela existência do recíproco, podemos definir o quociente *de um real qualquer, x, por um real não nulo $y \neq 0$, por meio de*

$$\frac{x}{y} = x \cdot y^{-1}\,.$$

Devido a isso, podemos escrever $x^{-1} = 1/x$.

Uma prova direta do Teorema 7.64 seria muito longa; na Leitura Complementar 7.11, daremos uma prova alternativa, mas mais curta. Por enquanto, nos limitaremos a provar a existência do recíproco de cada real positivo:

Proposição 7.66 -

Cada número real $x > 0$ tem um recíproco y, ou seja: $xy = 1$.

Prova:

Como x é positivo, sua expansão decimal nos dá um menor valor n_0, para n com o qual vale $x_n > 0$, de modo que

$$0 \notin \left[x_n, x_n + \frac{1}{10^n}\right], \quad \forall n \geqslant n_0\,.$$

Essa propriedade nos dá direito de formar a seguinte sequência de intervalos:

$$\left[\left(x_n + \frac{1}{10^n}\right)^{-1}, x_n^{-1}\right], \quad \forall n \geqslant n_0\,, \tag{7.5}$$

a qual afirmamos que é encaixante e evanescente.

– A sequência (7.5) é encaixante.

Da expansão decimal de x, temos que:

$$x_n \leqslant x_{n+1} < x_{n+1} + \frac{1}{10^{n+1}} \leqslant x_n + \frac{1}{10^n}\,, \quad \text{desde que } n_0 \leqslant n\,.$$

Ora, essas desigualdades envolvem apenas números racionais e, pelo que já sabemos de sua ordenação, é imediato se ver que no caso de racionais positivos:

$$0 < a < b < c < d \Rightarrow \frac{1}{d} < \frac{1}{c} < \frac{1}{b} < \frac{1}{a},$$

de modo que

$$\Big(x_n + \frac{1}{10^n}\Big)^{-1} \leqslant \Big(x_{n+1} + \frac{1}{10^{n+1}}\Big)^{-1} < x_{n+1}^{-1} < x_n^{-1}, \quad \text{desde que } n_0 \leqslant n\,.$$

Isso prova que (7.5) realmente é encaixante.

– A sequência (7.5) também é evanescente.

De fato, o comprimento de cada intervalo dessa sequência é dado por

$$\begin{aligned} x_n^{-1} - \Big(x_n + \frac{1}{10^n}\Big)^{-1} &= \frac{1}{x_n} - \frac{10^n}{10^n x_n + 1} = \frac{10^n x_n + 1 - 10^n x_n}{x_n(10^n x_n + 1)} \\ &= \frac{1}{x_n(10^n x_n + 1)} \leqslant \frac{1}{x_{n_0}(10^n x_{n_0} + 1)} \to 0\,. \end{aligned}$$

Como a sequência (7.5) é encaixante e evanescente, a Propriedade do Contínuo nos garante que existe exatamente um número real, que denotaremos por y, pertencente a todos seus intervalos, isso é:

$$\Big(x_n + \frac{1}{10^n}\Big)^{-1} \leq y \leq x_n^{-1}, \quad \forall n \geqslant n_0\,. \tag{7.6}$$

Nosso objetivo passa a ser mostrar que y é o recíproco de x. Para atingí-lo, a ideia é construir uma nova sequência de intervalos encaixantes e evanescentes, tal que tanto xy como 1 estão em todos seus intervalos. A unicidade do ponto de evanescência nos dará, então, que $xy = 1$.

Ora, como $0 < x_n \leqslant x < x_n + \frac{1}{10^n}$, de (7.6) e da compatibilidade da multiplicação com a ordem de números reais (vide Teorema 7.54) segue que:

$$x_n\Big(x_n + \frac{1}{10^n}\Big)^{-1} \leqslant xy < x_n^{-1}\Big(x_n + \frac{1}{10^n}\Big), \quad \forall n \geqslant n_0\,,$$

ou seja:

$$xy \in \Big[x_n\Big(x_n + \frac{1}{10^n}\Big)^{-1}, x_n^{-1}\Big(x_n + \frac{1}{10^n}\Big)\Big], \quad \forall n \geqslant n_0\,.$$

Mas, também vale:

$$1 \in \Big[x_n\Big(x_n + \frac{1}{10^n}\Big)^{-1}, x_n^{-1}\Big(x_n + \frac{1}{10^n}\Big)\Big], \quad \forall n \geqslant n_0\,.$$

Com efeito, todos esses intervalos têm a forma $[\frac{a}{b}\,,\,\frac{b}{a}]$, onde $a = x_n$ e $b = x_n + 1/10^n$ são números racionais positivos, com $0 < a < b$, de modo que $\frac{a}{b} < 1 < \frac{b}{a}$.

Após demonstrado que

$$xy,\, 1 \in \Big[x_n\Big(x_n + \frac{1}{10^n}\Big)^{-1},\, x_n^{-1}\Big(x_n + \frac{1}{10^n}\Big)\Big], \quad \forall n \geqslant n_0\,,$$

para podermos concluir que $xy = 1$, basta mostrarmos que tais intervalos são evanescentes.

Ora, na notação acima, temos:

$$\begin{aligned} x_n^{-1}\Big(x_n + \frac{1}{10^n}\Big) - x_n\Big(x_n + \frac{1}{10^n}\Big)^{-1} &= \frac{b}{a} - \frac{a}{b} = \frac{b^2 - a^2}{ab} \\ &= \frac{(b-a)(b+a)}{ab} = \big(\frac{1}{a} + \frac{1}{b}\big)(b-a) \\ &\leqslant \big(\frac{1}{x_{n_0}} + \frac{1}{x_{n_0} + 1/10^{n_0}}\big)\cdot\frac{1}{10^n} \quad \to \quad 0\,. \end{aligned}$$

CQD.

Dado $x > 0$, real, encontrado n_0, tal que $0 \notin [x_n, x_n + \frac{1}{10^n}]$, $\forall n \geqslant n_0$, vimos que $1/x$ é o ponto de evanescência da sequência

$$\Big[\Big(x_n + \frac{1}{10^n}\Big)^{-1},\, x_n^{-1}\Big], \quad \forall n \geqslant n_0.$$

Como as extremidades dessa sequência são números racionais, temos que o conhecimento da expansão decimal de x é suficiente para calcular esses intervalos, e assim determinar aproximações para $1/x$. Vejamos um exemplo:

Exemplo 7.67 -

Sabendo que $\sqrt{2} = 1{,}4142\,1356\,2373\,09504\ \ldots$, *pede-se calcular uma aproximação de* $1/\sqrt{2}$, *com erro na quarta casa decimal.*

Temos sucessivamente:

$$\begin{array}{rcl}
\big[x_n; x_n + \frac{1}{10^n}\big] & \to & \Big[\Big(x_n + \frac{1}{10^n}\Big)^{-1}; x_n^{-1}\Big] \\[2ex]
[1,4\,;\,1,5] & \to & [0,6666\ldots\,;\,0,7142\ldots] \\
[1,41\,;\,1,42] & \to & [0,7042\ldots\,;\,0,7092\ldots] \\
[1,414\,;\,1,415] & \to & [0,7067\ldots\,;\,0,7072\ldots] \\
[1,4142\,;\,1,4143] & \to & [0,70706\ldots\,;\,0,70711\ldots] \\
[1,41421\,;\,1,41422] & \to & [0,707103\ldots\,;\,0,707108\ldots]
\end{array}$$

de modo que $1/\sqrt{2} \simeq 0,7071$.

Levando o processo acima mais adiante, ou usando que $1/\sqrt{2} = \sqrt{2}/2$, *podemos obter uma aproximação mais exata:*

$$\frac{1}{\sqrt{2}} \simeq 0,7071\,0678\,1186\,5475\ \ldots\,.$$

De um modo totalmente semelhante ao que já ocorreu com o corpo dos números racionais, das propriedades do corpo dos reais saem uma grande quantidade de consequências, algumas das quais estão listadas a seguir.

Corolário 7.68 -

Sendo a, b, c *números reais:*

i). $0a = 0$

ii). $(-a)b = -(ab)$

iii). $(-a)(-b) = ab$

iv). $a + b = a\ \forall a \Rightarrow b = 0$ — [*unicidade do zero*]

v). $ab = a\ \forall a \Rightarrow b = 1$ — [*unicidade da unidade*]

vi). $a + b = 0 \Rightarrow b = -a$ — [*unicidade do simétrico*]

vii). $ab = 1 \Rightarrow b = a^{-1}$ — [*unicidade do recíproco*]

viii). $a + c = b + c \Rightarrow a = b$ — [*lei do cancelamento da* $+$]

ix). $c \neq 0, ac = bc \Rightarrow a = b$ — [*lei do cancelamento da* $\cdot$]

x). $a \neq 0\,,\ b \neq 0 \Rightarrow ab \neq 0$ — [*integridade da* $\cdot$]

Prova:

Fica como um exercício para o leitor. CQD.

– Estrutura de corpo ordenado de $[\mathbb{R}, +, \cdot, <]$

O teorema seguinte resume, sob um ponto de vista mais teórico, os resultados dos Teoremas 7.47 e 7.54.

Teorema 7.69 -

O campo $[\mathbb{R}, +, \cdot, <]$ tem a estrutura de corpo ordenado*, ou seja, é um corpo no qual existe uma relação de ordem, $<$, que verifica as duas seguintes propriedades. Sendo $a, b, c \in \mathbb{R}$:*

i). $a < b \iff a + c < b + c$, $\forall c \in \mathbb{R}$ [*compatibilidade da ordem com a adição*];
ii). $a < b \iff ac < bc$, $\forall c > 0$ [*compatibilidade da ordem com a multiplicação*].

Corolário 7.70 -

Sendo $a, b, c \in \mathbb{R}$:

i). a relação de ordem é preservada na adição:
$a < b \iff a + c < b + c,\ \forall c \in \mathbb{R}$,
$a \leqslant b \iff a + c \leqslant b + c,\ \forall c \in \mathbb{R}$;
ii). a relação de ordem é preservada na multiplicação por reais positivos:
$a < b \iff ac < bc,\ \forall c > 0$,
$a \leqslant b \iff ac \leqslant bc,\ \forall c > 0$;
iii). a relação de ordem é invertida *na multiplicação por reais negativos:*
$a < b \iff ac > bc,\ \forall c < 0$,
$a \leqslant b \iff ac \geqslant bc,\ \forall c < 0$.

Exercício 190 -

Mostre que as propriedades do teorema anterior nos permitem afirmar que, sendo $a, b, a', b' \in \mathbb{R}$:

i). $a < b$ e $a' < b' \Rightarrow a + a' < b + b'$;
ii). $0 < a < b$ e $0 < a' < b' \Rightarrow aa' < bb'$.

Exercício 191 -

Sendo a, b números reais, mostre que:
i). $0 < a < b \Rightarrow 1/b < 1/a$; *ii).* $a < b \nRightarrow 1/b < 1/a$.

– Densidade no campo dos números reais

Parafraseando o que já foi feito no campo dos números racionais, teremos as seguintes definições:

Definição 7.71 -

Chamamos de intermediário *de dois números reais $x < y$ a qualquer número real z verificando $x < z < y$.*

Definição 7.72 -

Dizemos que um conjunto A de números reais é denso em *$\mathbb{R}$ se, e só se, entre cada par de elementos (distintos) de números reais, exista ao menos um intermediário que esteja em A.*

No capítulo onde estudamos os números racionais foi introduzida a noção de conjunto "denso em $\mathbb{Q}$". Neste sentido, usando média aritmética, vimos que $\mathbb{Q}$ é denso no próprio $\mathbb{Q}$. O teorema a seguir mostra que, embora agora não baste usar o recurso da média aritmética, $\mathbb{Q}$ é denso em $\mathbb{R}$.

Teorema 7.73 -

Entre cada par de números reais existe ao menos um intermediário que é número racional. Ou seja: $\mathbb{Q}$ é denso em $\mathbb{R}$.

Prova:

Dados reais $x < y$, escrevamos suas expansões decimais não 9-terminantes do seguinte modo:

$$x = a_0, a_1 a_2 a_3 \dots \ < \ y = b_0, b_1 b_2 b_3 \dots .$$

Pela definição de ordem, segue que existe $n \geqslant 0$, tal que $a_0 = b_0$, $a_1 = b_1$, $\dots$, $a_{n-1} = b_{n-1}$ e $a_n < b_n$. Ademais, como estamos trabalhando com expansões não 9-terminantes, existe um menor índice $k > n$, tal que $a_k \neq 9$.

Isso posto, construímos o número racional dado por

$$z = c_0\,, c_1 c_2 c_3 \dots c_n \dots c_k = a_0\,, a_1 a_2 a_3 \dots a_n \dots a_{k-1} c_k\,,$$

onde $c_k = 1 + a_k \leqslant 9$. Afirmamos que $x < z < y$. Com efeito:

- $x < z$, pois as expansões decimais de x e z coincidem até a (k-1)-casa e, na casa seguinte, vale $a_k < c_k$;
- $z < y$, pois as expansões decimais de z e y coincidem até a (n-1)-casa decimal e, na casa seguinte, vale $c_n = a_n < b_n$. CQD.

Teorema 7.74 -

Entre cada par de números reais existe ao menos um intermediário que é número irracional. Ou seja: o conjunto $\mathbb{I}$ dos números irracionais é denso em $\mathbb{R}$.

Prova:

Usando a notação da prova do teorema anterior, construímos o número real

$$z' = c_0\,, c_1c_2c_3 \ldots c_k01001000100001\ldots\,.$$

Afirmamos que z' é irracional (imediato!) e que ele é intermediário entre x e y. Com efeito:

- $x < z'$, uma vez que, obviamente, $z < z'$;
- $z' < y$, uma vez que $c_i = a_i = b_i$, para $i = 0, 1, \ldots, n-1$, e $c_n = a_n < b_n$.

CQD.

Exercício 192 -

Mostre que entre dois números reais distintos existem infinitos intermediários racionais, e infinitos intermediários irracionais.

– Propriedade arquimediana de $[\mathbb{R}, +, \cdot, <]$

Teorema 7.75 -

O campo dos números reais possui a propriedade arquimediana: *dado um número real $\delta > 0$, para cada escolha de $x \in \mathbb{R}$, sempre será possível encontrar $n \in \mathbb{Z}$, tal que $x < n\delta$.*

(O leitor deve ver δ como sendo um módulo, ou valor de referência, com o qual procuramos fazer uma estimativa da magnitude de x).

Prova:

O resultado é obviamente verdadeiro para os casos $x \leqslant 0$; resta tratar dos casos $x > 0$, cuja expansão decimal é $x = m, a_1a_2a_3\ldots$, de modo que $x \leqslant m+1 =$ inteiro. Temos de considerar dois casos, de acordo com a racionalidade de δ:

- $\delta =$ número racional positivo.
  Neste caso, como o campo dos racionais é arquimediano, escolhendo $n \in \mathbb{Z}$ tal que $m+1 < n\delta$, podemos afirmar que $x < n\delta$.
- $\delta =$ número irracional positivo.
  Abortando convenientemente a expansão decimal de δ, é fácil percebermos que conseguimos um r racional, tal que $0 < r < \delta$. Pelo raciocínio do caso anterior, encontramos $n \in \mathbb{Z}$, tal que $m+1 < nr < n\delta$; de modo que $x < n\delta$.

CQD.

Exemplo 7.76 -

Observe que a verificação da propriedade $x < n\delta$ é imediata nos casos em que o módulo $\delta \geqslant x$. Com efeito, $n = 1$ já serve nos casos $x < \delta$, e no caso $x = \delta$, o menor n que serve é $n = 2$.

Exemplo 7.77 -

Outra situação trivial ocorre quando $x < 0$, caso em que qualquer $n \geqslant 0$ serve. Contudo, é possível tomarmos n negativo. Por exemplo, sendo o módulo de comparação $\delta = 1/10$, para $x = -\sqrt{2} = -1,414\ldots$ podemos tomar $n = -14$, o que equivale a dizer:

$$-\sqrt{2} < (-14)\,\delta = (-14) \times \frac{1}{10}\,.$$

Exemplo 7.78 -

Na prática usual, determinaremos n da maneira usada na demonstração do teorema anterior, ou seja: escolhemos n procurando fazer com que $n\delta$ fique maior do que $m+1 \geqslant m, a_1a_2a_3\ldots$.
Por exemplo,

$$\delta = \frac{1}{10} < x = \sqrt{2}\,,$$

mas, como $\sqrt{2} < 2$*, encontramos* $n\delta > x$ *buscando* n *tal que* $n\delta \geqslant 2$*. É imediato percebermos que o menor* n *que serve é* $n = 20$*, de modo que temos:* $\sqrt{2} < 20\delta$*.*

Exercício 193 -

Já mostramos diretamente que os racionais são densos nos reais. O objetivo deste exercício é mostrar que, em verdade, esta propriedade é uma consequência do fato que o campo dos números reais é arquimediano. Para tal, sendo dados dois números reais, $a < b$ *:*

i). denotando por d *o número real positivo* $d = b - a$*, mostre que existe um inteiro positivo* n *, tal que* $1/d < n$ *;*

ii). mostre que o conjunto dos inteiros positivos m *, tais que* $m/n \leqslant a$ *, tem um maior elemento* m_0 *, o qual verifica:*

$$\frac{m_0}{n} \leqslant a < \frac{m_0}{n} + \frac{1}{n} < b\,.$$

Ou seja, encontramos um número racional entre a *e* b*.*

Exercício 194 -

Mostre que o fato de os irracionais formarem um conjunto denso nos reais é uma consequência da propriedade arquimediana de $\mathbb{R}$ *.*
Sugestão:
dados dois números reais, $a < b$*, aplique o resultado do exercício anterior aos reais* $a' = a/\sqrt{2}$ *e* $b' = b/\sqrt{2}$ *.*

– Propriedade do Contínuo de $[\,\mathbb{R}, +\,, \cdot\,, <\,]$

O leitor, neste capítulo, já passou por uma seção dedicada a mostrar que o campo dos números reais tem a Propriedade do Contínuo. No item que se segue, faremos um resumo e acrescentaremos algumas observações de cunho mais teórico.

7.9 Leitura complementar: o Problema de Hankel

Por cerca de 1870, Hermann Hankel formulou a seguinte questão fundamental:

> *existem outros campos numéricos que têm essencialmente as mesmas propriedades que o campo dos números reais?*

Procuraremos responder, limitando-nos aos campos numéricos mais conhecidos e mais usados:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

todos os quais já estudamos com algum detalhe, exceto o campo dos números complexos, $\mathbb{C}$, que será tratado num capítulo logo adiante.

- Estrutura algébrica.

  Entre os campos acima, apenas $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm estrutura de corpo; $\mathbb{Z}$ é um mero anel, e $\mathbb{N}$ não tem estrutura algébrica interessante.

- Estrutura de corpo ordenado.
  Um corpo ordenado pode ser dividido em três partes disjuntas: o conjunto dos números positivos, o conjunto dos negativos e o conjunto formado pelo número zero; ademais, decorre da compatibilidade da multiplicação e a ordem que o conjunto dos positivos inclui o conjunto de todos os quadrados de números não nulos. Isso implica que é impossível colocarmos uma ordem em $\mathbb{C}$ de modo a transformá-lo num corpo ordenado. Com efeito, a unidade imaginária i se caracteriza por ter quadrado negativo: $i^2 = -1$. (No capítulo sobre números complexos, daremos uma prova detalhada dessa impossibilidade).

  Consequentemente, $\mathbb{Q}$ e $\mathbb{R}$ são corpos ordenados, mas $\mathbb{C}$ não!

- Estrutura de corpo arquimediano.
  Pelo item anterior, $\mathbb{C}$ está longe de ser arquimediano, uma vez que nem pode ser ordenado. Contudo, cabe perguntar: seria possível existir um campo numérico, obrigatoriamente não clássico, com a propriedade arquimediana e "maior" do que $\mathbb{R}$? Por cerca de 1900, o grande matemático David Hilbert mostrou que essa pergunta tem resposta negativa:

  $\mathbb{R}$ é um corpo arquimediano saturado (ou maximal): todo corpo arquimediano pode ser imerso em $\mathbb{R}$; ou seja: a menos de notação, todo corpo arquimediano é um subconjunto de $\mathbb{R}$.

- Propriedade do Contínuo.
  Hilbert também mostrou que

  o campo dos números reais é o único corpo ordenado que tem a Propriedade do Contínuo.

7.10 Leitura complementar: séries de números reais

Esta Leitura tem como objetivo maior interpretar como uma "soma limite" as expansões decimais de números reais:

$$x = m\,, a_1a_2a_3... = m + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots .$$

A maneira tradicional de se fazer isto consiste em apelar para o conceito de *série convergente*. O mesmo é desenvolvido extensamente em cursos de Cálculo Infinitesimal e Análise Matemática, sendo que aqui nos limitaremos ao essencial para atingir o objetivo acima.

No contexto dos números reais, dizemos que o erro de uma aproximação a de um valor exato α é a diferença entre α e a. Como esta diferença pode ser entendida como $\alpha - a$, ou $a - \alpha$, introduziremos a mais precisa denominação erro absoluto de a, como aproximação de α, como sendo $|a - \alpha|$.

Toda sequência de números reais, $a_1, a_2, a_3, \ldots$, pode ser vista como uma sequência de aproximações de qualquer número real α. Contudo, o grande interesse está nas sequências de aproximações cujos erros absolutos, relativamente a um certo α, tornam-se arbitrariamente pequenos:

$$|a_n - \alpha| \quad \text{arbitrariamente pequeno, à medida que } \; n \to +\infty\,.$$

Coloquemos isso numa definição mais cuidadosa:

Definição 7.79 -

Dizemos que uma sequência, $a_1, a_2, \ldots$, de números reais converge *a um número real α – ou* tem por limite *um número real α – se seus termos a_n ficam tão próximos de α quanto quizermos, e assim permanecerem, a partir de um n suficientemente grande.*

Equivalentemente, uma sequência, $a_1, a_2, \ldots$, de números reais converge *a um número real α – ou* tem por limite *um número real α – se o erro absoluto de a_n , como aproximação de α , fica tão próximo de zero quanto quizermos, e assim permanecer, a partir de um n suficientemente grande.*

Ou ainda, de modo mais preciso, dizemos que uma sequência $a_1, a_2, \ldots$ converge a α se, para cada cota de erro $\epsilon =$ número real > 0, pudermos encontrar um n_0 suficientemente grande de modo que, para $\forall n \geqslant n_0$, o erro absoluto de a_n fique menor do que a cota:

$$|a_n - \alpha| < \epsilon\,, \quad \forall n \geqslant n_0\,.$$

Exemplo 7.80 -

A sequência $1, 1/2, 1/3, 1/4, \ldots$ *converge a* $\alpha = 0$.
Com efeito, para qualquer cota $\epsilon > 0$ *, acha-se um* n_0 *inteiro tal que* $1/n_0 < \epsilon$ *(isto é intuitivamente óbvio, e prova-se formalmente, de modo imediato, apelando-se para a Propriedade Arquimediana do campo dos reais). Daí, para todo* $n \geqslant n_0$*:*

$$|a_n - \alpha| = \left|\frac{1}{n} - 0\right| = \frac{1}{n} \leqslant \frac{1}{n_0} < \epsilon.$$

Exemplo 7.81 -

A sequência $1, 0, 1, 0, 1, 0, \ldots$ *não converge a nenhum real* α.
Com efeito, seus termos ficam pulando alternadamente de 1 *para* 0 *e de* 0 *para* 1*, o que torna impossível que eles se aproximem, e* permaneçam, *arbitrariamente perto de algum número real. (Por exemplo, use a cota* $\epsilon = 0,5$.*)*

Exemplo 7.82 -

A sequência $1,\ 1/2,\ 1,\ 1/3,\ 1,\ 1/4,\ \ldots$ *não converge a* $\alpha = 0$, *embora possamos achar termos dela (mais precisamente, os termos da forma* $1/n$*) que chegam tão próximos quanto quisermos de* $\alpha = 0$. *O problema é que os demais termos não permanecem próximos de* $\alpha = 0$.
Mais um pouco de pensar nos mostra que ela não converge a nenhum α. *(Exercício!)*

Exemplo 7.83 -

A sequência $1/10\,,\ 1/10^2\,,\ 1/10^3$ *, etc., ou seja, a sequência*[12] $0,1\,;\ 0,01\,;\ 0,001\,;$ *etc. converge a zero.*
Olhando as expansões decimais dessa sequência, é imediato que, para cada cota de erro $\epsilon > 0$ *que estipularmos, determina-se um inteiro* n_0 *tal que*

$$\frac{1}{10^{n_0}} < \epsilon$$

(por exemplo: se $\epsilon = 0,03467$ *então* $n_0 = 2$ *serve). Daí, com maior razão:*

$$\frac{1}{10^{n_0}}\,,\ \frac{1}{10^{n_0+1}}\,,\ \frac{1}{10^{n_0+2}},\ \ldots < \epsilon\,,$$

[12]Quando os termos de uma sequência forem dados por meio de expansão decimal, para que a leitura fique mais clara, usaremos um ; para separar seus termos.

o que significa dizer que:

$$\left|\frac{1}{10^n} - 0\right| = \frac{1}{10^n} < \epsilon, \quad \forall n \geqslant n_0 .$$

Observação 7.84 -

Note que, pelo raciocínio inicial do Exemplo 7.83, para provarmos que uma sequência, $a_1, a_2, \ldots$, de números reais converge a um real α , basta testarmos cotas de erro do tipo $\epsilon = 1/10^N$, com $N = 1, 2, 3, \ldots$.

Exemplo 7.85 -

Generalizemos o exemplo anterior, provando que, sendo $r \in \mathbb{R}$:

$$1, r, r^2, r^3, \ldots, r^n, \ldots \text{ converge a zero } \iff |r| < 1 .$$

Prova:

Sendo x um número real, é imediato das propriedades da ordem que:
– nos casos $x > 1$, temos: $x < x^2 < x^3 < \ldots$;
– nos casos $0 < x < 1$, temos: $x > x^2 > x^3 > \ldots$.

Como $|r^n - 0| = |r|^n$, disto resulta que, nos casos $|r| > 1$, o erro absoluto de r^n, relativamente a $\alpha = 0$, cresce incessantemente e, então, não temos convergência. (O leitor é convidado a, por exemplo, escrever os termos da sequência nos casos $r = 2$ e $r = -2$). Nos casos $r = \pm 1$ também não há convergência a zero; com efeito, para $r = 1$, todos os termos da sequência valem 1 e, para $r = -1$, eles ficam oscilando entre 1 e -1.

Assim, resta examinarmos os casos $|r| < 1$, casos em que o erro absoluto decresce incessantemente. Mas, será que decresce a ponto de ficar menor do que qualquer cota dada? Mostremos que sim.

Sendo $0 < r < 1$, como $r < r^2 < r^3 < \ldots$, para termos $r^n < \epsilon, \forall\, n \geqslant\; n_0$, basta acharmos N , tal que $r^N < \epsilon$, e tomarmos $n_0 = N$.
Ora, como $R = 1/r > 1$, segue que $R < R^2 < R^3 < \ldots$ e cada termo é $R > 1$ vezes maior do que o anterior, de modo que para cada cota $\epsilon > 0$, existirá N suficientemente grande para que $R^N > 1/\epsilon$, ou seja, $1/r^N > 1/\epsilon$, e daí $r^N < \epsilon$.

Os casos $-1 < r < 0$ reduzem-se ao anterior, tomando-se valor absoluto.

CQD.

Exercício 195 -

A sequência $2\,;\,2,1\,;\,2,01\,;\,2,001\,;\,2,0001\,;\,\ldots$ *converge a* 2*.*

Exercício 196 -

Sendo $a_1, a_2, \ldots$ *, uma sequência de números reais e sendo* $c \neq 0$ *(número real não nulo):*

$$a_1, a_2, a_3, \ldots \text{ converge a zero } \iff ca_1, ca_2, ca_3, \ldots \text{ converge a zero}\,.$$

Dica:
dada uma cota de erro $\epsilon > 0$*, tome* n_0 *tal que* $|a_n - 0| < \epsilon/c$*,* $\forall n \geqslant n_0$*.*

Com a noção de sequência convergente, estamos com todos os ingredientes para, finalmente, interpretar as expansões decimais de números reais como uma "soma limite". Para isso, iniciamos observando que podemos ver a soma de qualquer quantidade finita de parcelas como o limite de uma sequência. Por exemplo, podemos ver $a + b + c$ como sendo o limite da sequência:

$$a\,,\, a+b\,,\, a+b+c,\, a+b+c+0\,,\, a+b+c+0+0\,,\, \ldots\,.$$

Generalizando, definiremos uma "soma" (note as aspas!) de infinitos números reais:

$$a_1 + a_2 + a_3 + \cdots + a_n + \cdots$$

como sendo o limite (se houver convergência) da sequência de somas parciais:

$$s_1 = a_1\,,\, s_2 = a_1 + a_2\,,\, \ldots\,, s_n = a_1 + a_2 + a_3 + \cdots + a_n, \ldots\,.$$

Coloquemos essas ideias numa definição, usando terminologia tradicional:

Definição 7.86 -

Uma série *de números reais é toda expressão da forma*

$$a_1 + a_2 + \cdots + a_n + \cdots\,,$$

ou, abreviadamente,

$$\sum_{k=1}^{\infty} a_k\,,$$

onde todos os $a_k \in \mathbb{R}$.

Dizemos que uma tal série converge *a um* $\alpha \in \mathbb{R}$, *ou que tem* $\alpha \in \mathbb{R}$ *como* soma limite, *se suas* somas parciais

$$s_1 = a_1\,,\; s_2 = a_1 + a_2\,,\; s_3 = a_1 + a_2 + a_3\,,\; \ldots\,, s_n = a_1 + a_2 + \cdots + a_n\,,\; \ldots$$

formarem uma sequência que converge a α.
Neste caso, também se costuma dizer que α *é a* soma da série, *e escrevemos*

$$\alpha = a_1 + a_2 + \cdots\,, \quad \text{ou} \quad \alpha = \sum_{k=1}^{\infty} a_k\,.$$

Exemplo 7.87 -

É imediato percebermos que, para qualquer escolha de uma quantidade finita de números reais, $a, b, c, \ldots, w$, *a série* $a + b + c + \cdots + w + 0 + 0 + 0 + \cdots$ *converge, e tem por soma limite o número real que é a soma* $a + b + c + \cdots + w$*; de modo que podemos escrever:*

$$a + b + c + \cdots + w = a + b + c + \cdots + w + 0 + 0 + 0 + \cdots\,.$$

Consequentemente, a noção de série convergente engloba a de soma de números reais. Equivalentemente: a noção de soma limite generaliza a de soma de números reais.

Exemplo 7.88 -

Nem toda série é convergente, um exemplo simples é:

$$1 - 1 + 1 - 1 + 1 - \cdots\,.$$

Com efeito, as somas parciais desta série formam uma sequência oscilante; formam a sequência não convergente do Exemplo 7.81:

$$s_1 = 1\,,\; s_2 = 0\,,\; s_3 = 1\,,\; s_4 = 0\,, \ldots\,.$$

Exercício 197 -

Outro tipo importante de séries não convergentes, é o das séries cujas somas parciais crescem infinitamente. O exemplo mais simples delas é o da série $1 + 1 + 1 + \cdots$. *Pede-se confirmar o que foi dito.*

Exemplo 7.89 -

Um dos mais importantes exemplos de séries convergentes é o da "soma" dos infinitos termos de uma progressão geométrica de razão r *, verificando* $|r| < 1$*.*
Com efeito, mostremos que

$$1 + r + r^2 + r^3 + \ldots = \frac{1}{1-r} \iff |r| < 1\,.$$

Prova:

Da teoria das séries geométricas, temos que, qualquer que seja $r \neq 1$:

$$s_n = 1 + r + r^3 + \ldots + r^{n-1} = \frac{1-r^n}{1-r}\,;$$

de modo que o erro absoluto da soma parcial s_n , em relação a $\alpha = 1/(1-r)$, será:

$$\Big|s_n - \frac{1}{1-r}\Big| = \Big|\frac{1-r^n}{1-r} - \frac{1}{1-r}\Big| = \frac{|r|^n}{|1-r|}\,.$$

Ora, pelo Exemplo 7.85 e o Exercício 196, segue que esse erro absoluto converge a zero $\iff$ $|r| < 1$.

CQD.

Exercício 198 -

Sendo $b \neq 0$*, mostre que a série* $a_1 + a_2 + a_3 + \cdots + a_n + \cdots$ *converge* $\iff$ *a série* $ba_1 + ba_2 + ba_3 + \cdots + ba_n + \cdots$ *converge, caso em que teremos:*

$$ba_1 + ba_2 + \cdots + ba_n + \cdots = b\big(a_1 + a_2 + \cdots + a_n + \cdots\big)\,.$$

Como um caso particular muito importante, se $a \neq 0$*:*

$$a + ar + ar^2 + ar^3 + \cdots = \frac{a}{1-r} \iff |r| < 1\,.$$

Exercício 199 -

A rigor, a prova do Exemplo 7.89 usou que uma série de números reais converge a $\alpha \in \mathbb{R} \iff$ *a sequência dos erros absolutos das suas somas parciais,* $|s_n - \alpha|$*, é uma sequência convergente a zero. Convença-se da veracidade disto.*

Exercício 200 -

Na prova do Exemplo 7.89, de saída, foi descartado o caso $r = 1$*. Por quê?*

- A noção de série numérica pode ser vista como uma generalização da noção de adição de números reais.
- Uma grande utilidade das séries convergentes é o fato que suas somas parciais nos dão aproximações arbitrariamente boas de sua soma limite.
- O Exemplo 7.88 nos mostra que nem toda série tem uma soma limite, ou seja: existem séries que não são convergentes. Outro exemplo importante desta possibilidade é o da série dos termos de uma progressão geométrica de razão $|r| \geqslant 1$.

Passemos, finalmente, a discutir diretamente o significado das expansões decimais de números reais como uma "soma limite". Iniciamos com um dos tipos mais simples de expansões decimais:

Exemplo 7.90 -

Pelo Exemplo 7.89, temos que:

$$r + r^2 + r^3 + \cdots = \frac{1}{1-r} - 1 = \frac{r}{1-r}\,, \quad \forall |r| < 1,$$

de modo que, pelo trivial Exercício 198, segue que:

$$ar + ar^2 + ar^3 + \cdots = \frac{ar}{1-r}\,, \quad \forall |r| < 1\,.$$

Disso, podemos escrever as seguintes igualdades, que devem ser vistas no contexto de séries convergentes:

$$\begin{aligned}
0{,}111\,111\ldots &= \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \cdots = \frac{1/10}{1-1/10} = \frac{1}{9}\\
0{,}222\,222\ldots &= \frac{2}{10} + \frac{2}{10^2} + \frac{2}{10^3} + \cdots = \frac{2/10}{1-1/10} = \frac{2}{9}\\
0{,}333\,333\ldots &= \frac{3}{10} + \frac{3}{10^2} + \frac{3}{10^3} + \cdots = \frac{3/10}{1-1/10} = \frac{3}{9}\\
&\cdots\cdots\cdots\\
0{,}999\,999\ldots &= \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \cdots = \frac{9/10}{1-1/10} = \frac{9}{9} = 1.
\end{aligned}$$

Vale a pena insistir que o exemplo anterior nos mostra que a Teoria das Séries nos permite interpretar

$$0,999\ldots = 1\,,$$

como uma igualdade dando o valor limite de uma série, resultado que já havíamos obtido usando intervalos encaixantes.

Exercício 201 -

Sem apelar para o Exemplo 7.89, conclua que $0,111\ldots = 1/9$ *depois de verificar que as somas parciais da série* $1/10 + 1/10^2 + 1/10^3 + \cdots$ *têm erro absoluto:*

$$\left|\frac{1}{10} + \frac{1}{10^2} + \cdots + \frac{1}{10^n} - \frac{1}{9}\right| = \frac{1}{9\cdot 10^{n+1}} \leqslant \frac{1}{10^n}\,.$$

O exemplo anterior nos leva a indagar se valeria um resultado semelhante para o caso de expansões decimais quaisquer. De modo mais preciso e completo:

Questão (1) –

> A todo número real r, dado por sua expansão decimal, $r = m, a_1a_2\ldots$, está naturalmente associada uma série numérica: $m + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots$. O exemplo anterior nos faz perguntar se tal série seria convergente e se sua soma limite valeria r. Em outras palavras, seria verdade que sempre vale a igualdade:
>
> $$m, a_1a_2\ldots = m + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots\ ?$$

Questão (2) –

> Reciprocamente, para toda escolha de $a_n \in \{0, 1, \ldots, 9\}$, podemos formar naturalmente uma série numérica, $\frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} + \cdots$, e é também natural perguntarmos se essa série seria convergente e se sua soma limite seria o número real dado pela expansão decimal associada: $0, a_1a_2\ldots$.

Essas duas questões têm resposta afirmativa, conforme se poderá perceber imediatamente a partir do resultado fundamental que segue.

Teorema 7.91 -

Sendo $a_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $\forall n \geqslant 1$, *formemos a série numérica:*

$$\frac{a_1}{10} + \frac{a_2}{10^2} + \cdots = \sum_{n=1}^{\infty} \frac{a_n}{10^n}.$$

Então, qualquer que tenha sido a escolha de valores feita para os a_n*, teremos que a série acima converge, e sua soma limite é o número real associado à expansão decimal* $0, a_1 a_2 \ldots$ *. Ou seja:*

$$0, a_1 a_2 \ldots = \sum_{n=1}^{\infty} \frac{a_n}{10^n} = \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots .$$

Prova:

Vendo os tais a_n como dígitos, formemos a expansão decimal $0, a_1 a_2 \ldots$, e indiquemos por r o número real por ela representado. Sabemos que vale:

$$\left| \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} - r \right| \leqslant \frac{1}{10^n}.$$

Ora, isso significa dizer que a série numérica

$$\sum_{n=1}^{\infty} \frac{a_n}{10^n}$$

tem somas parciais s_n verificando:

$$|s_n - r| \leqslant \frac{1}{10^n}, \forall n \geqslant 1,$$

o que, conforme já vimos algumas vezes, significa que tal série numérica converge, e tem r como soma limite:

$$0, a_1 a_2 \ldots = r = \sum_{n=1}^{\infty} \frac{a_n}{10^n} = \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots .$$

CQD.

Exercício 202 -

Usando o último teorema, responda as duas questões colocadas anteriormente.

Com o teorema e o exercício anteriores, estamos concluindo que igualdades do tipo

$$m, a_1 a_2 \dots a_n \dots = m + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} + \cdots ,$$

onde cada a_n é um dígito, podem ser interpretadas equivalentemente tanto pela Teoria das Séries Numéricas, como pela construção dos números reais – conforme vista neste livro.

Observação 7.92 -

O leitor que já estudou a Teoria das Séries, principalmente no contexto da Análise Matemática, deve estar lembrado de que lá o teorema recém enunciado é provado com o uso da bastante sofisticada noção de supremo. Ademais, lá também se precisa usar um teorema que garante que, se $a_1 + a_2 + \cdots$ é uma série cujos termos são todos positivos, então podemos afirmar que a mesma é obrigatoriamente convergente, sempre que cada $a_n \leqslant b_n$, onde os b_n são os termos de uma série que já se sabe ser convergente.[13]

A prova aqui dada evitou o uso dessas sofisticações, pois nossa construção dos números reais está solidamente alicerçada na estimativa do erro da aproximação $0, a_1 a_2 \dots a_n$ de $0, a_1 a_2 \dots$.

[13]Veja, por exemplo, *Análise Matemática Para a Licenciatura*, de Geraldo Ávila, Ed. Edgard Blücher.

7.11 Leitura complementar: prova de que os reais formam corpo ordenado

É possível se provar, usando argumentos exclusivamente baseados em intervalos encaixantes, como até aqui fizemos, que o campo dos números reais tem uma estrutura de corpo ordenado. Contudo, essa demonstração ficaria excessivamente cansativa e detalhista. Assim, visando uma argumentação alternativa, mais curta e de leitura menos desestimulante, optamos por combinar a ideia de limite (ou convergência) de sequências de números reais com a de intervalos encaixantes. Isso será feito sem elevar o nível de leitura para o de um curso de Análise Matemática.

Também é de se observar que, embora já tenhamos tratado da noção de convergência de sequências – na Leitura Complementar anterior, sobre séries –, a presente Leitura é independente daquela. Num exercício adiante, Exercício **??**, compara-se a ideia de convergência introduzida nessas duas Leituras.

Notação:
Iniciemos introduzindo algumas notações convenientes aos nossos propósitos:

- dado um número real x, passaremos a denotar por $x = M, a_1a_2a_3\dots$ uma sua expansão decimal (onde M é um inteiro positivo, negativo ou nulo);
- indicaremos por x_n o número racional que é o truncamento da expansão decimal de x na n-ésima casa decimal, ou seja: $x_n = M, a_1a_2\dots a_n$;
- por "sequência de números reais $x(n)$", deve-se entender que estamos nos referindo a uma sequência $x(1), x(2), \dots$ onde cada um dos termos é um real;
- indicaremos por $[x]_n$ o número racional dado por:

$$[x]_n = \begin{cases} M, a_1a_2\dots a_n & (\text{se } x \geqslant 0) \\ M, a_1a_2\dots a_n - \frac{1}{10^n} & (\text{se } x < 0)\,, \end{cases}$$

ou, equivalentemente:

$$[x]_n = \begin{cases} x_n & (\text{se } x \geqslant 0) \\ -|x_n| - \frac{1}{10^n} & (\text{se } x < 0)\,. \end{cases} \tag{7.7}$$

Uma especial vantagem da nova notação $[x]_n$ é que, qualquer que seja o sinal de x:

$$[x]_n \leqslant x \leqslant [x]_n + \frac{1}{10^n} \qquad (\forall n \geqslant 1)\,. \tag{7.8}$$

Também é importante observar que a sequência dos intervalos

$$\left[[x]_n \, , [x]_n + \frac{1}{10^n} \right]$$

é encaixante e evanescente, e contém x.

Exercício 203 -

Prove que para todo real $x \neq 0$, independentemente de seu sinal:

$$[-x]_n = -\,[x]_n - \frac{1}{10^n}\,.$$

Exercício 204 -

Prove que para quaisquer reais x e y, independentemente de seus sinais:

$$x < y \;\Rightarrow\; \textit{existe } n_0, \;\; \textit{tal que } [x]_n < [y]_n \, (\textit{para todo } n > n_0).$$

Dica: considere os três casos $0 \leqslant x < y$, $x < 0 \leqslant y$ e $x < y < 0$.

Proposição 7.93 -

Sendo x e y números reais, independentemente de seus sinais, sua soma $x + y$ é o único número real pertencente a todos os intervalos

$$\left[[x]_n + [y]_n \, , [x]_n + [y]_n + \frac{2}{10^n} \right]. \tag{7.9}$$

Prova:

São três possibilidades a considerar.

– Caso $x \geqslant 0$ e $y \geqslant 0$:
a afirmação é óbvia (veja definição de soma de números reais).
– Caso $x < 0$ e $y < 0$:
neste caso: $x + y = -(|x| + |y|)$, de modo que $x + y$ é o único número real comum a todos os intervalos

$$\left[-|x|_n - |y|_n - \frac{2}{10^n}, \; -|x|_n - |y|_n \right] .$$

Assim, de (7.7)

$$\left[-|x|_n - |y|_n - \frac{2}{10^n},\ -|x|_n - |y|_n\right] = \left[[x]_n + [y]_n\,, [x]_n + [y]_n + \frac{2}{10^n}\right].$$

– Caso $x \geqslant 0$ e $y < 0$:
da definição de soma, $x + y$ é o único número real comum a todos os intervalos

$$\left[x_n - |y|_n - \frac{1}{10^n},\ x_n - |y|_n + \frac{1}{10^n}\right] = \left[[x]_n + [y]_n\,, [x]_n + [y]_n + \frac{2}{10^n}\right].$$

CQD.

Proposição 7.94 -

Sendo x e y números reais:

- *caso $x \geqslant 0$ e $y \geqslant 0$, então seu produto $x \cdot y$ é o único real pertencente aos intervalos*

$$\left[[x]_n\,[y]_n\,, \left([x]_n + \frac{1}{10^n}\right)\left([y]_n + \frac{1}{10^n}\right)\right]\ ; \tag{7.10}$$

- *caso $x < 0$ e $y < 0$, então seu produto $x \cdot y$ é o único real pertencente aos intervalos*

$$\left[\left([x]_n + \frac{1}{10^n}\right)\left([y]_n + \frac{1}{10^n}\right), [x]_n\,[y]_n\right]\ ; \tag{7.11}$$

- *caso $x \geqslant 0$ e $y < 0$, então seu produto $x \cdot y$ é o único real pertencente aos intervalos*

$$\left[\left([x]_n + \frac{1}{10^n}\right)[y]_n\,, [x]_n\left([y]_n + \frac{1}{10^n}\right)\right]. \tag{7.12}$$

Prova:

– Caso $x \geqslant 0$ e $y \geqslant 0$:
este caso é óbvio da definição de produto.

– Caso $x < 0$ e $y < 0$:
neste caso, pela definição de produto de negativos: $x \cdot y = |x| \cdot |y|$, de modo que $x \cdot y$ é o único número real comum a todos os intervalos

$$\left[|x|_n |y|_n,\ \left(|x|_n + \frac{1}{10^n}\right)\left(|y|_n + \frac{1}{10^n}\right)\right]. \tag{7.13}$$

Usando (7.7), obtemos:

$$|x|_n|y|_n = (-|x|_n)\,(-|y|_n) = \left([x]_n + \frac{1}{10^n}\right)\left([y]_n + \frac{1}{10^n}\right)$$

e

$$\left(|x|_n + \frac{1}{10^n}\right)\left(|y|_n + \frac{1}{10^n}\right) = \left(-|x|_n - \frac{1}{10^n}\right)\left(-|y|_n - \frac{1}{10^n}\right) = [x]_n\,[y]_n\ ,$$

o que prova que podemos trocar (7.13) por (7.11), conforme afirmado.

– Caso $x \geqslant 0$ e $y < 0$:
neste caso, pela definição de produto: $x \cdot y = -(x \cdot |y|)$. Como $x \cdot |y|$ é o único número real comum a todos os intervalos

$$\left[x_n\,|y|_n\,,\left(x_n + \frac{1}{10^n}\right)\left(|y|_n + \frac{1}{10^n}\right)\right],$$

temos que $x \cdot y = -(x \cdot |y|)$ é o único número real comum a todos os intervalos

$$\left[-\left(x_n + \frac{1}{10^n}\right)\left(|y|_n + \frac{1}{10^n}\right), -x_n\,|y|_n\right] \overset{(7.7)}{=} \left[\left([x]_n + \frac{1}{10^n}\right)[y]_n\,, [x]_n\left([y]_n + \frac{1}{10^n}\right)\right].$$

CQD.

Definição 7.95 -

Dizemos que um intervalo $I = [a, b]$ é um ***intervalo em torno de*** x *se* $a < x < b$.

Note que é possível termos $[x]_n = x$, tanto no caso $x \geqslant 0$, como no caso $x < 0$. Por exemplo,

$$x = 3,53 \Rightarrow x = [x]_n\,,\ \text{para todo } n \geqslant 2;$$
$$x = -3,53\overline{9} \Rightarrow x = [x]_n\,,\ \text{para todo } n \geqslant 3,$$

de modo que a sequência dos intervalos

$$\left[[x]_n\,, [x]_n + \frac{1}{10^n}\right]$$

sempre é uma sequência encaixante e evanescente, mas nem sempre será formada por intervalos em torno de x.

Observação 7.96 -

No que segue, precisaremos falar tanto de sequências de números reais, como de sequências de intervalos. Será crucial o leitor observar os índices que usaremos para denotar os elementos dessas sequências.
Na medida do possível, denotaremos por $x(n)$ os elementos de sequências de números reais, e por I_m os elementos de sequências de intervalos.

Definição 7.97 -

Dizemos que uma sequência de números reais $x(n)$ converge a um real *α se pudermos determinar uma sequência encaixante e evanescente de intervalos I_m em torno de a, tal que, para cada escolha de $m \in \mathbb{N}$, exista n_0, tal que $x(n) \in I_m \quad (\forall n > n_0)$.*
Sendo $x(n)$ convergente a α também dizemos que α é o limite dos *$x(n)$, e escrevemos*

$$\alpha = \lim\ x(n)\,.$$

Exemplo 7.98 -

A sequência $1, 1/2, 1/3, \ldots$ (ou seja: a sequência dos $x(n) = 1/n$) converge a $\alpha = 0$. Por outro lado, a sequência $1, -1, 1, -1, \ldots$ (ou seja: a sequência dos $x(n) = (-1)^n$) não converge a nenhum número real.

Exercício 205 -

Prove que a definição acima está bem feita, no sentido de não depender da sequência dos intervalos I_m. Ou seja: sempre que outros J_m formarem uma sequência encaixante e evanescente de intervalos em torno de α, então, para cada m, existirá n_1 tal que $x(n) \in I_m \quad (\forall n > n_1)$ se, e somente se, para cada m, exista n_2, tal que $x(n) \in J_m \quad (\forall n > n_2)$.

Exercício 206 -

Prove a unicidade do limite, ou seja: se α e β são limites de uma mesma sequência de números reais, então $\alpha = \beta$.
Dica: note que se uma sequência de números reais $x(n)$ convergir a um real α, e se os I_m formarem uma sequência encaixante e evanescente de intervalos em torno de α, pelo Teorema dos Intervalos Encaixantes e Evanescentes, esse α será o único número real com a propriedade de pertencer a todos esses intervalos.

Também vale uma espécie de recíproca:

Proposição 7.99 -

Ocorrendo que os intervalos I_m formem uma sequência de intervalos encaixantes e evanescentes contendo α (mas não necessariamente em torno de α), sempre que os números reais $x(n)$ formarem uma sequência verificando $x(n) \in I_n \quad (\forall n \geqslant 1)$, poderemos afirmar que $x(n)$ converge para α.

Prova:

Denotando $I_m = [a_m, b_m]$, construamos:

$$J_m = \left[a_m - \frac{1}{m}\,,\, b_m + \frac{1}{m}\right].$$

É imediato se ver que os J_m também formam uma sequência de intervalos encaixantes e evanescentes, agora todos em torno de α, e que, qualquer que seja m, tem-se $x(n) \in J_m \quad (\forall n \geqslant m)$.

CQD.

Na proposição que segue, mostra-se como a notação [ ] nos permite fornecer um exemplo de sequência que converge a qualquer real pré-fixado x:

Proposição 7.100 -

Seja qual for o número real x, a sequência dos $x(n) = [x]_n$ sempre converge a x. Simbolicamente:

$$\boxed{x = \lim\,[x]_n\,.}$$

Prova:

É uma decorrência da proposição anterior, do fato que os $I_n = \left[[x]_n, [x]_n + \frac{1}{10^n}\right]$ formam uma sequência de intervalos encaixantes e evanescentes contendo x, e que $[x]_n \in I_n$, para todo n.

CQD.

Exemplo 7.101 -

Quando $x = 12,333\ldots$, *temos que* x *é o limite da sequência:*
$[x]_1 = 12,3$, $[x]_2 = 12,33$, $[x]_3 = 12,333$, $[x]_4 = 12,3333$, *etc.*

Exercício 207 -

Prove que a definição de limite dada acima é equivalente à noção de convergência dada na Leitura Complementar anterior, sobre séries.

Exercício 208 -

Dado um número real x*, como é usual, denotamos por* $x = M, a_1a_2a_3\ldots$ *uma sua expansão decimal. Na Leitura Complementar anterior, mostramos que a noção de série nos permite interpretar essa expansão decimal como uma "soma infinita":*

$$x = M, a_1a_2a_3\ldots = M + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots + \frac{a_n}{10^n} + \cdots = M + \sum_{n=1}^{\infty} \frac{a_n}{10^n}\,.$$

Mostre que o significado disso pode ser mais precisamente expresso como:

$$x = M, a_1a_2a_3\ldots = \lim \big(M + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots + \frac{a_n}{10^n}\big)\,.$$

Proposição 7.102 -

Sendo x *e* y *números reais, temos:*

i).
$$x + y = \lim\,[x+y]_n = \lim\,([x]_n + [y]_n) = \lim\,[x]_n + \lim\,[y]_n\,;$$

ii).
$$x \cdot y = \lim[x \cdot y]_n = \lim\,([x]_n \cdot [y]_n) = \lim\,[x]_n\, \cdot\, \lim\,[y]_n\,;$$

iii).
$$-x = \lim\,[-x]_n = \lim\,(-[x]_n)\,.$$

Prova:

Para (i):
a única afirmação que não decorre imediatamente da Proposição 7.100 é a igualdade $x + y = \lim\big([x]_n + [y]_n\big)$; mas, esta decorre facilmente da Proposição 7.93.

Para (ii):
a única afirmação que não decorre imediatamente da Proposição 7.100 é a igualdade $x \cdot y = \lim\big([x]_n \cdot [y]_n\big)$; mas, exceto nos casos em que $x \geqslant 0$ e $y < 0$, esta decorre facilmente da Proposição 7.94. Ora, para tais casos basta notar que:

$$\Big([x]_n + \frac{1}{10^n}\Big)[y]_n = [x]_n[y]_n + \frac{[y]_n}{10^n} \leqslant [x]_n[y]_n \leqslant [x]_n\,[y]_n + \frac{[x]_n}{10^n} = [x]_n\,\Big([y]_n + \frac{1}{10^n}\Big),$$

já que $[x]_n \geqslant 0$ e $[y]_n < 0$.

Para (iii):
como a afirmação é óbvia se $x = 0$, basta tratarmos dos casos em que $x \neq 0$. Em tais casos, o Exercício 203 mostra que $-[x]_n = [-x]_n + \frac{1}{10^n}$. Então, usando o fato óbvio que a sequência dos $1/10^n$ converge a 0 e que, pela Proposição 7.100, a sequência dos $[-x]_n$ converge a $-x$, segue que a sequência dos $-[x]_n$ converge a $-x$.

CQD.

Lema 7.103 -

Sejam $r(n)$, $s(n)$ e $t(n)$ números racionais *formando três sequências convergentes; suponhamos, ademais, que vale a seguinte igualdade de limites:*

$$\lim s(n) = \lim t(n)\,.$$

Então:

a). a sequência das somas $r(n) + t(n)$ e a das $r(n) + s(n)$ serão convergentes, e teremos $\lim r(n) + t(n) = \lim r(n) + s(n)$;

b). a sequência dos produtos $r(n) \cdot t(n)$ e a dos $r(n) \cdot s(n)$ serão convergentes, e teremos $\lim r(n) \cdot t(n) = \lim r(n) \cdot s(n)$.

Prova:

Para (a):
precisamos provar que $a+b = \lim\,(r(n) + s(n))$, se $a = \lim r(n)$ e $b = \lim s(n) = \lim t(n)$.

Iniciamos observando que, como $a \in \big[[a]_m, [a]_m + \frac{1}{10^m}\big]$ $\quad(\forall m \geqslant 1)$, e como $a = \lim r(n)$, podemos determinar, qualquer que seja m dado, um n_1 tal que:

$$r(n) \in \left[[a]_m, [a]_m + \frac{1}{10^m}\right] \quad (\forall n > n_1)\,,$$

ou, equivalentemente, para todo $n > n_1$:

$$[a]_m \leqslant r(n) \leqslant [a]_m + \frac{1}{10^m}\,.$$

Da mesma forma, existe n_2 tal que, para todo $n > n_2$:

$$[b]_m \leqslant s(n) \leqslant [b]_m + \frac{1}{10^m}\,.$$

Dessas desigualdades segue que, se $n_0 = \max\{n_1, n_2\}$, pela compatibilidade da ordem em relação à adição de *números racionais*, teremos:

$$[a]_m + [b]_m \leqslant r(n) + s(n) \leqslant [a]_m + [b]_m + \frac{2}{10^m}\,,$$

ou seja, a sequência dos $y(n) = r(n) + s(n) \in I_m$, para todo $n \geqslant n_0$. Ora, os intervalos

$$I_m = \left[[a]_m + [b]_m, [a]_m + [b]_m + \frac{2}{10^m}\right]$$

são encaixantes e evanescentes e contêm $a+b$, para todo $m \geqslant 1$, pela Proposição 7.93. Logo podemos afirmar não só que os $y(n)$ convergem, mas que $a + b = \lim y(n)$. Ademais, como para esta conclusão usou-se apenas o fato de que $a = \lim r(n)$ e $b = \lim s(n)$, decorre de maneira análoga que $a+b = \lim x(n)$, onde $x(n) = r(n) + t(n)$.

Para (b):
a prova é similar à feita em (a), mas aqui temos que considerar três casos: $x, y \geqslant 0$; $x, y \leqslant 0$; e $x \leqslant 0$, $y \geqslant 0$. Ora, pela Proposição 7.94, os intervalos I_m dados por (7.10), (7.11) e (7.12) são encaixantes e evanescentes, e tem-se que $xy \in I_m$, para todo $m \geqslant 1$; logo, da compatibilidade da ordem com relação à multiplicação de *números racionais*, decorre que, para cada $m \geqslant 1$, existirá um n_0 tais que as desigualdades seguintes são satisfeitas, para todos os $n \geqslant n_0$:

- no caso $x, y \geqslant 0$:

$$[x]_m\,[y]_m \leqslant r(n)s(n) \leqslant \left([x]_m + \frac{1}{10^m}\right)\left([y]_m + \frac{1}{10^m}\right)\,;$$

- no caso $x < 0$, $y < 0$:

$$\left([x]_m + \frac{1}{10^m}\right)\left([y]_m + \frac{1}{10^m}\right) \leqslant r(n)s(n) \leqslant [x]_m\,[y]_m\,;$$

- e no caso $x \geqslant 0$, $y < 0$:

$$\left([x]_m + \frac{1}{10^m}\right)[y]_m \leqslant r(n)s(n) \leqslant [x]_m\left([y]_m + \frac{1}{10^m}\right).$$

CQD.

Lema 7.104 -

Sejam duas sequências convergentes de números reais, $x(n)$ e $y(n)$, verificando $x(n) < y(n)$, para todo n maior ou igual a um certo $n_0 \geqslant 1$. Então, ou $\lim x(n) = \lim y(n)$ ou $\lim x(n) < \lim y(n)$.

Prova:

Escrevendo $a = \lim x(n)$ e $y = \lim y(n)$, temos de mostrar que $a \leqslant b$. Suponhamos, por absurdo, que $a > b$. Sejam $I_m = [r_m, s_m]$ e $J_m = [c_m, d_m]$ intervalos em torno de a e b, respectivamente, e formando sequências de intervalos encaixantes e evanescentes. Se $I_m \cap J_m \neq \varnothing \quad (\forall m \geqslant 1)$, então, para cada m, poderemos tomar um número real $z(m)$, tal que $z(m) \in I_m$ e $z(m) \in J_m$. Segue-se que a e b são limites da sequência dos $z(n)$. Da unicidade do limite (Exercício 206), concluímos $a = b$, absurdo. Logo tem de existir m_1, tal que $I_{m_1} \cap J_{m_1} = \varnothing$. Como $a > b$, segue facilmente da propriedade transitiva da relação de ordem que $d_{m_1} < r_{m_1}$. De $a = \lim x(n)$ e $b = \lim y(n)$ encontramos n_1, tal que $x(n_1) \in I_{m_1}$ e $y(n_1) \in J_{m_1}$, o que implica que

$$y(n_1) \leqslant d_{m_1} < r_{m_1} \leqslant x(n_1).$$

Logo: $y(n_1) < x(n_1)$, absurdo!

CQD.

Teorema 7.105 -

O campo dos números reais, $[\mathbb{R}, +, \cdot, <]$, forma um corpo ordenado.

Prova:
A demonstração desse teorema equivale a provar que, para quaisquer números reais x, y e z, valem as propriedades enumeradas de a) até k), a seguir.
Na demonstração, usaremos repetidamente que $[x]_n$ será um número racional, para

qualquer número real x, e que, pela Proposição 7.100, a sequência dos $[x]_n$ sempre converge a x.

a). Comutatividade da adição:
pela comutatividade da adição de números racionais, teremos:

$$x + y \overset{\text{Prop.7.102}}{=} \lim\left([x]_n + [y]_n\right) = \lim\left([y]_n + [x]_n\right) \overset{\text{Prop.7.102}}{=} y + x\,.$$

b). Existência de elemento neutro na adição:
pelo fato de 0 ser elemento neutro da adição de racionais teremos:

$$x + 0 \overset{\text{Prop.7.102}}{=} \lim\left([x]_n + [0]_n\right) = \lim\,[x]_n \overset{\text{Prop.7.102}}{=} x$$

c). Elemento simétrico aditivo:
pela Proposição 7.102 *(iii)* e pelo Lema 7.103 *(a)*, teremos:

$$x + (-x) = \lim\left([x]_n + [-x]_n)\right) = \lim\left([x]_n - [x]_n\right) = \lim 0 = 0\,.$$

d). Associatividade da adição:
fazendo uso da associatividade da adição de racionais, teremos:

$$\begin{aligned} x + (y+z) &\overset{\text{Prop. 7.102}}{=} \lim\left([x]_n + [y+z]_n\right) \overset{\text{Lema 7.103}(a)}{=} \lim\left([x]_n + ([y]_n + [z]_n)\right) \\ &\overset{\text{racion.}}{=} \lim\left(([x]_n + [y]_n) + [z]_n\right) \overset{\text{Lema 7.103}(a)}{=} \lim\left([x+y]_n + [z]_n\right) \\ &\overset{\text{Prop. 7.102}}{=} (x+y) + z\,. \end{aligned}$$

e). Comutatividade da multiplicação:
fazendo uso da comutatividade da multiplicação de racionais, teremos:

$$xy \overset{\text{Prop. 7.102}}{=} \lim\left([x]_n\,[y]_n\right) = \lim\left([y]_n\,[x]_n\right) \overset{\text{Prop. 7.102}}{=} yx\,.$$

f). Existência de elemento neutro na multiplicação (unidade):
pelo fato de 1 ser elemento neutro da multiplicação de racionais, teremos:

$$x.1 \overset{\text{Prop.7.102}}{=} \lim\left([x]_n\,[1]_n\right) = \lim\left([x]_n\,.1\right) = \lim\left([x]_n\right) \overset{\text{Prop.7.100}}{=} x\,.$$

g). Existência de inverso multiplicativo (recíproco):
dado $x \neq 0$, precisamos provar que existe y, tal que $xy = 1$. Faremos isso apenas no caso em que $x > 0$, deixando o caso $x < 0$ como exercício.

Dado um número real $x > 0$, existe um correspondente n_0, tal que $[x]_n > 0$, para todos os $n > n_0$ (basta, para tal, considerar a sequência de intervalos encaixantes e evanescentes $\left[0,\ x + \frac{1}{10^m}\right]$).

Daí os intervalos

$$I_m = \left[\frac{1}{[x]_m + \frac{1}{10^m}}, \frac{1}{[x]_m}\right], \ m > n_0,$$

contêm apenas números positivos, e são encaixantes e evanescentes, contendo, portanto, um único real y. Ora, a média aritmética, $z(m)$, entre os extremos de cada intervalo I_m, com $m > n_0$, verifica:

$$z(m) = \frac{1}{2} \cdot \left(\frac{1}{[x]_m + \frac{1}{10^m}} + \frac{1}{[x]_m}\right) \in I_m\,, \quad (\forall m > n_0)\,;$$

de modo que, conforme acima observado, $\lim z(m) = y$. Além disso, tem-se, pela compatibilidade da multiplicação de racionais com a ordem:

$$[x]_m\, z_m \in \left[\frac{[x]_m}{[x]_m + \frac{1}{10^m}}, \frac{[x]_m}{[x]_m}\right] = \left[\frac{[x]_m}{[x]_m + \frac{1}{10^m}}, 1\right].$$

Como todos esses intervalos contêm 1 e formam, além disso, uma sequência encaixante e evanescente, segue que:

$$\lim\left([x]_m\, z(m)\right) = 1.$$

Assim, como $y = \lim[y]_m = \lim z(m)$, do Lema 7.103 (b) segue:

$$xy = \lim\left([x]_m\, [y]_m\right) = \lim\left([x]_m\, z(m)\right) = 1\,.$$

h). Associatividade da multiplicação:
pela associatividade da multiplicação de racionais, teremos:

$$x(yz) \overset{\text{Prop.7.102}}{=} \lim\big([x]_n\, [yz]_n\big) \overset{\text{Lema } 7.103(b)}{=} \lim\big([x]_n\ ([y]_n[z]_n)\,\big)$$
$$= \lim\big(\,([x]_n[y]_n)\ [z]_n\big) \overset{\text{Lema } 7.103(b)}{=} \lim\big([xy]_n\, [z]_n\big) \overset{\text{Prop. } 7.102}{=} (xy)z\,.$$

i). Distributividade da multiplicação:
pela distributividade da multiplicação em relação à adição de racionais, teremos:

$$x\,(y+z) \underset{\text{Lema } 7.103(a)}{\overset{\text{Prop. } 7.102}{=}} \lim\big([x]_n\, ([y]_n + [z]_n)\,\big) =$$

$$= \lim\left([x]_n\, [y]_n + [x]_n\, [z]_n\right) \underset{\text{Lema } 7.103}{\overset{\text{Prop.7.102}}{=}} \lim\left([xy + xz]_n\right) = xy + yz\,.$$

j). Compatibilidade da ordem com a adição: $\mathbf{x} < \mathbf{y} \Rightarrow \mathbf{x} + \mathbf{z} < \mathbf{y} + \mathbf{z}$:
pelo Exercício 204, como $x < y$, segue que existe n_0, tal que $[x]_n < [y]_n$, para todos os $n > n_0$. Logo, pela compatibilidade da ordem com a adição de racionais, teremos:

$$[x]_n + [z]_n < [y]_n + [z]_n\,, \quad (\forall n > n_0)\,.$$

Ora, já sabemos pela Proposição 7.102 que

$$x + z = \lim [x]_n + [z]_n \quad \text{e} \quad y + z = \lim [y]_n + [z]_n\ ;$$

portanto, pelo Lema 7.104, podemos concluir que

$$x + z \leqslant y + z\,.$$

Resta provarmos que a igualdade não ocorre. Por absurdo: se $x+z = y+z$, somando $-z$ a ambos os membros, teríamos: $(x+z)+(-z) = (y+z)+(-z)$; mas, daí, pela associatividade da adição:

$$x + \big(z + (-z)\big) = y + \big(z + (-z)\big) \Rightarrow x + 0 = y + 0 \Rightarrow x = y\,.$$

Absurdo!

k). Compatibilidade da ordem com a multiplicação: $(\mathbf{x} < \mathbf{y})$ e $(\mathbf{z} > \mathbf{0}) \Rightarrow \mathbf{xz} < \mathbf{yz}$:
pelo Exercício 204, como $x < y$ e $z > 0$, segue que existe n_0 tal que $[x]_n < [y]_n$ e $[z]_n > 0$, para todos os $n > n_0$. Logo, pela compatibilidade da ordem com a multiplicação de racionais, teremos:

$$[x]_n\,[z]_n < [y]_n\,[z]_n\ , \quad (\forall n > n_0)\,.$$

Ora, já sabemos pela Proposição 7.102 que

$$xz = \lim [x]_n\,[z]_n \quad \text{e} \quad yz = \lim [y]_n\,[z]_n\,,$$

de modo que, pelo Lema 7.104, podemos concluir que

$$xz \leqslant yz\,.$$

Resta provarmos que a igualdade não ocorre. Por absurdo: se $xz = yz$, multiplicando ambos os membros pelo recíproco z^{-1} de $z > 0$, teríamos $(xz)z^{-1} = (yz)z^{-1}$; mas, daí, pela associatividade da multiplicação:

$$x(zz^{-1}) = y(zz^{-1}) \Rightarrow x \cdot 1 = y \cdot 1 \Rightarrow x = y\,.$$

Absurdo! CQD.

Considerações finais:

O leitor, se já familiarizado com a Teoria dos Limites, poderá observar que nesta Leitura Complementar não se fez nenhum uso daquela; foram usadas apenas propriedades de sequências numéricas especiais (como na Proposição 7.102 e no Lema 7.103).

Exercício 209 -

Prove a existência de inverso multiplicativo para $x < 0$.

Encerrando esta Leitura Complementar, deixamos para o leitor o seguinte exercício, que ressalta uma parte das duas demonstrações acima:

Exercício 210 -

Prove as Leis do Cancelamento:

i). da adição:
$x + y = x + z \Rightarrow y = z$ *(se* x, y *e* z *forem reais);*

ii). da multiplicação:
$(xy = xz)$ *e* $(x \neq 0) \Rightarrow y = z$ *(se* x, y *e* z *forem reais).*

7.12 Leitura complementar: Teorema Fundamental da Geometria Analítica

No que segue, por plano entenderemos o plano euclidiano e, por lugar geométrico, entenderemos o conjunto dos pontos do plano que satisfazem uma ou mais propriedades dadas, definitórias. Por exemplo, o círculo de raio r e centro no ponto O é o lugar geométrico dos pontos do plano que estão à distância r de O. Um tipo importante de lugares geométricos é o das curvas.

Um problema central da Geometria é a análise dos lugares geométricos, sendo que por tal análise entende-se o estudo e descrição das propriedades desses, e seu resumo por meio de um gráfico.

A disciplina Geometria Analítica é a parte da Geometria que estuda e descreve os lugares geométricos, usando na análise os métodos algébricos.

O objetivo desta Leitura é enfatizar que a Geometria Analítica resulta da mistura de três ingredientes:

- a correspondência biunívoca entre os pontos da reta euclidiana e o conjunto dos números reais; ou seja, depende crucialmente do que já chamamos de Teorema Fundamental da Geometria Analítica (TFGA);
- a álgebra literal;
- o uso de sistemas de coordenadas.

É importante destacar que os gregos clássicos, principalmente Menaichmos (c. 350 AC) e Apollonios (c. 200 AC), desenvolveram uma geometria analítica rudimentar. Embora tivessem bastante sucesso em sua aplicação no estudo das cônicas, era uma geometria analítica muito difícil, pois a álgebra que utilizava era uma *álgebra geométrica* e seus sistemas de coordenadas que usava dependiam muito do lugar geométrico em estudo (um exemplo: diâmetros das cônicas). Ou seja: além de difícil, dependia de engenhosas improvisações.

Essa situação perdurou até cerca de 1 620, quando Fermat estabeleceu uma correspondência entre lugares geométricos planos e equações do tipo $f(x,y) = 0$, onde x e y são as coordenadas dos pontos do lugar, relativamente a um sistema de eixos ortogonais. Mas a maior contribuição de Fermat consistiu em mostrar como analisar o lugar geométrico, processando a equação $f(x,y) = 0$ com o uso da álgebra literal criada por Viète, c. 1 600. Com efeito, com essa álgebra, ficou fácil e mecânico extrair da equação as propriedades geométricas do lugar.

Estava assim criada a Geometria Analítica atual. Esta e o Cálculo Infinitesimal foram os ingredientes que propiciaram o desenvolvimento explosivo das ciências e tecnologias a partir de c. 1 700.

Exemplo 7.106 -

Fixados os pontos de coordenadas cartesianas $A = (-2, 1)$ e $B = (0, 2)$, consideremos o seguinte lugar geométrico:

$$\gamma = \textit{conjunto dos pontos do plano que são equidistantes de } A \textit{ e } B.$$

Indicando por $P = (x, y)$ um ponto genérico de γ, da igualdade de comprimentos $\overline{AP} = \overline{BP}$, segue:

$$\overline{AP}^2 = \overline{BP}^2 \quad \therefore \quad (x+2)^2 + (y-1)^2 = (x-0)^2 + (y-2)^2 .$$

Desenvolvendo algebricamente os quadrados envolvidos:

$$x^2 + 4x + 4 + y^2 - 2y + 1 = x^2 + y^2 - 4y + 4 ,$$

o que, uma vez simplificado, nos dá a equação $f(x,y) = 0$ seguinte:

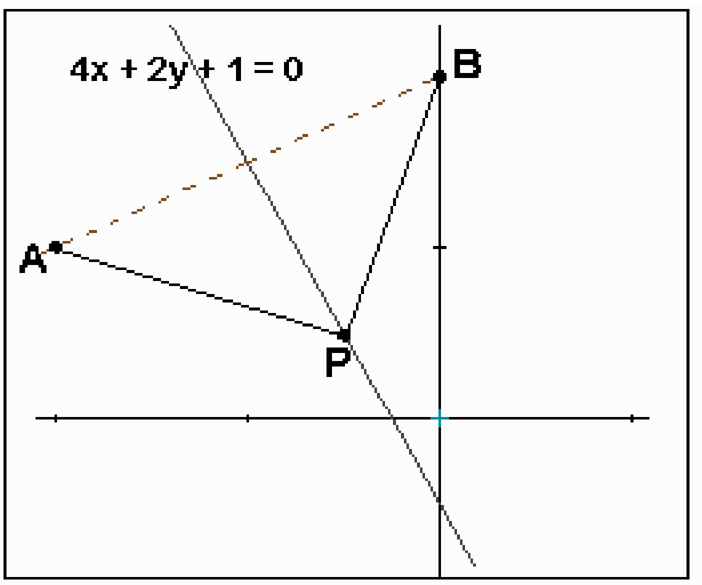
$$4x + 2y + 1 = 0 .$$

Sendo (x_1, y_1) *e* (x_2, y_2) *dois pontos quaisquer desse lugar geométrico, da equação obtemos:* $4x_1 + 2y_1 + 1 = 0$ *e* $4x_2 + 2y_2 + 1 = 0$*, de modo que:*

$$\frac{y_2 - y_1}{x_2 - x_1} = -\frac{1}{2} = \textit{constante}\,,\ \forall x_1 \neq x_2\,,$$

de onde concluímos que o lugar geométrico é uma reta.

Podemos melhorar a descrição dessa reta observando que $x = 0$ *dá* $0 + 2y + 1 = 0$*, ou seja: a reta passa pelo ponto* $(0, -1/2)$*. Ademais, a última relação pode ser intrepretada como dizendo que a inclinação, ou declividade, de tal reta é de* $+1$ *por* -2*. Com isso, podemos facilmente desenhar o lugar geométrico* γ*:*



CAPÍTULO 8

APROFUNDANDO O ESTUDO DOS NÚMEROS REAIS

8.1 Por que aprofundar o estudo dos irracionais?

A partir do que já vimos sobre números irracionais, podemos apresentar três caracterizações equivalentes deles:

i). são os números reais que não são racionais;

ii). são os números reais cuja expansão decimal é infinita não-periódica;

iii). são os números reais que expressam a medida de segmentos da reta euclidiana incomensuráveis com um segmento de reta unitário, e mais os simétricos destes números.

Enquanto no Ensino Médio os números naturais, inteiros e racionais são bastante estudados, os irracionais são tratados de forma muito superficial e, muitas vezes, de forma até errônea. Esse precário tratamento consiste, tipicamente, na apresentação das caracterizações i) e ii) mencionadas anteriormente, talvez seguidas de algumas informações adicionais, tais como a de que a diagonal de um quadrado de lado unitário não tem medida racional; a seguir, são citados exemplos bem conhecidos tais como o número π e as raízes quadráticas $\sqrt{2}$, $\sqrt{3}$. E o "estudo" dos irracionais fica essencialmente por aí.

Isso passa ao aluno várias ideias falsas, tais como as de que os irracionais são "anomalias numéricas" sem nenhuma importância teórica e prática. A prática escolar convence o aluno de que os números irracionais são inúteis e que tudo se resume a mais uma definição a ser memorizada.

Na verdade, poucas conclusões poderiam ser mais falsas e lamentáveis do que essas. Vejamos.

– Os irracionais são desimportantes?

- Diferentemente do que acontece com o estudo dos números racionais – que sob o ponto de vista da pesquisa matemática – está essencialmente terminado, há uma intensa atividade dos matemáticos da atualidade buscando descrever e elucidar as propriedades dos vários *tipos* de números irracionais.
- O conhecimento aprofundado dos irracionais é imprescindível em várias disciplinas matemáticas e tem se revelado de grande utilidade em diversos campos aplicados; assim, o estudo dos irracionais é essencial e, sob alguns aspectos, até muito mais importante do que o estudo dos racionais.

– Os irracionais são anomalias numéricas?

A primeira crítica que se pode fazer desse ponto de vista é que, assim como existem infinitos números racionais, também podemos facilmente listar infinitos irracionais, por exemplo: $\sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \ldots$. Mas, há muito mais do que isso: George Cantor, c. 1 870, provocou um imenso choque na comunidade matemática ao mostrar que a infinitude dos irracionais é muito superior a dos racionais. Mais precisamente, ele mostrou que $\mathbb{Q}$ forma um conjunto enumerável[1] enquanto que $\mathbb{I}$ tem uma variedade

[1] Ou seja: há uma correspondência biunívoca entre os números racionais e os números inteiros.

tão grande de números que não pode ser enumerado.

O significado desse "superior" , bem como o conceito de enumerabilidade, são explicados de maneira detalhada e rigorosa em cursos de Teoria dos Conjuntos. Contudo, podemos ter uma ideia intuitiva da diferença "populacional" entre $\mathbb{Q}$ e $\mathbb{I}$ com a seguinte reflexão alternativa, a qual procura comparar o "tamanho" de $\mathbb{Q}$ e $\mathbb{I}$, não por contagem, mas por medida (ou probabilidade).

A partir de um decaedro regular (poliedro regular de dez faces), faça um dado de 10 faces e enumere-as de 0 a 9. A seguir, comece a jogar o dado sobre uma mesa plana e, a cada lance, anote o dígito que aparece na face superior do mesmo, formando assim uma lista de dígitos. Continuando esse procedimento indefinidamente, conseguiremos uma lista infinita da forma $0, a_1 a_2 \ldots$ que representa um número real não negativo do intervalo $[0, 1]$. Observe então que, para que essa lista represente um número racional, é necessário que, a partir de um certo lance, todos os seguintes passem a repetir um certo padrão, de modo a caracterizar uma periodicidade. É bastante intuitivo que essa possibilidade seja extremamente remota, desde que o dado não seja viciado. Com efeito, a Teoria das Probabilidades nos permite mostrar rigorosamente que é nula (ou seja, de 0%), a chance de que venhamos a obter um racional dessa forma, enquanto que temos 100% de probabilidade de, da mesma forma, achar um irracional.

Uma outra maneira de mostrarmos a "pequenez" do conjunto do dos números racionais frente ao tamanho dos irracionais – afirmação esta, na verdade, equivalente à afirmação do parágrafo anterior – consiste em dizer que a chance de sortearmos ao acaso, na reta euclidiana, um ponto racional é de 0, enquanto que a chance de sortearmos um ponto irracional é de 100!

Vemos, portanto que, "se tamanho fosse documento", teríamos muito mais razões para estudarmos os irracionais do que os racionais.

Observação.
É provável que o leitor queira contestar as afirmações anteriores dizendo que, embora a chance de obter um ponto racional seja muito pequena, ela não pode ser zero pois, afinal, eles existem. No entanto, quando trata-se de conjuntos infinitos, possibilidade ou probabilidade zero não é o mesmo que impossibilidade. Assim, de fato, de acordo com a Teoria das Probabilidades, *a chance de sortearmos ao acaso, na reta euclidiana, um ponto racional é zero*; contudo, é perfeitamente possível que isto ocorra !

Exercício 211 -

Embora a equivalência "impossível = probabilidade zero" seja verdadeira em contextos envolvendo conjuntos finitos de possibilidades, acabamos de observar que a mesma é falsa em contextos envolvendo conjuntos infinitos.
Pergunta-se: "possível" é sinônimo de "probabilidade um (ou 100%*)"? Justifique.*

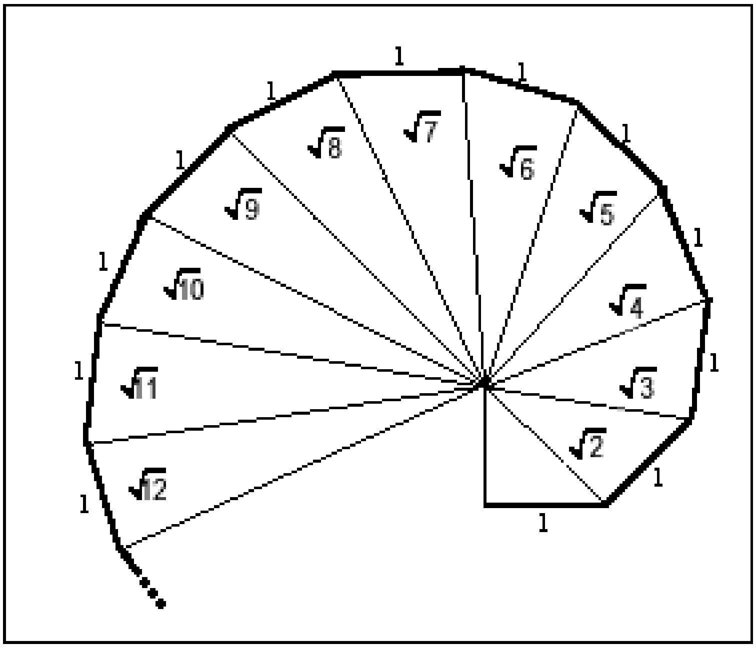
As ideias mencionadas anteriormente, principalmente aquela sobre o tamanho dos racionais comparado com o dos irracionais, foram discutidas de maneira bastante intuitiva. Neste momento, o objetivo principal é procurar ampliar um pouco o foco do leitor relativo à sua visão de números, em especial à de números irracionais, motivando-o assim para o estudo que faremos sobre estes números nas próximas seções.

Existem vários enfoques nos permitindo esclarecer as muitas facetas da noção de irracionalidade. Um aspecto interessante dessas investigações é que a maioria delas consegue rapidamente revelar a complexidade do comportamento dos números irracionais, mostrando tanto seu lado desafiador, como sua fertilidade matemática. É o que tentaremos mostrar nas seções que se seguem.

Antes de realmente iniciarmos este capítulo, propomos os exercícios seguintes, os quais farão com que o leitor trabalhe com a definição e propriedades básicas dos números irracionais. Isso tem tanto o propósito de uma revisão, como o de achar aritmeticamente números irracionais. Com efeito, o primeiro exercício trata da primeira família de irracionais descoberta pelos gregos clássicos, mais precisamente por Theodoros, c. 400 AC.

Exercício 212 (O Caramujo de Theodoros) -

Considere a sequência de triângulos retângulos da figura a seguir, iniciada pelo triângulo retângulo isósceles de lado unitário. Pede-se:



i). Provar que a medida h_n da hipotenusa do n-ésimo triângulo satisfaz

$$h_n^2 = n + 1\,.$$

ii). Mostrar que, dependendo do valor de n, ocorrem tanto valores racionais como irracionais para a medida da hipotenusa h_n.

iii). De acordo com sua intuição, completar a sentença que segue, de modo a torná-la verdadeira. A seguir, demonstre-a.

$$h_n \text{ é racional} \iff n + 1 \ldots .$$

iv). A partir de sua intuição em (iii) responda, justificando:

a). Quantas hipotenusas têm medida racional inteira?
b). Quantas hipotenusas têm medida racional não inteira?
c). Quantas hipotenusas têm medida irracional?

Exercício 213 -

Usando $\in \mathbb{Q}$ *ou* $\in \mathbb{I}$, *complete a tabela a seguir:*

x	y	$x+y$	$x \times y$
$\in \mathbb{Q}$	$\in \mathbb{Q}$		
$\in \mathbb{Q}$	$\in \mathbb{I}$		
$\in \mathbb{I}$	$\in \mathbb{Q}$		
$\in \mathbb{I}$	$\in \mathbb{I}$		

Fazer o mesmo com:

x	$y \neq x$	$x-y$	$x \div y$
$\in \mathbb{Q}$	$\in \mathbb{Q}$		
$\in \mathbb{Q}$	$\in \mathbb{I}$		
$\in \mathbb{I}$	$\in \mathbb{Q}$		
$\in \mathbb{I}$	$\in \mathbb{I}$		

Exercício 214 -

Apresente um par de irracionais x *e* y, *tais que* $x/y \in \mathbb{Q}$.

Exercício 215 -

Apresente um par de irracionais x *e* y, *tais que* $x/y \notin \mathbb{Q}$.

Exercício 216 -

Se $a, b, c \in \mathbb{R}$, *provar que*

i). *se* $a+b=c$ *e* $c \in \mathbb{Q}$, *então não poderemos concluir que* $a, b \in \mathbb{Q}$;

ii). *se* $a+b=c$ *e* $a, c \in \mathbb{Q}$, *então, necessariamente,* $b \in \mathbb{Q}$.

Exercício 217 -

i). *Mostre que se duas grandezas* x *e* y *são incomensuráveis, então cada vez que* x *assumir um valor racional, o correspondente valor de* y *será irracional.*

ii). *V ou F? Justifique. Um círculo tem raio racional se, e só se, sua circunferência for um número irracional.*

Exercício 218 -

Seja d a medida da diagonal do quadrado de lado 1. Sem usar calculadora, determine um racional que aproxime $d + 3,\overline{12}$ *, com um erro menor do que* $1/10^2$ *.*

Exercício 219 -

Para cada valor de x *indicado a seguir, determine (sem usar calculadora) um racional próximo de* x*, com um erro menor do que* $1/10^2$*. A seguir, responda a seguinte questão, justificando sua resposta: é* x *um número irracional?*
i) $x = 2 + \sqrt{2}$. *ii)* $x = \sqrt{2} + \sqrt{3}$.

8.2 Representação aritmética e algébrica dos números reais

Nos concentraremos em dois tipos de representações para os números reais:

– A *aritmética*, a qual consiste na expansão decimal do número ou, eventualmente, em sua expansão em base dois ou outra base mais conveniente.

– A *algébrica*, a qual consiste numa "fórmula" expressando o número real por meio de uma quantidade finita de operações aritméticas e de radiciações envolvendo apenas número inteiros; aqui, por operações aritméticas estamos entendendo as quatro operações básicas: adição, subtração, multiplicação e divisão. Exemplos de fórmulas algébricas para números são $\sqrt{1 + \sqrt{2}}$ e $1/(1 - \sqrt{2})$.

Vale a pena precisarmos melhor o que entendemos por "fórmula algébrica", ou representação algébrica de um número real. Esse conceito terá de ser enunciado recursivamente:

- Nível α_1:
  todos os números inteiros e as radiciações (raiz quadrada, raiz cúbica, raiz quártica, etc.) de inteiros que façam sentido (isto é, de inteiros positivos quando a raiz for de ordem par).
- Nível β_1:
  todas as expressões envolvendo um número finito de operações aritméticas com os números de α_1; por exemplo:

$$3\sqrt{2}\,, \quad 3\sqrt{2} - \sqrt{5}\,, \quad \frac{3\sqrt{2} - \sqrt{5}}{(\sqrt{2})^3}\,, \quad \frac{\sqrt[3]{2}}{1 + \sqrt{5}}\,.$$

- Nível α_2:
  todos os números dados pelas expressões de β_1, bem como suas radiciações que façam sentido (em $\mathbb{R}$).
- Nível β_2:
  todas as expressões envolvendo um número finito de operações aritméticas com os números de α_2; por exemplo:

$$\sqrt{3\sqrt{2}-\sqrt{5}}, \quad 3\sqrt{2}+\frac{3\sqrt{2}-\sqrt{5}}{(\sqrt{2})^3}+\sqrt[4]{\frac{\sqrt[3]{2}}{1+\sqrt{5}}}\,.$$

- Nível α_3:
  todos os números dados pelas expressões de β_2, bem como suas radiciações que façam sentido.
- Nível β_3:
  todas as expressões envolvendo um número finito de operações aritméticas com os números de α_3 .
- Etc.,
  o processo continua indefinidamente com níveis $\alpha_4, \beta_4, \alpha_5, \beta_5, \ldots$.

Exemplo 8.1 -

Os números racionais são representados algebricamente por fórmulas do nível β_1.

Exemplo 8.2 -

Com fórmulas de nível α_1 *podemos obter todos os irracionais do Caramujo de Theodoros, uma vez que todos eles podem ser escritos na forma* $\sqrt{n}$*, onde* n *é um inteiro positivo que não é um quadrado. Mas, também obtemos irracionais ainda mais complicados, desde que tomemos raízes cúbicas, quárticas, etc., de números naturais adequados:* $\sqrt{n}$, $\sqrt[3]{n}$, $\sqrt[4]{n}$, $\sqrt[5]{n}$*, etc.*
Contudo, tenha em vista possibilidades tais como $\sqrt[3]{8}=2$ *(uma raiz cúbica que se reduz a um inteiro) e* $\sqrt[4]{25}=\sqrt{5}$ *(uma raiz quártica que se reduz a uma raiz quadrada).*

As possibilidades levantadas pelo exemplo anterior nos levam a introduzir uma terminologia clássica:

Definição 8.3 -

Sendo r um número racional e $k = 2, 3, \dots$, dizemos que

$$\sqrt[k]{r}$$

é um número surdo *se esta expressão definir um número real irracional.*

Exemplo 8.4 -

Evidentemente, não basta verificarmos se um número real dado está no formato $\sqrt[k]{r}$ para podermos enquadrá-lo entre os surdos. Exemplos são $\sqrt{4} = 2$ e $\sqrt[4]{625} = \sqrt{\sqrt{625}} = \sqrt{25} = 5$.

Exemplo 8.5 -

Todos os irracionais do Caramujo de Theodoros são surdos.
Mas, cuidado, o quociente desses números, embora sempre possa ser escrito no formato da definição:

$$\frac{\sqrt{p}}{\sqrt{q}} = \sqrt{\frac{p}{q}},$$

nem sempre resulta num irracional. Por exemplo:

– quociente não surdo:

$$\frac{\sqrt{8}}{\sqrt{2}} = \sqrt{\frac{8}{2}} = \sqrt{4} = 2\,;$$

– quociente surdo:

$$\frac{\sqrt{2}}{\sqrt{3}} = \frac{\sqrt{2}\sqrt{3}}{3} = \frac{\sqrt{6}}{3} = \sqrt{\frac{6}{9}}\,.$$

Exercício 220 -

Mostrar que são exemplos de surdos:

a). $\sqrt[4]{25}$.
b). $\sqrt{6/9}$.
c). $\sqrt{12} + \sqrt{75}$.

Exercício 221 -

Provar que todos os quocientes $\sqrt{p}/\sqrt{q}$ são surdos, desde que p e q sejam inteiros positivos, e pq não seja um quadrado perfeito.

Cabem aqui duas observações:

– Primeira:
a denominação números surdos é de uso frequente em vários países, principalmente nos de língua inglesa. Contudo, não há consenso sobre o significado exato da mesma. Por exemplo, é comum se chamar de surdo apenas o que chamaríamos de surdos quadráticos, qual seja, os surdos da forma $\sqrt{N}$, onde N é um inteiro positivo que não seja um quadrado.

– Segunda:
é bastante comum se ver pessoas indagando o porquê do nome surdo. Nesse sentido, é certo que a denominação foi originada pela Aritmética de al-Khwarizmi, escrita c. 800 dC. Este, seguindo a tradição indiana e grega, denominava os números racionais de *muntaq* (palavra árabe que significa: audível, capaz de ser ouvido) e os irracionais de *jathr asamm* (significado: raiz surda). Quando a sua Aritmética foi traduzida para o Latim e popularizada no Mundo Cristão por Cremona e Fibonacci, por cerca de 1 200 dC, eles traduziram *assam* por *surdus*, denominação esta que ficou consagrada.

Mas, por que al-Khwarizmi usou a expressão "raiz surda"? Porque seguia a tradição pitagórica que descobriu que se, numa corda de lira, produzirmos vibrações com um comprimento de onda comensurável com o comprimento da corda, o som resultante é musical, enquanto que será não musical se houver incomensurabilidade. Ou seja: a lira é musicalmente audível no caso de comensurabilidade, e inaudível no de incomensurabilidade. Assim, podemos dizer que a visão pitagórica era compatível com chamar os números racionais de audíveis e os irracionais de inaudíveis.

Mas, pelo que vimos, seria de se esperar que al-Khwarizmi tivesse usado a palavra mudo e não surdo para denotar os irracionais. Como explicar a troca de palavras? Simplesmente não houve troca, pois o sentido original da palavra surdo era mudo, incapaz de produzir som, sentido este que ainda usamos em algumas situações: "tambor surdo", "escaparam na surdina", etc.

Os dois exercícios que se seguem introduzem duas famílias muito importantes de números irracionais expressos algebricamente.

Exercício 222 -

Indiquemos por $\left[\mathbb{Q},\sqrt{2}\right]$ o conjunto

$$\left[\mathbb{Q},\sqrt{2}\right] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Assim, pede-se:

i). Mostrar que $\left[\mathbb{Q},\sqrt{2}\right]$ é fechado aritmeticamente*, ou seja, que a soma, diferença, produto e quociente (este último por número não-nulo) de números de $\left[\mathbb{Q},\sqrt{2}\right]$ ainda é um número deste conjunto.*

ii). Mostrar que, se combinarmos $\sqrt{2}$ *com números racionais, de todas as maneiras aritmeticamente possíveis (isto é, usando somente adições, subtrações, multiplicações e divisões por número não-nulo), obteremos exatamente o conjunto* $\left[\mathbb{Q}, \sqrt{2}\right]$.

iii). Mostrar que $\frac{1}{1+\sqrt{2}} \in \left[\mathbb{Q}, \sqrt{2}\right]$. *Generalizando o raciocínio empregado, conclua que* $\left[\mathbb{Q}, \sqrt{2}\right]$ *é um corpo.*

iv). Mostrar que $\sqrt{3} \notin \left[\mathbb{Q}, \sqrt{2}\right]$.

Exercício 223 -

De um modo análogo ao feito anteriormente, definimos o conjunto

$$[\mathbb{Q}, \sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}\}.$$

Pergunta-se:

$$\frac{1}{1+\sqrt{2}+\sqrt{3}} \in [\mathbb{Q}, \sqrt{2}, \sqrt{3}] \ ?$$

O que você pode concluir de sua resposta?

É importante colocarmos que o estudo matemático da representação dos números reais segue, como qualquer outro estudo matemático, duas linhas gerais de ataque: a *computacional*, que trata da obtenção ou cálculo das representações, e a *teórica*, que procura elucidar a natureza e as propriedades dos números reais associados.

Os gregos clássicos eram bastante preconceituosos, e davam aos estudos matemáticos teóricos, que denominavam *Mathematiké*, um status bem superior aos estudos computacionais, que denominavam *Logistiké*. Esse preconceito ainda é comum de ser encontrado, mas não é mais justificável, uma vez que ambos os enfoques são importantes e atingem níveis comparáveis de sofisticação técnica. Na verdade, nos tempos atuais, praticamente todos os campos matemáticos são estudados tanto por meio do enfoque computacional, como do teórico.

Outro equívoco a ser corrigido é o de que os estudos computacionais resumem-se a cálculos numéricos. Essa é uma visão bastante obsoleta, pois já com François Viète, por volta de 1600, a Logística havia sido dividida em *Logistica Numerosa* (Cálculo Numérico) e *Logistica Speciosa* (Cálculo Literal ou Algébrico).

Voltando a tratar exclusivamente do que nos compete – qual seja, dos números reais –, iniciemos esclarecendo um possível mal entendido. Sempre que estivermos trabalhando com um número que é sabidamente real, poderemos garantir – pela própria definição de número real – que o mesmo tem uma expansão decimal $a_0, a_1 a_2 \ldots a_n \ldots$. Contudo, *essa garantia não equivale ao conhecimento de tal expansão.* Com efeito:

> *na grande maioria dos casos, o contato inicial com um número real não se dará diretamente com sua expansão decimal, e sim por meio de alguma propriedade que o caracterize, e a partir da qual não é imediato obtermos a expansão decimal desse número.*

Exemplos típicos são: "seja π o número que é a razão entre a circunferência e o diâmetro de cada círculo" e "seja x a raiz positiva da equação $x^3 + 2x^2 + 10x = 20$".

– Dificuldades na obtenção de expansões decimais de números reais

Essas dificuldades ocorrem tanto com números irracionais, como com números racionais. Vejamos um exemplo: sabe-se que toda equação polinomial de coeficientes reais e grau ímpar tem ao menos uma raiz real; assim, podemos afirmar, com certeza que existe um número real x_0 que é raiz da equação polinomial:

$$x^{1+100!^{100!^{100!}}} - x^4 - x^2 - 1 = 0\,. \tag{8.1}$$

No entanto, é muito difícil, e provavelmente impossível, de se descobrir qual a expansão decimal completa de tal x_0.

Para não deixarmos a impressão de que não podemos descobrir nada sobre tal x_0, propomos o exercício que segue.

Exercício 224 -

i). *Mostre que todas as raízes (reais) da equação (8.1) são números irracionais.*
Dica: mostre que ela não tem nenhuma raiz racional.

ii). *Mostre que todas as raízes (reais) da equação (8.1) são positivas.*
Dica: examine os graus dos termos da equação.

iii). *Mostre que tal equação tem uma raiz real, x_0, entre 1 e 2, ou seja: $1 < x_0 < 2$.*
(Neste item você precisará supor conhecido o seguinte fato, que é uma decorrência da Propriedade do Contínuo:
Se uma expressão polinomial assumir valores a e b, então assumirá também qualquer valor entre a e b.)

iv). Determine os dois primeiros algarismos da expansão decimal de tal x_0. Mais precisamente, prove que $x_0 = 1,0\ldots$.

Assim, pode ocorrer, e isso é o mais comum, que tenhamos de tratar com números reais para os quais, num momento inicial, estaremos na situação bastante desfavorável de ainda não conhecemos todos ou mesmo nenhum dos algarismos de sua expansão decimal.

Mais do que isso: mesmo nos casos favoráveis – aqueles para os quais já descobrimos, ou nos foi dada, uma regra ou procedimento que permita escrever os dígitos a_n da expansão do número – a nossa impotência poderá ser bastante grande. Com efeito, não é suficiente termos uma tal regra: é crucial que a mesma seja *eficiente* e *leve em conta as delimitações dos recursos computacionais disponíveis*. Examinemos essas duas qualidades brevemente.

– A necessidade de procedimentos eficientes

É bastante fácil de ser aceita. Por exemplo, existem problemas matemáticos teóricos que exigem o conhecimento de muitos algarismos – milhões e milhões deles – da expansão decimal de certos números irracionais, como é o caso do número π, a razão entre a circunferência e o diâmetro de círculos. Um exemplo desses problemas é o estudo da “normalidade” de π, assunto que abordaremos na próxima seção.

O primeiro método inventado para achar a expansão de π, o clássico método de Archimedes, é excessivamente lento para o cálculo de uma quantidade grande de algarismos, e o mesmo ocorre com praticamente todos os muitos outros métodos de cálculo deste número que foram inventados nos últimos séculos. Assim, um dos mais famosos recordes computacionais de todos os tempos foi estabelecido por William Shanks, em 1874, quando – depois de penosos 15 anos de cálculos – obteve os 707 primeiros dígitos de π.[2]

A questão da ineficiência dos métodos de cálculo de π só começou a ser resolvida com um procedimento descoberto em 1984 pelos irmãos Borwein. Só para o leitor poder avaliar o aumento da eficiência: com meras 56 operações aritméticas, que levaram poucos segundos para serem executadas num computador, eles puderam obter a mesma aproximação que tinha consumido 15 anos da vida de Shanks. O método dos Borwein continua sendo melhorado, e hoje é um dos usados no estudo da “normalidade” de π.

[2]Para o leitor arguto que poderia estar achando que a grande causa desse gasto de tempo tenha sido a inexistência de computadores eletrônicos na época de Shanks, adiantamos que esse recorde só foi quebrado em 1947, quando D. Ferguson conseguiu atingir 808 dígitos.

Ainda insistindo na importância da eficiência computacional, vale observar que é comum que tenhamos uma regra que teoricamente é capaz de nos dar a expansão decimal de um número desejado, mas que na hora de ser efetivamente calculada se revele extremamente ineficiente, porque gera os sucessivos algarismos da expansão cada vez mais lentamente. Vejamos um exemplo concreto, usando uma clássica expressão de π (a rigor, de seu quadrado dividido por 6) como soma limite de uma série numérica de termos bem simples:

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6}\,. \tag{8.2}$$

(Em Leitura Complementar, no capítulo anterior, já desenvolvemos brevemente a noção de série numérica e sua soma limite, em um texto suficientemente detalhado para se entender o que faremos a seguir.)
Usando-se técnicas do Cálculo Infinitesimal prova-se que, procedendo-se ao cálculo gradativo das somas parciais dessa série, a cada decuplicação da quantidade de parcelas somadas ganha-se mais uma casa decimal exata na aproximação de π. Como é fácil de se ver, o esforço computacional envolvido na obtenção da correspondente soma limite dessa série torna-se proibitivo, se quisermos um resultado com um mínimo de exatidão. Com efeito, a soma das 10 primeiras parcelas de (8.2) vale:

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} + \frac{1}{8^2} + \frac{1}{9^2} + \frac{1}{10^2} = 1,5497\ldots\,,$$

e como se sabe – por exemplo, usando o método dos Borwein – que

$$\pi^2/6 = 1,6449340668482264364724151666460251892189499012 06\ldots\,,$$

conclui-se que a soma das 10 primeiras parcelas está sendo capaz de nos fornecer uma aproximação de $\pi^2/6$, com apenas um algarismo exato. Sabendo-se isso, e usando a informação sobre decuplicação dada anteriormente, concluímos que precisamos somar as 100, 1.000, 10.000,..., 10.000.000.000 primeiras parcelas de (8.2) para calcularmos uma aproximação de $\pi^2/6$ com, respectivamente, 2, 3, 4,..., 10 algarismos exatos.

– As delimitações dos recursos computacionais existentes

Muito frequentemente não podemos nos limitar ao uso de "lápis e papel" para achar a expansão de um número real; exigências de tempo nos obrigam a usar algum tipo de calculadora ou computador. Esses, sendo objetos concretos, só podem tratar de expansões decimais finitas, o que pode provocar enormes alterações conceituais e numéricas no problema que estamos resolvendo. Exemplifiquemos. Enquanto, teoricamente falando, a equação $1 + x = 1$ tem como solução real apenas $x = 0$, a mesma equação admite muitos números reais como solução sob o ponto de vista de uma calculadora eletrônica. Com efeito, em calculadoras eletrônicas vale $1+x=1$ para, tipicamente, qualquer $0<x<10^{-20}$. Se numa equação tão simples assim já ocorrem surpresas, é de se ficar imaginando o que pode ocorrer na resolução de equações, ou outros problemas, muito mais complicados!

Exercício 225 -

Em qualquer calculadora, computador ou linguagem de programação, é de enorme importância conhecermos o número u, o qual é o maior número real x, representável pela máquina ou linguagem, e tal que $1+x=1$. Pede-se que V. tome uma calculadora e determine o valor do respectivo u, ao menos, aproximadamente.

Exercício 226 -

Considere a seguinte sequência:

$$\begin{aligned} a_0 &= \frac{1}{3}, \\ a_n &= 4a_{n-1} - 1 \ (n \geq 1). \end{aligned}$$

i). Prove algébricamente que $a_n = 1/3$, para todo $n \geq 0$.
ii). Usando uma calculadora, obtenha o valor numérico de $a_1, a_2, \dots, a_{20}$.
iii). Explique por que os valores de a_{20}, segundo (i) e (ii), são diferentes.

Também é importante salientar que existem muitas questões sobre a expansão dos números reais que têm um carácter *transcomputacional*, isto é, questões que não podem ser resolvidas com a ajuda de computadores e calculadoras. Aqui seguem alguns exemplos delas:

Exercício 227 -

Responda V ou F, justificando sua resposta.

a). Atualmente, existem calculadoras superpotentes que nos possibilitam operar (ou seja: somar, multiplicar, etc.) com qualquer número real, obtendo um resultado exato.
b). A afirmação anterior é falsa. No entanto, podemos assegurar que existem calculadoras que nos permitem operar com qualquer número racional, obtendo sempre um resultado exato.

c). A afirmação anterior é falsa. No entanto, podemos assegurar que existem calculadoras que nos permitem operar com qualquer número natural, obtendo sempre um resultado exato.

d). A afirmação anterior é falsa. No entanto, qualquer calculadora permite que operemos exatamente, desde que trabalhemos apenas *com um número finito de números, os quais, além disto, necessariamente têm que ser racionais.*

e). Todas as afirmações anteriores são falsas, já que uma calculadora nem sempre consegue operar exatamente, pois somente trabalha com um número finito de dígitos.

Exercício 228 -

Numa classe de 8ª série do Ensino Fundamental, foi perguntado se $\sqrt{6}$ era um número irracional, ou não. As respostas dos alunos foram de três tipos:

Resposta 1:
pela calculadora, vemos que $\sqrt{6}$ é irracional, pois não se percebe ocorrência de período.

Resposta 2:
no visor de nossas calculadoras sempre vemos números racionais, já que eles aparecem como um número com vírgula e com uma quantidade finita de dígitos depois da vírgula. Assim, fica impossível verificarmos – usando uma calculadora – se $\sqrt{6}$ é irracional ou não.

Resposta 3:
as calculadoras que temos não são "potentes" o suficiente para descobrir se $\sqrt{6}$ é, de fato, um número irracional.

Posto isso, pede-se que o leitor faça uma análise crítica das três respostas dadas.

Outra questão simples de formular: é possível que os dígitos da expansão decimal de $\sqrt{2}$ sejam todos diferentes de 4, a partir de uma certa casa decimal? Pergunta semelhante trocando $\sqrt{2}$ por $\sqrt{5}$, ou por π, ou mesmo trocando 4 por qualquer outro dígito. Questões como essas não podem ser resolvidas com máquinas. É preciso uma abordagem teórica!

Por outro lado, nunca é demais enfatizar que, embora possamos ter um supreendente desconhecimento até de propriedades simples da expansão decimal dos números reais em geral, não podemos de maneira alguma concluir que isso vá sempre ocorrer com qualquer número real, mesmo que ele seja irracional! Uma pequena amostra do que dissemos pode ser vista no exercício que se segue.

Exercício 229 -

Considerando o número irracional

$$0, a_1 a_2 \ldots a_n \ldots = 0,101001000100001000001 \ldots ,$$

pede-se uma fórmula dando o valor do algarismo a_n *para qualquer valor de* n *.*

As observações feitas acima apontam para a necessidade de todo um preparo especializado, se quisermos estudar os aspectos computacionais associados às expansões decimais dos números reais. Por isso, encerramos esse estudo aqui e passaremos para o estudo teórico do grau de complexidade dessas expansões.

8.3 Complexidade da expansão decimal dos irracionais

Já foi muito insistido que os *números racionais* podem ser caracterizados como os números reais cuja expansão decimal é finita, ou infinita periódica; enquanto que os *números irracionais* têm expansão infinita não periódica. Contudo, poderíamos dizer que essa caracterização esclarece tudo sobre os racionais, e muito pouco sobre os irracionais. Com efeito, ela não esclarece o quão complexa pode ser a irregularidade (ou não periodicidade) da distribuição dos algarismos da expansão decimal de um número irracional. O propósito desta seção é procurar sanar essa deficiência.

A mais antiga tentativa de se entender a diferença no grau de complexidade da expansão dos racionais, comparada com a dos irracionais, foi a introdução do conceito de "normalidade", por Émile Borel, no início do século XX:

Definição 8.6 -

Um número irracional é dito normal *se sua expansão decimal apresentar todos os dez algarismos, e se todos os blocos (listas ordenadas) de* N *algarimos ocorrreem com probabilidade* $1/10^N$*, para* $N = 1, 2, 3, \ldots$ *. Ou seja: cada algarismo aparece com probabilidade* $1/10$ *; cada par ordenado de algarismos aparece com probabilidade* $1/100$ *; cada trinca ordenada de algarismos aparece com probabilidade* $1/1000$ *; etc.*

Enfatizamos que para que um número seja normal é necessário que em sua expansão decimal apareçam todos os algarismos, bem como todos os possíveis blocos (finitos) de algarismos, e isto com uma probabilidade que depende apenas do tamanho do bloco.

Isso nos permite a seguinte interpretação intuitiva da normalidade. Suponha que fizemos um dicionário associando a cada letra do alfabeto um dígito, e, a cada palavra, o correspondente bloco de dígitos. Então, se o número π for normal, a heroína do livro e filme *Contato,* do astrônomo Carl Sagan, teria sucesso em sua tarefa de achar um segredo cósmico entre os dígitos de π; qualquer pessoa, desde que vasculhe uma quantidade suficientemente grande dos dígitos de π, seria capaz de ler o Sermão da Montanha na expansão decimal deste número, bem como todos os palavrões tupiniquins e as palavras que Santa Genoveva murmurou nos ouvidos de Átila, o Huno, fazendo com que ele desistisse de conquistar Paris!

– Como calcular tal probabilidade de ocorrência?

Uma vez que expansão decimal de todo irracional envolve infinitos dígitos, a probabilidade de ocorrência de um dado dígito é obtida por meio do comportamento limite da frequência média de ocorrência deste dígito. Mostremos isso por meio de um exemplo.

> Dado um irracional $m, a_1a_2\ldots$, suponha que queiramos saber, por exemplo, a probabilidade de ocorrência do dígito 4 nesta expansão. Para isso, dado n, contamos o número de $4's$ que aparecem na lista $a_1 \ldots a_n$ e denotamos tal número por $N_4(n)$. Temos então que a frequência média com que o 4 aparece nos n primeiros dígitos é de $N_4(n)/n$.
>
> Resta, assim, determinar o que acontece com o quociente $N_4(n)/n$ à medida que n crescer indefinidamente. Se $m, a_1a_2\ldots$ for normal, então esse quociente deve se aproximar de $1/10$ à medida que n vai aumentando.

Da mesma forma, a normalidade implica que, por exemplo, $N_7(n)/n$ deva se aproximar de $1/10$, onde $N_7(n)$ é o número de $7's$ que aparecem em $a_1a_2\ldots a_n$. Na verdade, ser normal significa muito mais do que isso: além de testarmos todos os possíveis blocos de um algarismo, também temos de testar todos os blocos com dois ou mais algarismos. Por exemplo, dado n, seja $N_{634}(n)$ o número de ocorrências do agrupamento 634 em $a_1\ldots a_n$. Então, $N_{634}(n)/n$ deve se aproximar de $1/1000$ à medida que n for se tornando arbitrariamente grande.

– Por que os racionais foram deixados de fora?

Primeiro, pois um número racional pode ter mais de uma expansão decimal. Segundo, porque nos racionais com duas expansões, na expansão 0-terminante o dígito 0 ocorre com probabilidade $1 \neq 1/10$, e o mesmo ocorre com o dígito 9 na expansão 9-terminante. Terceiro, para os demais racionais também é impossível atribuir normalidade, pois tomando como bloco de dígitos o período do número, temos que a probabilidade de ocorrência deste bloco é 1.

Em particular, o terceiro argumento acima mostra que, para declararmos que um número é normal, *não basta examinarmos a uniformidade da distribuição de seus dígitos.* Também precisamos examinar a uniformidade da distribuição dos blocos de dígitos.

– É possível decidir a normalidade?

Sim, mais isso tende a ser muito difícil.

Exemplo 8.7 -

Um caso de decisão negativa *fácil é o dos números irracionais cuja expansão decimal não contenha todos os algarismos: da definição, segue imediatamente que eles nunca são normais. Um exemplo muito importante desse tipo de irracionais não normais é:*

$$0,\,1010010001000001000000001\ldots\,.$$

Exemplo 8.8 -

Não se conhece nenhum caso de decisão positiva fácil. *O primeiro exemplo de número normal foi dado somente por Waclaw Sierpinski, em 1 917. Esse, como a grande maioria dos exemplos hoje conhecidos de números normais, tem uma complexa construção artificial. Outros exemplos importantes, mas fáceis de exibir são:*

• *a constante de Champernowne (1933):* $0,\,1234567891011121314151617\ldots$ *, que é obtida concatenando todos os números naturais*
(este foi o primeiro exemplo simples de número normal a ser descoberto; o feito ocorreu quando Champernowne ainda era aluno do curso de Matemática da Universidade de Cambridge (veja [Ch] e [Me])); [3]*,*

• *a constante de Copeland-Erdös (1 945):* $0,2357111317192329313741\ldots$ *, que é obtida concatenando todos os números primos.*

Complementando o exemplo anterior, é de se observar que ainda não se conseguiu decidir a normalidade de nenhum número irracional que tenha uma ocorrência natural em problemas de Matemática, como é o caso π, $\sqrt{2}$, $\log 2$. Temos, contudo, grande

[3]O leitor entusiasmado por desafios é convidado a mostrar que a frequência dos blocos de um dígito na Constante de Champernowne é, de fato, 1/10.

evidência empírica que tais números são, de fato, normais. Por exemplo, inúmeros estudos experimentais têm sido feitos sobre os primeiros bilhões de algarismos de π. As tabelas a seguir mostram a frequência com que ocorre cada um dos dez algarismos decimais entre os 100 000 e os 1 000 000 primeiros dígitos, respectivamente, da representação decimal do número π:

ALGARISMO	OCORRÊNCIA entre os 100 000 primeiros dígitos de π
0	9 999
1	10 137
2	9 908
3	10 025
4	9 971
5	10 026
6	10 029
7	10 025
8	9 978
9	9 902

ALGARISMO	OCORRÊNCIA entre os 1 000 000 primeiros dígitos de π
0	99 959
1	99 758
2	100 026
3	100 229
4	100 230
5	100 359
6	99 549
7	99 800
8	99 985
9	100 106

Resultados análogos também foram obtidos para a ocorrência de pares de algarismos (como 00, 01, 02, ..., 11, 12, 13, ... ,222, 23, ...), bem como para trincas, quadras, etc.

Como evidência experimental simples dessas possibilidades, pode-se dizer que se sabe que, lá pela 300 000 000ª casa decimal de π, já terá ocorrido o bloco 6 666 666 666, e que, lá pela 500 000 000ª casa decimal, terá ocorrido o bloco 123 456 789. Por outro lado, rigorosamente falando, não se sabe se, a partir de uma certa casa decimal de π, nunca mais ocorrerá o algarismo 7, ou qualquer outro algarismo dado.

Gregory Chudnovsky, um grande matemático de nosso tempo, está há vários anos, junto com seu irmão, estudando a normalidade de π, e está convencido que ele é normal.

Exercício 230 -

Se for confirmada a conjectura de que π e $\sqrt{2}$ são números normais, poderemos afirmar que, em cada um destes números, existe uma casa decimal a partir da qual nunca mais aparecerá o dígito 5 ? Justifique-se.

Exercício 231 -

Dê infinitos exemplos de números irracionais não normais.

Exercício 232 -

V ou F? Justifique. "Existe um irracional cuja expansão decimal envolve apenas 3 vezes o dígito 2." Em caso afirmativo, responda: é esse número normal?

Exercício 233 -

V ou F? Justifique. Ainda não sabemos se $\sqrt{2} = 1,\, b_1 b_2 b_3 \ldots$ é normal, mas podemos afirmar que o número $1,\, 9b_1 9b_2 9b_3 \ldots$ não é normal.

Exercício 234 -

Dizemos que um número real, racional ou irracional, é simplesmente normal *se cada um dos dez algarismos aparece com probabilidade $1/10$ em sua expansão decimal. Pede-se:*

- *i). Exibir um número real, racional que seja simplesmente normal.*
- *ii). Exibir um número racional que não seja simplesmente normal.*
- *iii). Obviamente, todo número irracional normal é simplesmente normal. Vale a recíproca?*

Exercício 235 -

Discuta a veracidade, ou falsidade, de cada uma das frases que seguem.

i). Ainda não se sabe se a expansão decimal de π pode ser

$$3,14159\ldots 01010101\ldots .$$

ii). Ainda não se sabe se a expansão decimal de π pode ser

$$3,14159\ldots 01001000100001\ldots .$$

– Quão comuns são os irracionais normais?

As três maneiras tradicionais de medirmos o "tamanho" do conjunto dos números normais, bem como o dos não normais, são: achando a medida desses conjuntos, achando a probabilidade de sortearmos tais números, e determinando seu grau de enumerabilidade.

– *O conjunto dos números não normais tem medida zero.*
A noção de "medida zero" é sofisticada demais para o nível deste texto, sendo estudada mais adequadamente em cursos de Análise Matemática. Nos limitaremos a comentar que, muito intuitivamente falando, ela se aplica a conjuntos, talvez muito complicados, que são tão pequenos que têm "comprimento" nulo.

Os exemplos mais simples de conjuntos de medida zero são os conjuntos finitos e os conjuntos infinitos enumeráveis, como é o caso dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$. Contudo, existem conjuntos não enumeráveis que, apesar disso, têm medida zero. Com efeito, Émile Borel mostrou que isso é precisamente o que ocorre com os números não normais.

– *O conjunto dos números normais do intervalo* $[0,1]$ *tem medida um.*
Ou seja, retirando desse intervalo todos os números não normais (inclusive os racionais), não ocorre mudança da medida: continuamos tendo um conjunto de medida um, pois o que foi retirado tem medida zero.

> Em termos de probabilidades, os resultados anteriores podem ser interpretados como dizendo que, se sortearmos ao acaso um número real do intervalo $[0,1]$, teremos que a probabilidade deste número
> – ser normal é um;
> – não ser normal é zero.

– *O conjunto dos números normais é infinito.*
Com efeito, é fácil vermos que as seguinte infinitas variantes da constante de Champernowne) são todas números normais:

$$0,223456789101112\ldots\ ;\ 0,3123456789101112\ldots\ ;\ 0,423456789101112\ldots\ ,\text{etc.}$$

– *O conjunto dos números não normais também é infinito.*
A resposta trivial seria: basta pegar infinitos números racionais. Mas, o realmente significativo é mostrar que existem infinitos irracionais que não são normais. Para isso, observe que é fácil vermos que existem infinitos números irracionais que não têm o dígito 2 (exercício!), e obviamente eles não são normais.

– *O conjunto dos números normais não é enumerável.*
A maneira mais simples de se provar usa a Teoria da Medida. Com efeito, se fosse enumerável, teria medida zero, e isto já vimos que não é o caso.

– *O conjunto dos números não normais não é enumerável.*
Com efeito, isto decorre do fato que pode-se provar que o conjunto dos irracionais que não têm o dígito 2 não pode ser enumerado. Trata-se de um fato notável, uma vez que, apesar disso, esse conjunto tem medida zero.

– Normalidade X aleatoriedade.

Uma ideia relacionada à noção de normalidade é a de "aleatoriedade". Sabendo-se que um dado número é normal, é de se imaginar que os dígitos que aparecem em sua expansão decimal devam ocorrer de forma aleatória, uma vez que a suposição contrária nos levaria a entender a existência de um padrão na expansão decimal deste número, o que não é, aparentemente, nem um pouco coerente com sua normalidade.

Contudo, esse raciocínio não está correto. Com efeito, a constante de Champernowne

$$0,1234567891011121314151617181920\ldots\ ,$$

é obtida por meio de um processo bem determinista: concatenando-se a sequência de todos os números naturais.

Consequentemente, embora não tenhamos definido aqui o conceito de aleatoriedade da expansão decimal de um número real, é de se esperar, pelo menos intuitivamente, que o máximo que podemos dizer é que a normalidade é uma condição necessária, mas não suficiente, para a "aleatoriedade".

Apesar disso, é opinião generalizada que devam existir estreitas ligações entre a aleatoriedade e a normalidade. Nesse sentido, um grande avanço ocorreu em 2001, quando David Bailey e Richard Crandall reduziram a prova da normalidade de π à prova de resultados da Teoria dos Sistemas Dinâmicos Caóticos.

Outra área em que a normalidade pode desempenhar um papel fundamental é na construção de algoritmos *geradores de números aleatórios*, o que tem importância decisiva na simulação computacional do comportamento dos sistemas dinâmicos.

O tema da aleatoriedade dos números tem fascinado gerações de matemáticos, mas tem se mostrado pouco "cooperativo". Além disso, Andrei Kolmogorov, uma das maiores inteligências matemáticas do século XX, achava que nenhuma das constantes clássicas da Matemática (como π, $\sqrt{2}$ e $\log 2$) sejam números "aleatórios", pois conhecemos maneiras recursivas de calcular quantos dígitos quisermos de cada uma delas.

– Normalidade em outras bases.

Uma crítica ao conceito de número normal é que, na verdade, se definiu a normalidade da *expansão decimal* do número. Em outras palavras, em princípio, poderia ocorrer de um número ser normal em base 10 e não ser normal em base dois, ou outra base. O próprio Borel percebeu isso e contra-atacou da seguinte maneira:

Definição 8.9 -

Sendo $B \geqslant 2$ uma base de sistema de numeração posicional, dizemos que um número irracional é B-normal *se em sua expansão base B todos os blocos (listas ordenadas) de N algarimos ocorrerem com probabilidade $1/B^N$, para $N = 1, 2, 3, \dots$.*

Definição 8.10 -

Um número irracional é denominado número absolutamente normal *quando ele for B-normal em todas as bases de representação posicional $(B = 2, 3, 4, \dots, 10, \dots)$.*

Exemplo 8.11 -

O primeiro exemplo de número absolutamente normal foi o construído por Waclaw Sierpinski, em 1917.

Exemplo 8.12 -

Se indicarmos por Champ(B) o número que se obtém concatenando em base B os números primos, temos que Champ(B) é B-normal. Confira a prova em [Me]. Contudo, ainda não se sabe se a Constante de Champernowne –ou seja, Champ(10)– é B-normal em todas as bases B.
(O grande matemático Alan Turing foi quem motivou Champernowne a dedicar-se aos números normais. Turing o chamava afetuosamente de Champ.)

8.4 Irracionalidades quadráticas

A mais conhecida família de números irracionais é a dos números do Caramujo de Theodoros, ou seja: os números reais do tipo $\sqrt{n}$, onde n não é um quadrado perfeito (veja Exercício 212). Nesta seção, introduziremos uma família ainda maior de irracionais: as chamadas *irracionalidades quadráticas*.

Definição 8.13 -

Por irracionalidade quadrática entende-se todo número irracional que seja raiz de alguma equação quadrática (isto é, do segundo grau) cujos coeficientes sejam números inteiros.

Exemplo 8.14 -

Sendo n um inteiro positivo que não é uma quadrado de inteiro, temos que $x = \sqrt{n}$ é uma solução irracional da equação quadrática $x^2 - n = 0$. Ou seja: todos os números do Caramujo de Theodoros são irracionalidades quadráticas.

O exercício a seguir chama a atenção do leitor para a importância do campo onde estão os coeficientes da equação polinomial. Se tratarmos de equações quadráticas de coeficientes não racionais poderemos ter, ou não, soluções que sejam irracionalidades quadráticas. Mais precisamente:

Exercício 236 -

i). Mostre que todo número irracional que é raiz de alguma equação quadrática de coeficientes racionais, tem de ser uma irracionalidade quadrática.

ii). Mostre que nem todo número irracional que é raiz de alguma equação quadrática de s coeficientes irracionais tem de ser irracionalidade quadrática.

Os resultados a seguir caracterizam de modo completo e simples o universo das irracionalidades quadráticas:

Teorema 8.15 -

Seja uma equação do segundo grau, $ax^2+bx+c=0$, onde todos os coeficientes são números inteiros. Então, as raízes dessa equação são irracionalidades quadráticas quando, e só quando, b^2-4ac for um número positivo que não seja quadrado perfeito.

Prova:

As raízes da equação dada são convenientemente obtidas pela fórmula de Bhaskara:

$$x_1=\frac{-b+\sqrt{b^2-4ac}}{2a}, \quad x_2=\frac{-b-\sqrt{b^2-4ac}}{2a},$$

e serão números reais $\iff b^2-4ac \geq 0$. Ora, como estamos supondo que os coeficientes são inteiros, vê-se facilmente que:

– as raízes serão racionais quando b^2-4ac for um quadrado perfeito;
– as raízes serão irracionais quando b^2-4ac for positivo, mas não for um quadrado perfeito.

CQD.

A partir do último resultado, é imediato deduzirmos o seguinte:

Teorema 8.16 -

As irracionalidades quadráticas são os números que têm ou a forma

$$\frac{m+\sqrt{p}}{n},$$

ou

$$\frac{m-\sqrt{p}}{n},$$

onde m e n são inteiros quaisquer, com $n\neq 0$, e p um inteiro positivo que não é um quadrado perfeito.

Prova:

De fato, basta seguir a demonstração do teorema anterior, e definir $p = b^2 - 4ac$.

Reciprocamente: dado $\alpha = (m \pm \sqrt{p})/n$, temos que α é raiz da equação

$$n^2x^2 - 2mnx + m^2 - p = 0\ .$$

CQD.

Exercício 237 -

Prove a última afirmação da demonstração anterior.

Exercício 238 -

Prove que todas as equações da forma

$$x^2 - nx - 1 = 0\,,$$

onde $n \geqslant 1$ e é inteiro, produzem irracionalidades quadráticas.

Exemplo 8.17 *(números metálicos)* -

Além dos números que aparecem no Caramujo de Theodoros (veja Exercício 212), uma outra muito conhecida família de irracionalidades quadráticas é a dos números metálicos*, os quais são as raízes positivas das equações da forma:*

$$x^2 - nx - 1 = 0\,,$$

onde $n \geqslant 1$ e é um inteiro positivo (confira sua irracionalidade no Exercício 238). Dada sua importância, vejamos os principais casos particulares.

- *Para $n = 1$, temos o* número de ouro *.*
  Neste caso, a equação fica $x^2 - x - 1 = 0$, a qual tem apenas uma raiz positiva, a saber,

  $$\phi = \frac{1 + \sqrt{5}}{2}\,.$$

  A letra grega ϕ é usada internacionalmente para indicar o número de ouro.

– *Para $n = 2$, temos o* *número de prata.*
Neste caso, a equação fica: $x^2 - 2x - 1 = 0$, *a qual tem apenas uma raiz positiva, a saber:*

$$\frac{4 + \sqrt{8}}{2} = 1 + \sqrt{2}\,.$$

– *Para $n = 3$, temos o* *número de bronze.*
Neste caso, a equação fica: $x^2 - 3x - 1 = 0$, *a qual tem apenas uma raiz positiva, a saber,*

$$\frac{3 + \sqrt{13}}{2}\,.$$

Ao contrário do número de ouro, não há um símbolo padrão para os números de prata e bronze.

Dos número metálicos, principalmente para o número de ouro, se conhece uma imensa quantidade de propriedades, algumas das quais apresentaremos como exercício, a seguir. Essas propriedades são bastante utilizadas nas artes humanas –como, por exemplo, arquitetura e pintura– e frequentemente encontradas no estudo de fenômenos naturais.

Exercício 239 *(importante)* -

Mostre que o número de ouro é o único número real positivo verificando a seguinte equação:

$$x = 1 + \frac{1}{x}\,.$$

Exercício 240 -

A mais clássica ocorrência do número de ouro, ϕ, é na chamada divisão áurea *de um segmento de reta qualquer. Indicando por ℓ o comprimento desse segmento, fazer sua divisão áurea – ou dividí-lo em* média e extrema razão *– consiste em dividí-lo em duas partes de comprimentos x e y, com $y < x$, tais que valha a seguinte relação de proporcionalidade:*

$$\ell : x = x : y\,.$$

Ou seja: "o todo está para a maior parte, assim como esta maior parte está para a menor parte".

Pede-se mostrar que

$$\frac{x}{y} = \phi,$$

e disto concluir que

$$x = \frac{\ell}{\phi}\,,\; y = \frac{\ell}{1+\phi}\,.$$

Exercício 241 -

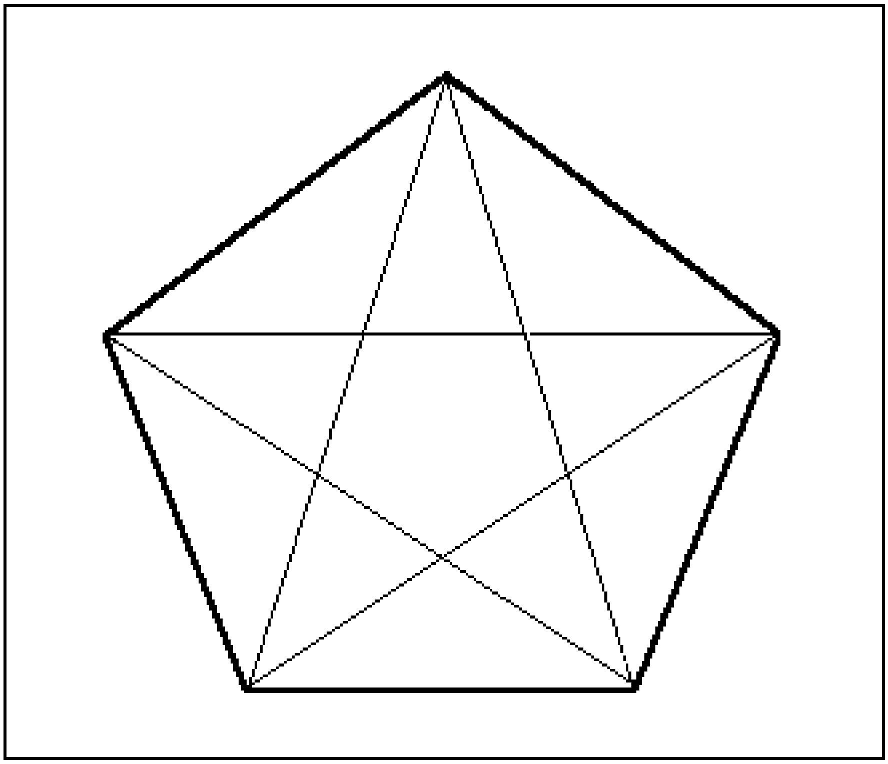
Mostrar que na sequência das potências de ϕ:

$$1, \phi, \phi^2, \phi^3, \dots\,,$$

cada termo, a partir do terceiro, é a soma dos dois anteriores.
(*Sequências numéricas com esta propriedade são chamadas* sequências de Fibonacci.)

Exercício 242 -

Acredita-se que a descoberta do número de ouro foi feita pelos pitagóricos, por volta de 500 AC, quando investigavam as propriedades do pentágono. Ficaram tão maravilhados pela beleza e riqueza das propriedades dessa figura que acabaram adotando o pentagrama *– figura baseada no pentágono e mostrada a seguir – como símbolo esotérico de sua escola.*
Pede-se mostrar que a razão entre a diagonal e o lado do pentágono regular é o número de ouro.



Exercício 243 -

Dada uma equação $x^2 + bx + c = 0$ *, onde os coeficientes* b *e* c *são números inteiros, mostre que suas raízes reais são ou números inteiros. ou números irracionais.*

Exercício 244 -

i). A soma de duas irracionalidades quadráticas é ainda uma irracionalidade quadrática?

ii). Se r *for uma irracionalidade quadrática, é verdade que* $1/r$ *também o será?*

Exercício 245 -

Descreva os números que, simultaneamente, sejam surdos e irracionalidades quadráticas.

8.5 Irracionalidades cúbicas

Os matemáticos gregos conheciam apenas as irracionalidades quadráticas. Somente por volta de 1200 dC é que Fibonacci mostrou que essa visão era incompleta. Assim sendo, nosso próximo passo será examinar o que Fibonacci fez.

Em seu livro de álgebra, denominado *Flos*, Fibonacci conta que um tal de Magister Johannes lhe desafiou a encontrar "um cubo que, com dois quadrados e dez coisas, valesse 20". Ou seja, lhe desafiou a resolver a cúbica, que chamaremos de cúbica de Fibonacci:

$$x^3 + 2x^2 + 10x = 20\,. \tag{8.3}$$

É fácil mostrarmos que essa equação tem apenas uma raiz real e que ela é positiva. Ou seja, como diziam os antigos, ela tem uma única "raiz verdadeira", uma raiz que pode ser interpretada como a medida de algum segmento de reta.

Exercício 246 -

i). Prove que a equação (8.3) tem uma raiz real positiva, e que ela está no intervalo $[1, 2]$.
(*Para isso, V. deverá supor conhecido o fato que, se uma a expressão polinomial, como* $x^3 + 2x^2 + 10x - 20$, *assumir os valores* a *e* b, *então assumirá também qualquer valor intermediário entre* a *e* b.)

ii). Prove que a equação (8.3) não tem mais nenhuma outra raiz real.
(*A maneira mais fácil de fazermos isso consiste em mostrar, usando Geometria Analítica, que o gráfico cartesiano da cúbica* $y = x^3$ *intercepta em um único ponto o gráfico da parábola* $y = -2x^2 - 10x + 20$.)

É ainda mais fácil e mais elementar provarmos que a raiz real da equação de Fibonacci é irracional:

Exercício 247 -

Mostre que a raiz verdadeira da equação de Fibonacci não *pode ser um número racional.*

Resta, assim, mostrarmos como Fibonacci conseguiu provar que a raiz verdadeira de sua equação não está na família das irracionalidades quadráticas, sendo então um irracional de outra natureza, o que para sua época foi um grande feito. Ora, como já sabemos que essa raiz é irracional, resta provarmos que ela não é raiz de nenhuma equação quadrática de coeficientes inteiros.

Essa prova requer uma certa manipulação "bem-feita" da cúbica envolvida. No entanto, ela é uma prova inteiramente elementar, que usa apenas fatos que todo estudante do Ensino Médio conhece. Por isso, achamos extremamente educativo que o estudante, antes de ler a demonstração que daremos a seguir, tente provar esse resultado. Mesmo que, ao final, não consiga chegar à prova do mesmo, o ganho matemático que terá na tentativa deve sobejamente compensar o insucesso.

Vamos, enfim, ao teorema principal de Fibonacci:

Teorema 8.18 -

A equação

$$x^3 + 2x^2 + 10x = 20 \tag{8.4}$$

não tem raízes no campo das irracionalidades quadráticas.

Prova:

Suponhamos por absurdo que a equação

$$x^3 + 2x^2 + 10x = 20$$

admita uma irracionalidade quadrática como raiz. Pelo Teorema 8.16, podemos escrever tal irracionalidade na forma

$$\frac{m + \varepsilon\sqrt{p}}{n},$$

com $\varepsilon = \pm 1$ e p um inteiro positivo que não é um quadrado perfeito. Mas, então, substituindo tal valor na equação dada, e multiplicando todos os termos por n^3, obteremos

$$(m + \varepsilon\sqrt{p})^3 + 2n(m + \varepsilon\sqrt{p})^2 + 10n^2(m + \varepsilon\sqrt{p}) = 20n^3\,,$$

ou seja, como $\varepsilon^2 = 1$,

$$\begin{aligned} 20n^3 = {} & m^3 + 3m^2\varepsilon\sqrt{p} + 3mp + \varepsilon p\sqrt{p} + 2m^2n + 4mn\varepsilon\sqrt{p} + \\ & + 2np + 10mn^2 + 10n^2\varepsilon\sqrt{p}\,, \end{aligned}$$

ou ainda,

$$20n^3 - m^3 - 3mp - 2m^2n - 2np - 10mn^2 = \varepsilon(3m^2 + p + 4mn + 10n^2)\sqrt{p}\,.$$

Afirmamos que $3m^2+p+4mn+10n^2 \neq 0$ (vide exercício a seguir) e isto nos permite concluir que $\sqrt{p}$ é um número racional. Ora, essa conclusão é absurda, uma vez que p é um inteiro que não é um quadrado perfeito (recorde os resultados do Exercício 212).

CQD.

Exercício 248 -

Sendo m, n inteiros quaisquer, e p um inteiro positivo, prove que

$$3m^2 + p + 4mn + 10n^2 > 0\,.$$

Faça isso provando que a identidade clássica $(a-b)^2 = a^2 - 2ab + b^2$ (onde a, b são números reais) produz: $a^2 + b^2 \geqslant 2ab$.

É natural pensarmos em classificar a raiz irracional da cúbica de Fibonacci como uma irracionalidade "cúbica". Para introduzirmos formalmente o conceito geral de irracionalidade cúbica, é preciso termos o cuidado de proibir que elas sejam também irracionalidades quadráticas. Assim, a definição tem de ficar como segue:

Definição 8.19 -

Por irracionalidade algébrica de grau 3, ou irracionalidade cúbica, entendemos qualquer número irracional que seja raiz de uma equação polinomial de grau 3 e coeficientes inteiros, mas que não seja também raiz uma equação polinomial de grau menor e coeficientes inteiros.

Exemplo 8.20 -

Os resultados anteriores nos permitem afirmar que a única raiz verdadeira da equação de Fibonacci,

$$x^3 + 2x^2 + 10x = 20\,,$$

é uma irracionalidade cúbica.

O cálculo numérico de Fibonacci.

Fibonacci também calculou uma aproximação da raiz verdadeira da cúbica (8.4). Para isso, provavelmente, usou o que hoje chamamos de "algoritmo da falsa posição". No *Flos*, ele resumiu-se a dar o valor dessa aproximação, expressando-a, conforme costume da época, no sistema sexagesimal:

$$1^{\circ}22'7''42'''33^{iv}4^{v}40^{vi}.$$

O leitor é convidado a mostrar que a aproximação que Fibonacci deu para a raiz verdadeira de sua cúbica tem como expansão decimal:

$$1,36880811... .$$

Os métodos computacionais modernos nos permitem facilmente calcular o valor exato das primeiras dezenas de algarismos decimais de tal raiz verdadeira:

$$1,368808107821372635227414330 0... .$$

O leitor é convidado a estimar o erro cometido por Fibonacci.

Exercício 249 -

Mostre que $\sqrt[3]{2}$ é uma irracionalidade cúbica.
Dica: imitando Fibonacci, use que conhecemos a fórmula de todas as irracionalidades quadráticas.

Exercício 250 -

V ou F? Justifique.

$$\textit{O real } r \neq 0 \textit{ é irracionalidade cúbica} \iff 1/r \textit{ é irracionalidade cúbica.}$$

Existem outros exemplos de irracionalidades cúbicas? Sim, mas a prova da existência sempre esbarra em uma dificuldade análoga à enfrentada por Fibonacci: além de termos de achar uma cúbica da qual o "candidato" é raiz, temos de garantir que ele não é raiz de nenhuma equação quadrática de coeficientes inteiros. A experiência mostra que, normalmente, não vale a pena provar tal garantia, sendo suficiente sabermos que o irracional em questão é raiz de alguma equação de coeficientes inteiros; não interessando o grau da mesma. Números com esse tipo de propriedade são denominados "números algébricos" e serão estudados na próxima seção.

8.6 Números algébricos

Esta seção tem duas partes. Na primeira, introduziremos uma família de números irracionais de complexidade crescente, embora caracterizados de maneira estritamente algébrica. A estratégia de construção de tal família será baseada na generalização dos conceitos de irracionalidades quadráticas e cúbicas, definindo as irracionalidades quárticas, quínticas, etc.

Na segunda parte, trataremos de investigar se esses números podem ser expressos por meio de fórmulas algébricas.

Apesar das questões que investigaremos serem bastante naturais e formuladas em termos bem elementares, a prova da maioria dos respectivos teoremas exige técnicas matemáticas mais pesadas do que as que dispomos no momento. Assim, nos limitaremos a comentar sobre essas provas. Com isso, esperamos ao menos estar motivando o leitor para estudos menos elementares. Além do que, a maioria desses teoremas propicia a oportunidade de mostrarmos exemplos de resultados recentes da pesquisa matemática, mais especificamente da pesquisa recente em Teoria Algébrica dos Números.

Definição 8.21 -

Por irracionalidade algébrica de grau n *(onde n é um inteiro $\geqslant 2$), entendemos qualquer número real que é raiz de uma equação polinomial de grau n e coeficientes inteiros, mas que não é raiz de nenhuma equação polinomial de grau menor e coeficientes inteiros.*

Como o número surdo $x = \sqrt[k]{2}$ verifica a equação $x^k - 2 = 0$, é de se esperar que $\sqrt[2]{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}, \ldots$ formem uma família de irracionalidades algébricas de graus, respectivamente, iguais a 2, 3, 4, ... Contudo, a prova disso não é trivial, exigindo conhecimentos que não foram até aqui abordados. Assim, nos limitaremos a enunciar o seguinte teorema que garante a existência de irracionalidades de grau n, qualquer que seja $n \geqslant 2$.

Teorema 8.22 (*generalizado de Fibonacci*) -

Para cada $n \geqslant 2$, existem irracionalidades algébricas de grau n.

A essência da utilidade da noção de irracionalidade de grau n está na possibilidade de se usar o grau de irracionalidade como uma medida do “quão complicada” é a expressão do respectivo número irracional. Com efeito, podemos esperar uma correspondência entre o grau de irracionalidade e a complexidade da expressão algébrica de um irracional pois, à medida que formos aumentando o grau das equações polinomiais, vai aumentando a complexidade das fórmulas que expressam suas raízes em termos dos coeficientes. Ou seja, quanto maior for o grau da irracionalidade de um número algébrico, é de se esperar que mais complicada fique sua expressão em termos de operações aritméticas e de radiciação sobre os coeficientes inteiros da equação polinomial que o originou.

Resumindo, podemos dizer que a noção de grau de irracionalidade algébrica nos dá uma "escala de complexidade" para os números irracionais, e que o teorema generalizado de Fibonacci nos garante que todos os níveis desta escala são realizados.

Exercício 251 -

V ou F? Justifique.

"O real $r \neq 0$ é algébrico de grau $n \iff 1/r$ é algébrico de grau n."

Infelizmente, conforme já sabemos da cúbica de Fibonacci, na prática é difícil tratarmos com a noção de irracionalidade de grau n. Isso nos leva a introduzir uma ideia mais trabalhável, embora menos precisa:

Definição 8.23 -

Por irracionalidade algébrica, *entendemos todo número irracional que é raiz de uma equação polinomial de coeficientes inteiros.*

O resultado a seguir mostra que, em verdade, não introduzimos nenhum novo tipo de número irracional, apenas demos uma caracterização menos precisa deles.

Teorema 8.24 -

Cada irracionalidade algébrica tem um grau, ou seja: podemos encontrar um n, tal que ela seja irracionalidade de grau n.

Prova:

Seja r a irracionalidade algébrica dada. Pela definição, ela é raiz de uma equação polinomial de coeficientes inteiros e um certo grau n. Como r é irracional, temos que $n \geqslant 2$. Mostremos que r é irracionalidade de um grau k, com $2 \leqslant k \leqslant n$.

Para que o argumento fique bem claro, suponhamos inicialmente que $n = 4$, e indiquemos por E_k o universo das equações polinomiais de coeficientes inteiros e grau k. Se r não é raiz de nenhuma equação de E_3 ou E_2, teremos $k = 4$. Caso contrário, indiquemos por E_m a última família de equações E_i (tomadas na sequência decrescente, $i = 3\,,2$) onde encontramos r como raiz. Então:

- se $m = 3$, temos que r é raiz de uma equação de E_3, mas não é raiz de uma equação de E_2; logo, r é uma irracionalidade cúbica, ou seja: $k = 3$;
- se $m = 2$, temos que r é raiz de uma equação de E_2, e então, como ele é irracional, terá de ser uma irracionalidade quadrática; ou seja: $k = 2$.

No caso geral, de $n \geqslant 2$ qualquer, como r é irracional, sempre encontraremos um $2 \leqslant m \leqslant n$, tal que r é raiz de uma equação de E_m e não é raiz de nenhuma equação de E_i, para $i < m$. O ponto básico sendo que, sempre existe um menor possível valor para m: este será $m = 2$.

CQD.

Exemplo 8.25 -

Todo número surdo é uma irracionalidade algébrica.
Com efeito, dado $x = \sqrt[k]{r}$, *onde* r *é um número racional, temos que* $x^k = r$. *Escrevendo* $r = m/n$, *temos que* x *é raiz da equação* $nx^k - m = 0$. *Ademais, um* x *dessa forma é surdo se, pela definição, ele for irracional.*

Exemplo 8.26 -

Um exemplo de irracionalidade algébrica que não é surdo é $\sqrt{1+\sqrt{2}}$.
Com efeito, denotando-o por x, *temos que* $x^2 = 1 + \sqrt{2}$, *de modo que* $x^2 - 1 = \sqrt{2}$ *e, então:* $(x^2 - 1)^2 = 2$. *Ou seja, ele é uma raiz real da equação polinomial de coeficientes inteiros:*

$$x^4 - 2x^2 - 1 = 0\,.$$

Ademais, ele também é irracional.
Com efeito, se ele fosse racional, seu quadrado, x^2, *também seria, o que daria o absurdo:* $x^2 = 1 + \sqrt{2} =$ *irracional.*

Exercício 252 -

Provar que $\sqrt{2} + \sqrt{3}$ *é uma irracionalidade algébrica.*

Exercício 253 -

Provar que são irracionalidades algébricas todos os números do conjunto

$$\left[\mathbb{Q}, \sqrt{2}\right]^* = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}, com\ b \neq 0\}\,.$$

Exercício 254 -

Mostre que o grau de cada irracionalidade algébrica é único.

Vimos que a noção de irracionalidade de grau n é difícil de ser trabalhada na prática. Por sua vez, as irracionalidades algébricas têm o inconveniente de não formarem um campo com estrutura algébrica minimamente cômoda. Com efeito, mesmo uma soma de irracionalidades algébricas pode ser racional. Confira: $(1 + \sqrt{2}) + (1 - \sqrt{2}) = 2\,!$ Isso nos motiva introduzir uma nova noção que nos permita incluir as irracionalidades algébricas num campo com estrutura de corpo:

Definição 8.27 -

Denominamos número real algébrico *todo número real – racional ou irracional – que seja raiz de alguma equação polinomial de coeficientes inteiros:*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0\,, (a_n \neq 0\,, a_k \in \mathbb{Z}\,,\ \forall k)\,.$$

Exemplo 8.28 -

Equações da forma $mx - n = 0$ (com $m \neq 0$ e n inteiros) mostram que todo número racional é um real algébrico.
Ademais, também é imediato que toda irracionalidade algébrica é um número real algébrico.

Pelo exemplo anterior, temos que

> o conjunto dos números reais algébricos pode ser dividido em duas partes disjuntas:
>
> – o corpo dos números racionais e
> – o conjunto das irracionalidades algébricas.

O exemplo e observação anteriores sugerem que se existirem números irracionais "fora" do universo dos números algébricos, eles se originam em contextos que transcendem o âmbito da Álgebra. Voltaremos a isso na próxima seção.

Exercício 255 -

Provar que um número real é algébrico se, e somente se, ele for raiz de um polinômio com coeficientes racionais.

Observação 8.29 -

O exercício anterior nos chama a atenção para o fato que, se tivessemos definido número real algébrico como sendo raiz de uma equação polinômial de coeficientes racionais, não obteríamos nenhum novo número real como número algébrico. Mais geralmente, na Teoria dos Polinômios, mostra-se que, mesmo que passemos das equações polinomiais de coeficientes inteiros para as equações polinomiais de coeficientes reais algébricos quaisquer – possivelmente até irracionais algébricos –, não ganharemos nada de novo: as raízes reais destes polinômios mais gerais continuarão sendo números reais algébricos. Deixamos a demonstração desse resultado para a Álgebra.

Exercício 256 -

Mostre que, se r é um número real algébrico não-nulo, então $1/r$ também é algébrico.

Exercício 257 -

Mostre que, se r é um número real algébrico, então $-r$ também o é.

Exercício 258 -

Mostre que, se r é um número real algébrico não nulo, e positivo e k é um número natural não-nulo, então $\sqrt[k]{r}$ também é um número real algébrico.
Dica: escrevendo $y = \sqrt[k]{r}$, substitua $r = y^k$ na equação de coeficientes inteiros da qual r é raiz.

Teorema 8.30 -

A adição, subtração, multiplicação e divisão de números reais algébricos, bem como a radiciação de algébricos positivos, sempre produz como resultado um número real ainda algébrico.

Comentários sobre a prova desse teorema.

Obviamente, os exercícios 256, 257 e 258 são casos particulares desse teorema. Para qualquer um desses três casos, a "fabricação" de uma equação polinomial que seja satisfeita por $1/r$, $-r$ ou $\sqrt[p]{r}$ pode ser feita de forma razoavelmente fácil a partir da equação polinomial satisfeita por r. Contudo, os demais casos contemplados pelo teorema não têm uma demonstração tão simples.

Por exemplo, para mostrar que a soma $r+s$ de números reais algébricos r e s é um número real também algébrico, temos que partir de uma equação polinomial verificada pela parcela r e de uma outra equação verificada pela parcela s, e, então, fabricar uma terceira equação com coeficientes inteiros que seja verificada pela soma $r+s$. Tarefa difícil, pois além dos coeficientes poderem ser diferentes, os graus das equações não precisam ser iguais; de fato, o grau da equação polinomial verificada por $r+s$ será, em geral, maior do que os graus das equações verificadas por r e s.

Isso tudo indica que precisamos de um argumento muito engenhoso ou de ferramentas mais poderosas. Por essas razões, deixaremos a prova desse teorema para a Álgebra.

Corolário 8.31 -

O conjunto dos números reais algébricos é um corpo.

Exercício 259 (*cuidado!*) -

V. ou F.? Justifique:

i). racional + irracionalidade algébrica = irracionalidade algébrica;
ii). irracionalidade algébrica + irracionalidade algébrica = irracionalidade algébrica.

– Relação entre a noção de número algébrico e de fórmula algébrica

Já que os números algébricos têm uma caracterização totalmente algébrica, é natural de se esperar que eles também possam ser expressos algebricamente.

Iniciamos observando que, se um número real pode ser expresso por fórmula algébrica, então ele tem de ser um número algébrico.

Teorema 8.32 -

Todo número real que possa ser expresso em termos de uma fórmula algébrica envolvendo apenas números inteiros será um número algébrico.

Prova:

A demonstração é uma mera generalização do argumento usado no Exemplo 8.26.

CQD.

Resta-nos investigar se vale a recíproca, ou seja: será que todo número algébrico é representável por uma fórmula algébrica?

Teorema 8.33 *(Teorema de Galois)* -

Existem números irracionais algébricos que não podem ser expressos por meio de uma fórmula algébrica. Um exemplo deles é a raiz real da equação $x^5 - x - 1 = 0$.

Comentários sobre a prova desse teorema.

Usando Geometria Analítica, é fácil vermos que essa equação tem apenas uma raiz real, e que ela é positiva. Ademais, é imediato se verificar que essa equação não tem nenhuma raiz racional, consequentemente, sua única raiz é um número algébrico irracional. Assim, resta provar que ela não pode ser expressa por meio de uma fórmula algébrica, no sentido expresso na Seção 8.2.

Infelizmente, a demonstração dessa impossibilidade envolve técnicas matemáticas bem mais avançadas do que as deste livro, sendo mais adequada e completamente realizada num importantíssimo campo da Álgebra chamado de Teoria de Galois.

Observação 8.34 -

Além das dificuldades técnicas que apontamos anteriormente, há uma razão de ordem estrutural para deixarmos para a Álgebra um estudo mais aprofundado e completo dos números algébricos. Essa razão de ordem estrutural consiste na necessidade de trabalharmos num campo numérico que seja, ao contrário do dos números reais, algebricamente completo*: um campo no qual se possa afirmar que toda equação polinomial de grau $n \geqslant 1$ tenha exatamente n raízes. Por exemplo, a equação polinomial $x^2 + 1 = 0$ não tem raízes no campo dos reais; logo, $\mathbb{R}$ não é algebricamente completo. Contudo, ela tem duas raízes no campo completo dos números complexos ou imaginários, que iniciaremos a estudar no próximo capítulo.*

8.7 Transcendência: todos os irracionais são algébricos?

O Teorema de Galois mostra que a ideia de classificar o grau de complexidade dos números irracionais por meio de sua fórmula algébrica não pode atingir sucesso pleno. Com efeito esse teorema garante que existem números irracionais que nem ao menos têm uma fórmula algébrica.

Isso, por si só, já demonstra uma impotência da Álgebra. Mas podemos ir além, perguntando se existem números irracionais não algébricos. Se existirem, teremos exemplos de números transcendendo totalmente a capacidade da Álgebra. O primeiro matemático que examinou essa questão foi Leonhard Euler, em torno de 1750, e é dele a seguinte definição:

Definição 8.35 -

Número transcendente é todo número real que não é algébrico.

Obviamente, todo número transcendente tem de ser irracional. Talvez, por isso Euler não tenha sido capaz de achar um único exemplo de transcendência, tendo "empacado" na tentativa de confirmar sua suspeita de que π e a base e dos logaritmos naturais seriam números transcendentes.

A decisão da existência, ou não, de números transcendentes passou a ser cada vez mais embaroçosa para a comunidade matemática. Os esforços só começaram a frutificar cem anos depois de Euler, quando, em 1844, Joseph Liouville demonstrou o resultado que segue.

Teorema 8.36 -

Existem números reais (irracionais) não algébricos. Ou seja: existem números transcendentes.

A prova de Liouville consistiu em mostrar que o seguinte número real é transcendente:

$$0,110001000000000000000001000\dots\,.$$

Observe que trata-se de um número irracional, pois a quantidade de zeros vai crescendo fatorialmente. Ele pode ser definido mais precisamente da seguinte maneira: $0,a_1a_2\dots$, onde

$$a_n = \begin{cases} 1, & \text{se } n = k!\,, \text{ para algum natural não-nulo } k\,; \\ 0, & \text{caso contrário.} \end{cases}$$

Omitiremos os detalhes da demonstração, uma vez que os mesmos requerem recursos de Cálculo Infinitesimal, o que não estamos exigindo neste livro.

> O campo $\mathbb{R}$ dos números reais pode ser dividido em duas partes disjuntas:
> – o conjunto dos números (reais) algébricos e
> – o conjunto dos números (reais) transcendentes.

Exercício 260 -

i). Mostre que a soma de um número algébrico com um transcendente sempre será transcendente.

ii). Escreva infinitos exemplos de números transcendentes.

O exemplo de número transcendente dado por Liouville era obviamente artificial, sem nenhum outro uso em Matemática. Foram precisos mais quase trinta anos para se descobrir o primeiro transcendente ocorrendo naturalmente. Com efeito, em 1 873, Charles Hermite conseguiu mostrar que e, a base dos logaritmos naturais, também é transcendente. Quase dez anos depois, em 1 882, Ferdinand von Lindmann, finalmente, conseguiu mostrar que π também é transcendente. A repercussão da prova da transcendência de π foi das maiores. Por exemplo, sabendo isso, os matemáticos puderam alcançar um objetivo que vinha sendo perseguido há mais de dois mil anos, desde o tempo dos gregos clássicos:

> finalmente, pode-se provar que *é impossível se fazer a quadratura do círculo usando apenas régua e compasso.*

É importante entendermos o papel da transcendência de π nessa demonstração. Para tal, iniciemos recordando que "fazer a quadratura" do círculo consiste em construir um quadrado, cujo lado seja um segmento de reta com medida ℓ verificando:

$$\ell^2 = \pi$$

(isto é, a área do tal quadrado tem de ser igual à do círculo de raio unitário). Por outro lado, fazer a quadratura do círculo "usando régua e compasso" significa que temos de construir o lado do tal quadrado usando apenas esses instrumentos (para maiores detalhes veja o Capítulo 5). Ora, prova-se que todos os segmentos de reta que podemos construir com régua e compasso, a partir de um segmento unitário, têm como medida um número algébrico; logo, resta aplicar o item (ii) do seguinte:

Exercício 261 -

i). Mostre que a raiz quadrada de um número irracional pode ser um número real algébrico.

ii). Mostre que a raiz quadrada de um número transcendente nunca pode ser um número real algébrico.

Também é importante se dizer que, antes de Lindemann ter conseguido provar que π é transcendente, o grande matemático George Cantor, em 1874, fez outra das mais sensacionais descobertas de todos os tempos ao demonstrar que

A grande maioria dos números reais é constituída de números transcendentes!

O resultado de Cantor é bem pouco intuitivo. Contudo, expressa um fato semelhante ao que já observamos, quando comparamos o tamanho do conjunto dos números racionais com o tamanho do conjunto dos irracionais. Com efeito, na Teoria dos Conjuntos, mostra-se que "a infinitude da quantidade de números algébricos" é do mesmo tipo que a do conjunto dos números racionais – é um infinito que pode ser "enumerado"[4] ou "contado" –, enquanto "a infinitude da quantidade de números transcendentes" é do mesmo tipo que a do conjunto dos números dos irracionais – é um infinito *tão grande* que não pode ser "enumerado" ou "contado" (ou seja, *não* pode ser posto em correspondência biunívoca com o conjunto dos naturais).

Esse resultado de Cantor caiu como um raio na comunidade matemática. Com efeito, naquela época, eram conhecidos infinitos irracionais algébricos, mas, essencialmente, apenas dois exemplos de números transcendentes!

– O Sétimo Problema de Hilbert

Alguns anos depois do resultado de Cantor, mais precisamente em 1900, foi realizado um congresso mundial de matemáticos em Paris, no qual a principal conferência foi

[4]De um modo geral, um conjunto é dito ser *infinito enumerável* quando se pode estabelecer uma correspondência biunívoca entre este conjunto e o conjunto dos números naturais

feita por David Hilbert, um dos mais importantes matemáticos daquela época. Nessa histórica conferência, entitulada *Os problemas da Matemática,* Hilbert se propôs a nada mais nada menos do que dar uma lista de problemas que deveriam nortear os rumos da Matemática no século XX. Entre seus 23 problemas estava o seguinte:

decidir se $2^{\sqrt{2}}$ *é irracional algébrico, ou irracional transcendente.*

A resposta para esse problema veio apenas em 1 930, quando R. Kuzmin e C. L. Siegel provaram, independentemente, o seguinte teorema que tornou-se uma preciosa fonte geradora de exemplos de números transcendentes:

Teorema 8.37 -

O número $2^{\sqrt{2}}$ *é transcendente e o mesmo ocorre com* $a^{\sqrt{n}}$*, sempre que* a *for um número real algébrico não nulo, diferente da unidade, e* n *for um inteiro positivo não quadrado.*

Quatro anos depois, o russo A. Gelfond generalizou esse teorema para:

Teorema 8.38 (*Gelfond*) -

O número a^b *é transcendente sempre que* a *for um número algébrico não nulo, diferente da unidade, e* b *não for um número racional.*

Para encerrarmos esses comentários sobre números algébricos e transcendentes, observemos ainda que o estudo dos mesmos originou um novo e importantíssimo campo matemático, a chamada Teoria Algébrica dos Números. Essa usa de forma vital e muito produtiva os números complexos ou imaginários, que estudaremos no capítulo seguinte, e inicia estendendo a noção de número real algébrico para número complexo algébrico (ou meramente, número algébrico). Essa extensão é a mais natural possível: um número (complexo) algébrico é meramente toda raiz (real ou complexa) de uma equação polinomial de coeficientes inteiros.

Como exemplo do poder dessa teoria, examinemos a natureza do número e^{π}. A transcendência desse número é facilmente estabelecida a partir da versão imaginária do Teorema de Gelfond e das igualdades seguintes:

$$e^{\pi} = e^{-2i \ln i} = i^{-2i}\,.$$

Com efeito, restaria observar que i é um número complexo algébrico, pois é raiz de $x^2 + 1 = 0$, e que certamente $-2i$ não é racional.

CAPÍTULO 9

NÚMEROS COMPLEXOS

O caminho mais curto entre duas verdades do campo real
passa através do campo complexo.
Jacques Hadamard.

Vimos que o campo dos números racionais é insuficiente para a medida de muitas grandezas geométricas – como é o caso da medida da diagonal do quadrado –, o que nos força a passar a tratar $\sqrt{2}$ como número. A introdução do campo dos números reais elimina esse grave defeito, mas ainda deixa muito a desejar, tanto aritmética quanto algebricamente.

Uma das principais causas da *insuficiência aritmética* do campo dos reais reside em sua incapacidade de nos permitir operar adequadamente com números negativos. Essa incapacidade já se manifesta com as operações algébricas, uma vez que é impossível atribuir um valor real para $\sqrt{-1}$, ou qualquer outra raiz quadrada de número negativo, pois o quadrado de todo número real não nulo é positivo. Se passarmos ao nível das operações transcendentais, encontraremos uma impossibilidade ainda maior de operações numéricas. Por exemplo, embora os números reais sejam plenamente suficientes para permitir atribuir sentido a expressões como 2^{π}, eles são incapazes de gerar valor numérico para, por exemplo, $(-2)^{\pi}$. Analogamente, os reais nos permitem calcular logaritmos de números positivos, como $\log(2)$, mas não são suficientes para o cálculo de logaritmos de números negativos, como o $\log(-2)$, pois isto implica achar um número x tal que 10^x seja um valor negativo, o que é uma impossibilidade no universo dos números reais.

O primeiro passo no sentido de resolver essas insuficiências aritméticas do campo dos números reais foi dada por Raphael Bombelli, em 1572, quando teve – em suas próprias palavras – a "ideia louca" de tratar $\sqrt{-1}$, e as expressões mais gerais $a+b\sqrt{-1}$ (onde a e b são números reais), como se fossem números. Essas expressões são o que hoje chamamos de *números complexos*.

Somente trezentos anos após Bombelli, depois de muita resistência, muitos impasses e polêmicas, acabou-se concluindo a demonstração de que os números complexos são capazes de enfrentar adequadamente todas as insuficiências aritméticas já apontadas, bem como foram estabelecidas regras para cálculos que até há alguns séculos eram totalmente impensáveis, tais como:

$$\sqrt{-1}^{\sqrt{-1}} = 0,20787957635076190854\ldots\ .$$

O estudo sistemático dos números complexos, que iniciaremos a seguir, terá uma primeira parte que concluirá com a demonstração dos fatos mencionados acima e que serão resumidos por meio dos chamados *Teoremas Finais da Aritmética*, pela primeira vez provados por Karl Weierstrass, num curso que deu em 1863.

A segunda parte do nosso estudo do campo dos números complexos terá como principal objetivo mostrar que esse campo também "resolve" a *insuficiência algébrica* do campo dos números reais. Com isso, queremos dizer que o campo dos números complexos é capaz de dar resposta a questões básicas da teoria dos polinômios e das equações polinomiais. Como é importante que desde já fique claro o que estamos dizendo, examinemos duas das mais importantes dessas questões.

– A questão da existência de raízes das equações polinomiais.

Por muitos séculos, as raízes de uma equação eram vistas como um fim em si: eram o valor de uma altura buscada, de uma área desejada ou o valor de alguma outra grandeza geométrica. Naquela época, o fato de uma equação não ter nenhuma raiz real significava apenas que o problema fora mal formulado, não tinha solução. Por cerca de 1600, esse ponto de vista foi dramaticamente alterado com o surgimento do cálculo literal introduzido na *Logistica Speciosa*, de François Viète. Com isso, passou-se a ter condições de trabalhar com equações de coeficientes literais e grau qualquer. Em particular, ficou natural verificar se as relações entre raízes e coeficientes – hoje chamadas de fórmulas de Newton-Viète, e que Cardano havia descoberto por volta de 1550 no caso de certas cúbicas – continuavam a valer para equações polinomiais de qualquer grau.

Exemplo 9.1 -

Fórmulas de Newton-Viète nos casos de equações polinomiais de grau baixo:

i). equações de grau $n = 2$ (quadráticas):
indicando por r_1, r_2 as raízes da equação quadrática $ax^2 + bx + c = 0$, valem as relações

$$r_1 + r_2 = -b/a, \quad r_1 r_2 = c/a\,;$$

ii). equações de grau $n = 3$ (cúbicas):
indicando por r_1, r_2, r_3 as raízes da equação cúbica $ax^3 + bx^2 + cx + d = 0$, valem as relações

$$r_1 + r_2 + r_3 = -b/a\,, \quad r_1 r_2 + r_1 r_3 + r_2 r_3 = c/a\,, \quad r_1 r_2 r_3 = -d/a\,.$$

Ora, a possibilidade da existência de uma relação entre as raízes e os coeficientes depende de um resultado mais básico: *toda equação polinomial de grau n deve ter n raízes.* Este resultado é obviamente falso no contexto de equações sobre o campo dos números reais: basta tomarmos a equação $x^2 + 1 = 0$. Contudo, conforme veremos, ele é sempre verdadeiro no campo dos números complexos, verdade essa que constitui o chamado Teorema Fundamental da Álgebra, o principal resultado da segunda parte de nosso estudo.

– A questão da fatoração dos polinômios.

A necessidade de se fatorar um polinômio tornou-se muito importante com o estudo da chamada integração das frações racionais, $p(x)/q(x)$, o que ocorreu lá por cerca de 1700. Foi prontamente mostrado que a resolução desse importante problema do Cálculo Integral resumia-se à possibilidade de se *fatorar, em termos de fatores reais lineares e/ou reais quadráticos, qualquer polinômio de coeficientes reais.* Embora esse resultado esteja enunciado totalmente no campo dos números reais, sua demonstração é equivalente à do Teorema Fundamental da Álgebra e, então, depende de modo essencial do campo dos números complexos.

Sob uma perspectiva maior, que permita vislumbrar todo o "edifício matemático", podemos dizer que, apesar da maneira suspeita com que os números complexos foram recebidos na Matemática (tanto que inicialmente eram chamados de imaginários e sofísticos), eles, além de se mostrarem plenamente capazes de resolver todas as insuficiências aritméticas e algébricas dos números reais, também se mostraram ser uma ferramenta muito eficaz para descobrir relações entre os mais diversos campos matemáticos e serem o contexto natural para entendermos muitos objetos matemáticos importantes, tais como as funções analíticas. Com isso, eles se firmaram como uma parte essencial do "kit de ferramentas" de todo matemático.

A importância dos números complexos, como consequência quase que automática do valor matemático intrínseco destes números, também se consolidou "fora" da Matemática. Hoje, os mais diversos campos da Ciência e da Tecnologia fazem deles um uso muito frutífero: na análise dos sistemas dinâmicos contínuos, no controle e estabilidade dos mais diversos sistemas de engenharia, no projeto de circuitos e motores de corrente alternada, na análise e síntese de sinais físicos e biológicos, etc.

Exemplo 9.2 -

A análise e projeto de circuitos de corrente alternada e motores elétricos emprega o conceito de número complexo; foi aí que, pela primeira vez, se usou a noção de número complexo em um problema fora do âmbito da Matemática. O grande pioneiro nessa área foi Oliver Heaviside, em torno de 1890. O leitor é convidado a consultar uma enciclopédia ou outra fonte de informações históricas para ficar sabendo um pouco sobre o trabalho desse polêmico engenheiro.

Exercício 262 -

Uma das mais antigas e respeitadas escolas de Engenharia é a École Polytechnique, de Paris. Durante o século XIX, ela imperou absoluta como o mais avançado centro de formação de engenheiros no mundo.

Por volta de 1880, os alunos dessa escola fizeram uma grande greve, seguida de incêndios e depredações, exigindo o expurgo de disciplinas e conteúdos curriculares que eles consideravam como obsoletos ou sem nenhuma utilidade no trabalho dos engenheiros. Um dos conteúdos que figurava na "lista negra" daqueles alunos era o estudo dos números complexos.
Pergunta-se: levando-se em conta o que foi dito anteriormente, que moral pode-se tirar desse acontecimento?

9.1 Motivação à introdução dos números complexos: o "destravamento de cálculos algébricos"

Toda equação de grau um e coeficientes inteiros, ou racionais, tem raízes no campo dos números racionais. Contudo, já muito insistimos que o mesmo não vale para as equações de grau dois. É o caso da equação $x^2-2=0$, que só tem raízes no conjunto das irracionalidades quadráticas. Essa insuficiência algébrica do campo dos números inteiros, e mesmo dos racionais, não fica completamente sanada com a introdução do campo dos números reais. Com efeito, a equação $x^2+1=0$ nos mostra que existem equações polinomiais de coeficientes reais (na verdade: inteiros) mas sem raízes reais. Essa observação leva a maioria dos livros elementares a uma *conclusão histórica incorreta*, qual seja, a afirmar que o campo dos números complexos foi introduzido para podermos resolver todas as equações do segundo grau, sanando asssim a insuficiência do campo dos reais.

Na verdade, a introdução dos números complexos foi historicamente motivada por um problema diferente, a saber: dada uma equação polinomial cujos coeficientes estão num campo numérico $\mathbb{K}$, e *a qual é sabido ter raízes em tal* $\mathbb{K}$, deseja-se decidir se é possível calcular tais raízes usando-se somente operações algébricas (ou seja: as quatro operações aritméticas, bem como as radiciações) válidas em $\mathbb{K}$ e envolvendo apenas os coeficientes da equação. De um modo um pouco mais resumido:

> Dada uma equação polinomial com coeficientes num campo numérico $\mathbb{K}$, é possível obter as raízes que estão em $\mathbb{K}$ por meio do cálculo de uma fórmula envolvendo os coeficientes dessa equação?
> (Entende-se que somente serão permitidas operações algébricas válidas em $\mathbb{K}$.)

Quando $\mathbb{K} = \mathbb{R}$ e a equação for de grau um ou dois, a resposta é "Sim, sempre!", conforme veremos. Contudo, a situação muda completamente de figura no caso das equações cúbicas.

Com efeito, veremos em detalhe adiante que a conhecida fórmula de Tartaglia-Cardano, embora normalmente seja capaz de calcular – em álgebra real – as raízes reais de equações cúbicas de coeficientes reais, em certos tipos especiais de cúbicas (como é o caso de $x^3 - 15x - 4 = 0$, que tem somente raízes reais: $x = 4,\ x = -2 + \sqrt{3}$ e $x = -2 - \sqrt{3}$) "trava", não nos permitindo concluir o cálculo das raízes que sabemos existirem e serem reais.

A *verdadeira introdução do campo dos números complexos* ocorreu como um artifício que Raphael Bombelli, por volta de 1570, inventou para conseguir "destravar"a fórmula de Tartaglia-Cardano e possibilitar que ela chegue até as raízes reais de qualquer cúbica.[1]

Antes de passarmos a examinar com detalhe essas questões de "travamento", é conveniente que examinemos com mais cuidado o milenar trabalho de obtenção de procedimentos para resolver equações. Esse trabalho, idealmente, começa com uma *etapa heurística* que, a partir da suposição da existência de raízes para a equação dada, procede a uma série de manipulações algébricas até se conseguir isolar a incógnita da equação, expressando-a em termos de uma fórmula que envolve os coeficientes da mesma. No entanto, é importante salientar-se que é necessária uma segunda etapa, a da *legitimação*, que tratará de mostrar que as operações algébricas da fórmula produzida pela heurística são executáveis no campo numérico em consideração, e

[1] Além da fórmula de Tartaglia-Cardano, hoje são conhecidas várias outras fórmulas para se resolver cúbicas. É importante termos isso em vista, pois o fato de a fórmula de Tartaglia-Cardano travar no cálculo das raízes de algumas cúbicas não quer dizer que o mesmo tenha obrigatoriamente de ocorrer com essas outras fórmulas. Exatamente por isso, o próprio Cardano gastou os últimos anos de sua vida na busca de uma fórmula que nunca travasse. Sua busca não teve sucesso, nem poderia ter tido, pois hoje sabemos que de fato não existe uma fórmula com tal propriedade. Contudo, não insistiremos nisso por se tratar de assunto avançado, e porque o efeito produzido pela fórmula de Tartaglia-Cardano foi suficiente para forçar o surgimento dos números complexos.

que o número que ela produz efetivamente satisfaz a equação dada.

Nesse sentido, não é demais se insistir que na etapa heurística pode-se (e deve-se!) dar asas à criatividade, e não sobrecarregá-la com preocupações acerca da validade das operações algébricas que se atinou e ousou usar. A preocupação com o rigor pode ficar para a etapa da legitimação; essencialmente, é só aí que devemos nos preocupar com a capacidade de a fórmula obtida produzir as raízes desejadas.

Exemplifiquemos esse trabalho de heurística e legitimação na resolução da equação quadrática geral (de coeficientes reais) por meio da chamada fórmula de Bhaskara.

– Heurística da fórmula de Bhaskara

Tomemos a equação quadrática geral de coeficientes reais

$$ax^2 + bx + c = 0.$$

Para isolarmos x, iniciamos multiplicando essa equação por $4a$, obtendo

$$4a^2x^2 + 4abx + 4ac = 0\,;$$

a seguir, observando que os termos $4a^2x^2 + 4abx$ são as duas primeiras parcelas do desenvolvimento do quadrado $(2ax + b)^2$, reescrevemos a equação como:

$$(2ax + b)^2 + 4ac - b^2 = 0\,,$$

ou, colocando $\Delta = b^2 - 4ac$:

$$(2ax + b)^2 - \Delta = 0\,.$$

Extraindo a raiz quadrada, ficamos com

$$(2ax + b) = \pm\sqrt{\Delta}\,,$$

de onde, finalmente, obtemos a conhecida fórmula de Bhaskara:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\,.$$

– Legitimização da fórmula de Bhaskara no campo dos reais

Iniciamos observando que a heurística mencionada nem cogitou da possibilidade de não existirem raízes reais para a equação quadrática

$$ax^2 + bx + c = 0\,.$$

Como consequência, não deve vir como surpresa a constatação de que a fórmula de Bhaskara não é calculável em aritmética real nos casos em que $b^2 - 4ac < 0$. Assim, nossa análise deve tratar de garantir tanto a existência de raízes reais como a viabilidade de seu cálculo. Ambas tarefas ficarão mais fáceis se fizermos uma ligeira modificação do raciocínio anterior (raciocínio que também pode ser legitimado, mas com um desenvolvimento mais extenso). Para isso, vamos fazer uso da identidade clássica

$$u^2 - v^2 = (u - v)(u + v). \tag{9.1}$$

Iniciamos observando que a equação dada é equivalente à

$$4a^2x^2 + 4abx + 4ac = 0,$$

pois a segunda foi obtida multiplicando a primeira pelo fator não nulo $4a$. A seguir, como antes, reescrevemos a segunda equação como

$$(2ax + b)^2 + 4ac - b^2 = 0\,,$$

ou, colocando $\Delta = b^2 - 4ac$:

$$(2ax + b)^2 - \Delta = 0.. \tag{9.2}$$

Prosseguindo, distinguiremos dois casos, conforme o sinal de Δ.

– *Primeiro caso*: $\Delta \geqslant 0$.
Neste caso, como Δ tem uma raiz quadrada real, podemos expressá-lo como o quadrado desta raiz quadrada, de modo que a equação (9.2) pode ser escrita como $(2ax + b)^2 - (\sqrt{\Delta})^2 = 0$ e então, pela identidade (9.1), pode ser reescrita como:

$$\Big((2ax + b) - \sqrt{\Delta}\Big)\Big((2ax + b) + \sqrt{\Delta}\Big) = 0\,,$$

onde não devemos deixar de observar que cada termo dos dois fatores é, de fato, um número real; logo, os fatores também são reais. Consequentemente, calcular as raízes reais da equação quadrática $ax^2 + bx + c = 0$ equivale a achar todas as possibilidades de $x \in \mathbb{R}$ anular o último produto. Ora, esse anulamento ocorre de duas, e só duas, maneiras possíveis:

$$\text{quando } (2ax + b) - \sqrt{\Delta} = 0\,, \text{ ou quando } (2ax + b) + \sqrt{\Delta} = 0\,;$$

equivalentemente, como $a \neq 0$:

$$\text{quando } x = \frac{-b + \sqrt{\Delta}}{2a}\,, \text{ ou quando } x = \frac{-b - \sqrt{\Delta}}{2a}\,.$$

Assim, nos casos em que $\Delta \geqslant 0$, a equação $ax^2 + bx + c = 0$ sempre tem duas raízes reais (possivelmente iguais):

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

Essas duas fórmulas podem ser aglutinadas numa única, a conhecida fórmula de Bhaskara:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

– *Segundo caso*: $\Delta < 0$.
Neste caso, é impossível encontrarmos um $x \in \mathbb{R}$ dando $(2ax + b)^2 - \Delta = 0$, pois $(2ax+b)^2 - \Delta = (2ax+b)^2 + (-\Delta) > 0$, uma vez que $-\Delta > 0$ e que $(2ax+b)^2 \geqslant 0$, para todos os $x \in \mathbb{R}$. Logo, quando $\Delta < 0$, nossa equação não pode ter nenhuma raiz real.

Podemos resumir toda essa discussão da seguinte maneira:

Teorema 9.3 -

Relativamente a uma equação quadrática de coeficientes reais,

$$ax^2 + bx + c = 0,$$

e à respectiva fórmula de Bhaskara

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

i). sempre que os coeficientes da equação fizerem com que o cálculo dessa fórmula não trave em aritmética real (equivalentemente, se os coeficientes da equação forem tais que seja possível executar, em aritmética real, todas as operações da fórmula de Bhaskara), os valores produzidos pela fórmula serão as raízes reais da equação dada;

ii). reciprocamente, se a fórmula travar *em aritmética real (ou seja: se for impossível calcular, em aritmética real, os valores da fórmula de Bhaskara) é porque a equação não tem raízes reais.*

De uma maneira semelhante, passamos agora a examinar a resolução no campo real, e pelo método de Tartaglia-Cardano, das equações cúbicas mais importantes, as da forma

$$x^3 + px + q = 0. \tag{9.3}$$

– Heurística da fórmula de Tartaglia-Cardano

Exploraremos uma outra identidade algébrica clássica:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3,$$

ou seja,

$$(a+b)^3 = 3ab(a+b) + a^3 + b^3,$$

ou ainda,

$$(a+b)^3 - 3ab(a+b) - (a^3+b^3) = 0. \tag{9.4}$$

Comparando (9.3) com (9.4), vemos que, se determinarmos $a, b \in \mathbb{R}$ tais que

$$\begin{cases} -3ab = p \\ -a^3 - b^3 = q\,, \end{cases} \tag{9.5}$$

então $x = a + b$ é uma solução de (9.3). Assim, para buscarmos soluções de (9.3), procuramos soluções $a, b \in \mathbb{R}$ de (9.5). Ora, as igualdades (9.5) e o exemplo 9.1 nos dizem que a^3 e b^3 são as raízes da equação quadrática

$$z^2 + qz - \frac{p^3}{27} = 0\,.$$

Resolvendo esta última equação por Bhaskhara, e extraindo raízes cúbicas, vemos que os valores procurados, a e b, são dados por

$$a = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad \text{e} \quad b = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\,,$$

de modo que um presumível candidato a raiz real de (9.3) é

$$x = a + b = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\,. \tag{9.6}$$

Tentaremos agora tornar legítimo o candidato encontrado em (9.6). Mais precisamente, perguntamo-nos:

Dada uma equação cúbica de coeficientes reais, $x^3 + px + q = 0$, é verdade que, sempre que ela tiver alguma raiz real, ao menos uma delas será dada pela fórmula

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\ ?$$

E se os valores dos coeficientes p e q "travarem" (em aritmética real) tal fórmula, será que poderemos garantir que a equação dada não tem nenhuma raiz real?

A resposta para ambas as questões é *não*. E o exemplo comprobatório é a equação

$$x^3 - 15x - 4 = 0.$$

De fato, note que, por um lado, por inspeção direta, vemos que a mesma tem 4, $-2 + \sqrt{3}$ e $-2 - \sqrt{3}$ para raízes reais (e como discutiremos em seções posteriores, prova-se que não há nenhuma outra raiz real). Por outro lado, fazendo a substituição de $p = -15$ e $q = -4$ na fórmula candidata, obtemos

$$\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}\,,$$

expressão absurda no campo numérico dos reais, pois o lado direito envolve extração da raiz quadrada de um número negativo: uma impossibilidade, em aritmética real.

Concluímos então:

Teorema 9.4 -

Relativamente à equação cúbica de coeficientes reais,

$$x^3 + px + q = 0\,,$$

e à respectiva fórmula de Tartaglia-Cardano

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\,,$$

temos que:

i). sempre que os coeficientes da equação fizerem com que o cálculo da fórmula de Tartaglia-Cardano não trave em aritmética real (equivalentemente: se os coeficientes da mesma forem tais que seja possível calcular, em aritmética real, os valores da fórmula de Tartaglia-Cardano), o valor produzido pela fórmula será uma raiz (real) da equação dada;

ii). contudo, a fórmula pode travar em aritmética real, mesmo nos casos em que a equação tenha raízes reais, sendo então impossível legitimar *tal fórmula em aritmética real.*

No entanto, nem tudo está perdido: a fórmula de Tartaglia-Cardano pode ser legitimada no corpo dos números *complexos*. Com efeito, essa proeza foi realizada pelo italiano Raphael Bombelli, em 1572, quando percebeu que é perfeitamente possível dar uma explicação para a igualdade

$$4 = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}\,,$$

desde que tenhamos a ousadia de permitir a existência de "números" cujos quadrados sejam reais negativos e, além disso, também permitirmos operar com estes números segundo as regras operacionais do campo dos números reais.

Acompanhe, a seguir, o desenvolvimento feito por Bombelli, onde é aplicada, conforme ele mesmo mencionou, a "ideia louca" de operar com expressões do tipo $a + b\sqrt{-1}$ como se fossem números reais e, desta forma, "destravar" o cálculo das raízes da cúbica $x^3 - 15x - 4 = 0$:

$$\begin{aligned} x &= \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} \\ &= \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}} \\ &= \sqrt[3]{(2 + \sqrt{-1})^3} + \sqrt[3]{(2 - \sqrt{-1})^3} \\ &= (2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4\,. \end{aligned} \tag{9.7}$$

Exercício 263 -

Justifique cada uma das igualdades de (9.7) por meio da "ideia louca" de Bombelli.

Nas próximas seções, usaremos esse desenvolvimento natural como motivação para estabelecer – de forma rigorosa – a construção dos números complexos.

Exercício 264 -

Relativamente à fórmula de Tartaglia-Cardano, que acabamos de descrever:

i). Verifique se a mesma é capaz de calcular soluções reais das cúbicas:
a). $x^3 - 4x + 5 = 0$ *b).* $x^3 - 18x - 35 = 0$ *c).* $x^3 - 15x - 4 = 0$.

ii). Para os casos do item (i) que tiveram resposta afirmativa, decida se existem, ou não, outras soluções reais; caso existam, calcule-as.
Dica: se r *é raiz real de uma equação cúbica de coeficientes reais,* $p(x) = 0$, *então podemos reescrevê-la como* $(x - r)q(x) = 0$, *onde* $q(X)$ *é um polinômio quadrático de coeficientes reais. (Adiante, será demonstrada a versão geral, grau* $n \geqslant 2$, *desse resultado básico do Ensino Médio.)*

Exercício 265 -

Fazendo uso da propriedade de fatoração mencionada no ítem (ii) do exercício anterior, e sabendo que $x = 4$ *é uma solução da equação* $x^3 - 15x - 4 = 0$, *prove que as outras raízes desta equação são:* $-2 + \sqrt{3}$ *e* $-2 - \sqrt{3}$.

9.2 Leitura complementar: um rápido histórico sobre a origem dos números complexos

– Raízes verdadeiras versus raízes falsas

Para que entendamos o que segue, precisamos enfatizar que, desde os gregos e até antes da algebrização da Matemática (o que foi feito por volta de 1630 por René Descartes e seus seguidores), a noção de número real era restrita aos números que expressavam medidas de grandezas geométricas e físicas: era restrita ao que hoje chamamos de *números reais positivos*.

Uma primeira consequência desse ponto de vista era só se permitir equações com coeficientes positivos, o que obrigava a se ter de considerar, para cada grau dado, vários tipos de equações. Por exemplo, eram considerados vários tipos de equações cúbicas: $x^3 + px = q$, $x^3 = px + q$ e $x^3 + q = px$ etc., pois os coeficientes p e q tinham que ser positivos.

Uma segunda consequência desse ponto de vista era que as raízes também tinham que ser buscadas no universo dos números reais positivos. Quando surgiram os primeiros problemas nos quais havia sentido material falar-se em raízes negativas (como ocorre, por exemplo, ao tratarmos de débitos em questões de Contabilidade), passou-se a chamar as raízes positivas de *raízes verdadeiras* e as negativas de *raízes falsas*.

– A crise das Cúbicas Irredutíveis

Essa crise ocorreu entre 1550 e 1600 e, como veremos, os esforços de resolvê-la acabaram fazendo com que os números complexos fossem incorporados ao universo dos números.

Os gregos, principalmente Menaichmos e Archimedes, tinham usado métodos geométricos para resolverem alguns tipos muito particulares de equações cúbicas. Muitos séculos depois, entre 800 e 1100 d.C., vários matemáticos islamitas estudaram famílias bem gerais de cúbicas, sempre com o uso de métodos geométricos, principalmente baseados no uso de cônicas. Desses matemáticos, quem maior sucesso teve foi Omar Khayyami, o qual, por volta de 1 100 d.C., chegou a esboçar uma teoria geral das equações cúbicas e mostrou que existem 13 possíveis tipos delas com raízes verdadeiras.

O próximo acontecimento importante deu-se com a divulgação de uma das mais importantes e influentes enciclopédias de Matemática do Renascimento, a *Summa* do italiano Lucca Pacioli, publicada em 1494. Esse enorme livro resumia toda a matemática conhecida pelos europeus naquela época e, ao tratar da resolução das cúbicas, afirmava que seria impossível resolver $x^3 + px = q$ e $x^3 + p = qx$, onde p e q eram números reais positivos. Essa afirmação acabou funcionando como um verdadeiro desafio para os matemáticos italianos quinhentistas, que passaram a concentrar seus esforços na resolução dessas equações.

Em 1515, Scipio dal Ferro, então professor da Universidade de Bologna, descobriu uma regra, ou procedimento, capaz de resolver as cúbicas do tipo $x^3 + px = q$, onde p e q são reais positivos. Essa regra, traduzida em termos de fórmula e notação modernas, dava para valor da única *raiz verdadeira* (ou positiva) dessa equação:

$$x = \sqrt[3]{\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} + \frac{q}{2}} - \sqrt[3]{\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} - \frac{q}{2}}\,.$$

Anos depois, lá por 1540, Tartaglia conseguiu redescobrir a regra de dal Ferro, bem como uma variante para as cúbicas do tipo $x^3 = px + q$.

Embora dal Ferro e Tartaglia mantivessem em segredo suas descobertas, que eram usadas em desafios e concursos matemáticos, este último deixou vazar informações preciosas a Cardano, que acabou não só redescobrindo as duas regras já conhecidas, como mostrou como resolver qualquer cúbica. Esse trabalho foi tornado público, buscando glória, em seu livro *Artis Magnae, sive de regulis algebraicis* (de 1545, comumente abreviado como *Ars Magna*). Nele, Cardano mostrou como resolver as cúbicas em duas etapas:

- resolução dos tipos básicos de cúbicas (sempre com p e q positivos):
  $x^3 + px = q$
  $x^3 = px + q$
  $x^3 + q = px$;
- redução dos demais tipos de cúbicas de raízes verdadeiras aos três tipos básicos.

Mas o que mais nos interessa aqui é chamar a atenção do seguinte: ao testar seus procedimentos em vários exemplos numéricos, Cardano ficou perplexo ao descobrir que no caso da cúbica $x^3 = 15x+4$, que ele sabia ter a raiz verdadeira $x = 4$, a regra levava ao cálculo de

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}\,,$$

o qual ele não podia reduzir, ou simplificar, de modo a chegar até a raiz desejada $x = 4$. Essas cúbicas paradoxais ele denominou de cúbicas irredutíveis. Estava, assim, instalada a crise que acabou sendo a geradora, quase 30 anos depois de Cardano, dos números complexos.

– Bombelli e a resolução da Crise das Irredutíveis

Em 1572, Raphael Bombelli mostrou como "destravar" o cálculo das raízes em casos de cúbicas irredutíveis –como a $x^3 = 15x + 4$, encontrada por Cardano–, conforme detalhamos anteriormente. Na verdade, Bombelli foi bem mais longe do que realizar o desenvolvimento apresentado anteriormente. Seu livro, *l'Algebra,* inicia introduzindo os números da forma $a+b\sqrt{-1}$ (que ele dizia serem entidades associadas a "uma nova espécie de raízes quadradas"), e então gasta nada menos do que 74 páginas para investigar a álgebra dessas novas grandezas.

9.3 Conceituação de número complexo e suas operações aritméticas

No contexto dos números reais, o símbolo $\sqrt{-1}$ não tem sentido, devendo ser visto como uma tentativa frustrada de busca de um número cujo quadrado vale -1. Pois bem, seguindo a "ideia louca" de Bombelli, atribuiremos a esse símbolo um significado numérico estendido e o denotaremos por i.

Dizemos que dotaremos i de um significado numérico "estendido" pois, embora ele não seja um número real, passaremos a aceitar qualquer tipo de multiplicação e adição envolvendo i e números reais. Exemplificando: passaremos a aceitar como um novo tipo de número listas como $5i$, $1+5i$, $2i+1+5i$, $-3+2i+1+5i$, etc. Mais do que aceitar essas listas, *queremos que elas obedeçam às mesmas propriedades aritméticas básicas que obedecem os números reais: associatividade, comutatividade e distributividade.* Em particular, sempre poderemos escrever qualquer uma dessas listas na forma $a + bi$, com a e b reais.

Exemplo 9.5 -

Como exemplo do novo tipo de algebrismo que estamos introduzindo:

$$\begin{aligned}
&2i + 1 + 5i \overset{comutatividade}{=} \\
&= 1 + 2i + 5i \overset{associatividade}{=} \\
&= 1 + (2i + 5i) \overset{distributividade}{=} \\
&= 1 + (2+5)i \\
&= 1 + 7i,
\end{aligned}$$

e

$$\begin{aligned}
&-3 + 2i + 1 + 5i \overset{comutatividade}{=} \\
&= -3 + 1 + 2i + 5i \overset{associatividade}{=} \\
&= (-3+1) + (2i + 5i) \overset{distributividade}{=} \\
&= -2 + (2+5)i \\
&= -2 + 7i.
\end{aligned}$$

Em geral,

$$(a+bi) + (c+di) = (a+c) + (b+d)i\,.$$

Mais importante é observarmos que podemos multiplicar listas do tipo que acabamos de mencionar. Como estamos aceitando as propriedades da associatividade, comutatividade e distributividade, o produto $(a+bi)\cdot(c+di)$, com a, b, c, d reais, pode ser expandido da seguinte forma natural:

$$\begin{aligned}
&(a+bi)\cdot(c+di) \overset{distributividade}{=} \\
&= (a+bi)c + (a+bi)di \overset{distributividade}{=} \\
&= ac + bic + adi + bidi \overset{comutatividade}{=} \\
&= ac + bci + adi + bdii \overset{distributividade}{=} \\
&= ac + (bc+ad)i + bdii\,.
\end{aligned}$$

Ora, lembremos que a intenção maior disso tudo é nos permitir tratar $i = \sqrt{-1}$ como um número, o que torna natural exigirmos que a multiplicação que estamos introduzindo verifique $ii = -1$. Usando essa convenção, o produto $(a + bi) \cdot (c + di)$ deve ser dado por

$$(a + bi) \cdot (c + di) = ac + (ad + bc)i - bd = (ac - bd) + (ad + bc)i.$$

Tratemos de resumir, e formalizar essas considerações heurísticas. Iniciaremos com a definição formal de números complexos:

Definição 9.6 -

Daremos ao símbolo $\sqrt{-1}$ um significado numérico estendido, fora do campo dos números reais, e o denotaremos por i. O conjunto de todas as expressões da forma

$$a + bi,$$

onde a e b são números reais, será chamado de conjunto dos números complexos *e será denotado por $\mathbb{C}$.*
Considera-se dois números complexos $a+bi$ e $c+di$ como iguais quando, e só quando, valerem as igualdades de números reais $a = c$ e $b = d$.

Consideraremos $a + ib$ como indicando o mesmo número complexo que $a + bi$; isto será útil principalmente quando b for dado por uma expressão complicada.

Mais importante, queremos que os números complexos incluam os números reais como casos particulares. Para conseguir isso, convencionaremos escrever: $a+0i = a$, sempre que $a \in \mathbb{R}$, tendo então:

$$\mathbb{R} \subset \mathbb{C}.$$

Em particular, também escreveremos: $0 + 0i = 0$. Conforme veremos adiante, depois de definirmos adição de números complexos, isso equivale a dizer que o zero dos números reais é o zero dos complexos.

De um modo análogo, também usaremos a abreviação notacional $0 + bi = bi$. Em particular, também escreveremos $0 + 1i = 1i = i$.

Definição 9.7 -

Os números complexos da forma $0 + bi$, com $b \in \mathbb{R}$, são denominados imaginários puros. *O número complexo i é denominado* unidade imaginária

Definição 9.8 -

Dado um número complexo $a+bi$, com $a,b\in\mathbb{R}$, dizemos que:

– *sua* parte real *é a, e escrevemos* $\mathrm{Re}(a+bi)=a$ *;*
– *sua* parte imaginária *é b, e escrevemos* $\mathrm{Im}(a+bi)=b$ *.*

Passemos a tratar da faceta mais importante da "ideia louca" de Bombelli, mostrando que a adição e multiplicação que ela nos leva a introduzir em $\mathbb{C}$ estendem as correspondentes operações em $\mathbb{R}$, e isto de modo que o campo $[\mathbb{C},\,+\,,\,\times\,]$ também tenha uma estrutura de corpo, no qual está imerso o corpo dos números reais. Para tal, iniciaremos definindo formalmente a adição e multiplicação de números complexos.

Definição 9.9 -

A adição e multiplicação de dois números complexos, $a+bi$ e $c+di$, são definidas da seguinte maneira:

$$\begin{aligned}(a+bi)+(c+di)&=(a+c)+(b+d)i\,,\\ (a+bi)\cdot(c+di)&=(ac-bd)+(ad+bc)i\,.\end{aligned}\tag{9.8}$$

Exercício 266 -

Mostre que, identificando o número real r com o número complexo $r+0i$, as operações de adição e multiplicação de números complexos são extensões das de números reais. (*Ou seja: para somarmos ou multiplicarmos números reais, podemos trabalhar no campo dos reais ou no campo dos complexos, o resultado final é sempre o mesmo.*)

Exercício 267 -

Mostre que a operação de multiplicação de números complexos é compatível com a propriedade chave: $i^2=ii=-1$. Em outras palavras, mostre que $i^2=-1$, diretamente da definição (9.8) de multiplicação de números complexos.

Teorema 9.10 (*o corpo dos complexos*) -

O campo dos números complexos, $[\mathbb{C}, +, \cdot]$, *tem o seguinte conjunto de propriedades básicas que lhe dão uma estrutura de corpo. Para todos os* $z, w, v \in \mathbb{C}$:

i). as operações $+$ *(adição) e* $\cdot$ *(multiplicação) são fechadas em todo o* $\mathbb{C}$:
$z + w \in \mathbb{C}$ [*a operação* $+$ *é fechada*]
$z \cdot w \in \mathbb{C}$ [*a operação* $\cdot$ *é fechada*]

ii). associatividade das operações:
$z + (w + v) = (z + w) + v$ [*associatividade da* $+$]
$z \cdot (w \cdot v) = (z \cdot w) \cdot v$ [*associatividade da* $\cdot$]

iii). existência de elemento neutro:
$z + (0 + 0i) = z + 0 = z$ [$0 = 0 + 0i$ *é elemento neutro da* $+$]
$z \cdot 1 = z \cdot (1 + 0i) = z$ [$1 = 1 + 0i$ *é elemento neutro da* $\cdot$]

iv). existência de inverso:
$\exists z' \in \mathbb{C}$, *tal que* $z + z' = 0$. *Com efeito, se* $z = a + bi$:

$$z' = -a - ib\,.$$

[$z' = -a - ib$ *é o simétrico de* $z = a + ib$]
sendo $z \neq 0$, $\exists z^{-1} \in \mathbb{C}$, *tal que* $z \cdot z^{-1} = 1$. *Com efeito, se* $z = a + ib \neq 0$:

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i\,.$$

[z^{-1} *é o recíproco de* z]

v). comutatividade das operações:
$z + w = w + z$ [*comutatividade da* $+$]
$z \cdot w = w \cdot z$ [*comutatividade da* $\cdot$]

vi). distributividade da multiplicação:
$z \cdot (w + v) = z \cdot w + z \cdot v$ [*distributividade da* $\cdot$]

Prova:

A demonstração desses resultados consiste numa mera aplicação de (9.8) e das propriedades do corpo dos reais e fica como um (cansativo) exercício para o leitor.

CQD.

Exercício 268 -

Usando a definição de multiplicação de números complexos e que $0 = 0 + 0i$, *prove que em* $\mathbb{C}$ *continua válida a propriedade: "multiplicando qualquer número por zero obtemos zero". Simbolicamente:* $0 \cdot z = 0, \ \forall z \in \mathbb{C}$.

Exercício 269 -

Quando vimos que o campo dos números racionais forma um corpo, também vimos que esta propriedade estrutural implica automaticamente que a multiplicação tenha a propriedade da integridade (recorde o Exercício 73). Semelhantemente, o fato de os números complexos formarem um corpo proibe existirem divisores de zero neste campo, ou seja: sempre que soubermos que $z, w \in \mathbb{C}$, *e que* $z \cdot w = 0$, *poderemos concluir que ao menos um desses números será igual a zero.*
Pede-se provar esta conclusão diretamente da definição de multiplicação e de igualdade de números complexos.

Exercício 270 -

i). Mostre que o simétrico de todo $z \in \mathbb{C}$ *é único.*
ii). Mostre que o recíproco de todo $z \in \mathbb{C}$ *não nulo é único.*

Vejamos como definir as demais operações aritméticas: a subtração e a divisão.

– Subtração de números complexos
Dados $z, w \in \mathbb{C}$, a diferença $z - w$, se existir, será caracterizada como o único $v \in \mathbb{C}$, tal que $z = v + w$.
Mostremos que ela sempre existe e é dada por $v = z - w = z + w'$, onde w' é o simétrico de w. Com efeito: $v + w = (z + w') + w = z + (w + w') = z + 0 = z$.
Na prática, sendo $z = a + bi$ e $w = c + di$, temos:

$$z - w = (a + bi) + (-c - di) = (a - c) + (b - d)i \,.$$

– Divisão de números complexos
Dados $z, w \in \mathbb{C}$, o quociente de z por w, se existir, será denotado por z/w, e caracterizado como o único $v \in \mathbb{C}$, tal que $z = vw$.
Examinemos as duas possibilidades para w:

– se $w \neq 0$, sabemos que ele tem um único recíproco, w'. Daí, de $1 = ww'$, segue que $z = z \cdot ww' = zw' \cdot w$, de modo que existe o quociente, e ele vale $z/w = zw'$;

– se $w = 0$, teremos $vw = 0$, para todo $v \in \mathbb{C}$; logo, a relação $z = vw = 0$ nunca poderá ser satisfeita quando $z \neq 0$; ao contrário, se $z = 0$, teremos que $0 = z = vw = v \cdot 0$ será satisfeita, mas para infinitas escolhas de v! Conclusão: quando $w = 0$, tanto nos casos $z \neq 0$, como no caso $z = 0$, não existe o quociente z/w.

Podemos resumir isso tudo dizendo que o quociente de $z \in \mathbb{C}$ por $w \in \mathbb{C}$ estará definido quando, e somente quando, tivermos $w \neq 0$, casos em que teremos:

$$\frac{z}{w} = zw^{-1},$$

de modo que, se $z = a + bi$ e $w = c + di \neq 0$:

$$\frac{z}{w} = \frac{a+bi}{c+di} = (a+bi) \cdot \left(\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2} i\right).$$

Na prática, esse resultado é mais cômodo de calcular como:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2}.$$

O próximo passo é tentar estender a ordem dos números reais para todos os números complexos, continuando a ter um corpo ordenado. Nesse sentido, recordemos que um corpo é considerado corpo ordenado quando nele estiver definida uma ordem que seja compatível com as operações de adição e multiplicação. Em particular, a ordem deve ser preservada na multiplicação por números positivos.
O teorema a seguir mostra que nosso objetivo é inatingível em $\mathbb{C}$.

Teorema 9.11 -

É impossível estender a relação de ordem $<$ dos números reais para todos os números complexos e de modo a tornar $[\mathbb{C}, +, \times, <]$ um corpo ordenado.
Mais precisamente, é impossível estender a ordem dos números reais para todos os números de $\mathbb{C}$ e isto de modo que ela seja compatível com a operação de multiplicação. Ou seja, é impossível que a implicação seguinte seja sempre verdadeira para números complexos:

$$z < z' \text{ e } w > 0 \Rightarrow wz < wz'.$$

Prova:

De fato, suponhamos que tenhamos conseguido estender a conhecida ordem $<$ de números reais para todos os números complexos, e isso de modo que a ordem continue compatível com a multiplicação (agora, de números complexos). Então, em particular, comparando i e 0, temos duas alternativas possíveis:

– ou $0 < i$ (isto é, i é positivo)
e então, multiplicando ambos os lados de $0 < i$ por $i > 0$, teríamos que a desigualdade não se altera, pois tal ordem é compatível com a multiplicação:

$$0 \cdot i < i \cdot i \quad \text{ou seja } 0 < -1\,, \text{um absurdo;}$$

– ou $i < 0$ (isto é, i é negativo)
e então, multiplicando ambos os lados desta desigualdade pelo número $-i > 0$ (ele tem de ser positivo pois estamos supondo que $i < 0$), teríamos que a desigualdade não se altera, pois tal ordem é compatível com a multiplicação:

$$1 = i \cdot (-i) < 0 \cdot (-i) = 0, \quad \text{ou seja } 1 < 0\,, \text{um absurdo.}$$

CQD.

Proposição 9.12 -

As potências de i repetem-se periodicamente:

$$i^0 = 1,\ i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1,\ i^5 = i,\ i^6 = -1,\ i^7 = -i, \ldots .$$

Em geral, para cada $n \geqslant 1$ inteiro:

$$i^{4n} = 1, \quad i^{4n+1} = i, \quad i^{4n+2} = -1, \quad i^{4n+3} = -i\,.$$

Exercício 271 -

Prove a Proposição 9.12.

Exercício 272 -

Sem usar o binômio de Newton, determine todos os inteiros $n \geqslant 1$ satisfazendo

$$(2i)^n + (1+i)^n + 16i = 0\,.$$

Exercício 273 -

Ao n variar entre os inteiros positivos, quantos são os diferentes valores da soma $i^n + 1/i^n$?

Exercício 274 (*PUCRS, 1997*) -

Determine o produto dos 20 primeiros termos da progressão geométrica de razão i e primeiro termo igual a 1.

Proposição 9.13 -

O campo dos números complexos é fechado para as chamadas operações racionais. Ou seja: para quaisquer polinômios $p(X)$ e $q(X)$ com coeficientes reais ou mesmo complexos, e para qualquer número complexo z, teremos

$$\frac{p(z)}{q(z)} \in \mathbb{C},$$

desde que seja possível a divisão (ou seja, $q(z) \neq 0\,.$)

Prova:

Como cada um dos polinômios envolve um número finito de adições e de multiplicações, e como soma e produto de números complexos ainda é um número complexo, segue que $p(z)$ e $q(z)$ serão números complexos. Para finalizar a prova, resta observar que, como $q(z) \neq 0$, está bem definida a divisão $p(z)/q(z)$.

CQD.

Exercício 275 -

É importante não banalizarmos o trabalho conceitual que acabamos de desenvolver, no sentido de parecer imediato que as propriedades das operações entre reais continuarão sendo válidas para as operações entre complexos.

Para que possamos melhor apreciar a necessidade dessa cautela, consideremos a ideia de números duais, *os quais são formados acrescentando ao conjunto dos números reais um símbolo δ com o seguinte significado: δ não é nem zero, nem um número real, mas $\delta^2 = 0$. Assim, o conjunto* D *dos números duais é definido como o conjunto das expressões $a + b\delta$, onde $a, b \in \mathbb{R}$; sendo que dois duais $a + b\delta$ e $c + d\delta$ são iguais quando, e só quando, $a = c$ e $b = d$. Posto isso, pede-se:*

i). Descobrir como teríamos de definir adição e multiplicação de números duais, de modo tal que estas operações verifiquem as propriedades de comutatividade, associatividade e distributividade.

ii). Mostrar que nenhum número dual da forma $b\delta$ tem inverso. Conclua daí que, para que possamos fazer a divisão de números duais, não basta que o divisor seja diferente de zero.

iii). Mostrar que, por outro lado, se $c \neq 0$, sempre será possível fazer a divisão de $a + b\delta$ por $c + d\delta$. Nesse caso, determine a expressão do respectivo quociente.

A seguir responda: D é um corpo, ou não?

Exercício 276 -

Verifique se o conjunto dos números duais D introduzido no Exercício 275 é fechado em relação às operações racionais (compare esta questão com a Proposição 9.13).

Antes de encerrarmos esta seção, gostaríamos de salientar que é bastante frequente encontrarmos situações onde a introdução do cálculo com números complexos permite estabelecer um resultado que, em seu enunciado, nada tem a ver com números complexos. Como exemplo, vejamos três resultados da Teoria dos Números.

Exercício 277 -

Cauchy, por volta de 1 830, provou que se multiplicarmos dois inteiros que podem ser escritos como uma soma de quadrados de inteiros, então o produto também pode ser escrito como uma soma de quadrados de inteiros. Simbolica, e mais precisamente:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + cb)^2 \,,$$

onde a, b, c, d são números inteiros.

Pede-se provar esse resultado a partir do cálculo dos produtos $(a + bi)(c + di)$ e $(a - bi)(c - di)$, e a posterior multiplicação dos resultados membro a membro.

Exercício 278 -

Generalizando o resultado anterior, mostre que qualquer produto de somas de quadrados ainda é uma soma de quadrados. Mais precisamente: dado um par de listas de n números inteiros $a_1, a_2, \ldots, a_n$ e $b_1, b_2, \ldots, b_n$, mostre que existem inteiros x e y tais que

$$(a_1^2 + b_1^2) \cdot (a_2^2 + b_2^2) \cdots (a_n^2 + b_n^2) = x^2 + y^2 \,.$$

Exercício 279 -

Karl F. Gauss, por volta de 1830, introduziu o conjunto dos inteiros gaussianos, *o qual é formado pelos números complexos da forma $a+bi$, com a e b inteiros. O principal uso desses números complexos ocorre no estudo dos números primos. Por exemplo, eles nos permitem investigar a possibilidade de escrevermos números primos como a soma de dois quadrados. Com efeito, note que os primos da forma $4n+1$ – com n natural não nulo, tais como 5, 13, 17, ... – podem ser fatorados com inteiros gaussianos:*

$$5=(1+2i)(1-2i)=1^1+2^2\,,\quad 13=(3+2i)(3-2i)=3^2+2^2,\ldots\,.$$

Tendo isso em vista, pede-se provar que nenhum primo da forma $4n+3$ é a soma de dois quadrados de inteiros.

9.4 Leitura complementar: a crise da legitimidade dos números complexos

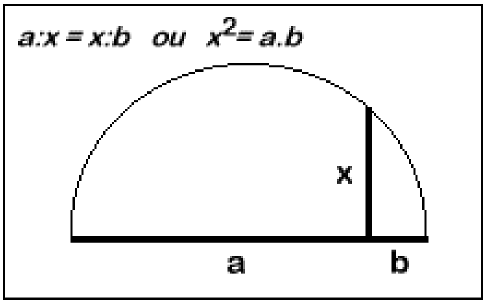
Se por um lado Bombelli resolveu a Crise das Cúbicas Irredutíveis, por outro lado o modo artificioso e algébrico com que introduziu os números complexos acabou produzindo uma crise ainda maior, que denominaremos *Crise da Legitimidade*. Com efeito, como a matemática da época era toda fundamentada na Geometria Euclidiana, os números complexos só poderiam ser legitimamente vistos como um novo tipo de grandeza se fosse apresentada uma *teoria geométrica* para eles.

Isso significava dizer que era preciso provar que os números complexos podiam ser interpretados como objetos geométricos e que – muito importante – era possível estender a teoria das proporções contida nos *Elementos* de Euclides para eles.

Em outras palavras, a Crise da Legitimidade pedia muito mais do que achar uma mera interpretação geométrica para os números complexos, mesmo que se mostrasse útil na visualização das operações aritméticas com esses, bem como na visualização das soluções de equações e inequações. Naquela época era preciso muito mais do que isso: era preciso construir uma *teoria geométrica* para esses números!

A denúncia da existência de uma crise ocorreu com o próprio Cardano. Imediatamente depois que Bombelli publicou sua *Algebra,* Cardano, então com 72 anos, reagiu violentamente com um panfleto intitulado *Sermo de plus et minus*, no qual ele condenava o uso dos números complexos. Contudo, a vasta maioria dos matemáticos da época manteve uma atitude de "distância prudente". Essa maioria, muito a contragosto, apenas tolerava o uso das *grandezas imaginárias e sofísticas* para estabelecer propriedades das grandezas geométricas ou números reais, e torcia para que esses inconvenientes intermediários oportunamente fossem "chutados para a lata de lixo da História".

A primeira tentativa de resolução da Crise da Legitimidade ocorreu só cem anos depois da *Algebra* de Bombelli, quando o inglês John Wallis publicou, em 1673, seu livro *De Algebra Tractatus, Historicus e Practicus.* Nele, Wallis partiu do procedimento tradicional da construção da média proporcional x entre dois segmentos de medidas a e b, resumido na figura que se segue; esta média x verifica a proporção $a : x = x : b$, de modo que sua determinação equivale a resolver a equação $x^2 = ab$.



Wallis interpretou a proporção $+1 : x = x : -1$ como "dizendo" que $\sqrt{-1}$ é a média proporcional entre $+1$ e -1, e que $\sqrt{-1}$ deve ser interpretado como a medida de um segmento ortogonal a dois segmentos de sentidos opostos e de "medidas" respectivamente iguais a $+1$ e -1.

Infelizmente, fracassou redondamente no passo seguinte, o da interpretação dos números imaginários puros $b\sqrt{-1}$, ou bi. Essa interpretação, que seria fácil hoje, na época de Wallis era dificultada pela natureza ainda imatura da interpretação geométrica dos números negativos. Com efeito, em vez de Wallis concluir que os números $b\sqrt{-1}$ podem ser interpretados como medidas de segmentos no eixo de $\sqrt{-1}$ e, então, ortogonais ao eixo dos segmentos reais, ele concluiu que eles fariam um ângulo variável com este eixo, de acordo com o valor de b. Como consequência, ele nem conseguiu interpretar geometricamente a soma de dois números complexos, tendo de interromper sua tentativa.

Como veremos, as próximas tentativas de resolução da crise só surgiram cem anos depois de Wallis, lá por cerca de 1800. Nesses mais de duzentos anos que se passaram desde Bombelli, a Crise da Legitimidade acabou aumentando, se desdobrando em duas componentes: a *componente geométrica,* já caracterizada anteriormente, e a *componente operacional.* A crise da legitimidade operacional foi formada à medida que alguns matemáticos mais destemidos, incorporando o uso dos números complexos na base do "ide adiante que a fé aumentará", passaram a encontrar alguns resultados paradoxais e contraditórios.

Dentre esses resultados operacionais, o que mais polêmicas provocou foi descoberto em cerca de 1715. Partindo-se de $0 = \log 1 = \log(1^2) = \log((-1)^2)$, se deduziu que $0 = 2\log(-1)$, e daí que $\log(-1) = 0$, o que era contraditório com o valor $\log(-1) = \pi i$, que se obtém tomando $x = \pi$ na então já conhecida fórmula de Côtes: $\log(\cos x + i \operatorname{sen} x) = xi$. Estava criada a famosa *Controvérsia dos Logaritmos de Números Negativos*, a qual durou décadas e envolveu grandes matemáticos da época, como G. W. Leibniz, Johann Bernoulli, Jean d'Alembert e Leonhard Euler; um formidável elenco de nomes que por si só já é suficiente para mostrar o estado confuso das ideias acerca de números complexos naquela época.

Mas, não apenas operações transcendentais produziram paradoxos. Por volta de 1740, d'Alembert, ao trabalhar com radiciação de números complexos, muito se debateu com as igualdades

$$\begin{aligned}\sqrt{6} &= \sqrt{(-2)(-3)}\\ &= \sqrt{-1}\sqrt{2}\sqrt{-1}\sqrt{3}\\ &= i\sqrt{2}i\sqrt{3}\\ &= i^2\sqrt{6} = -\sqrt{6}\,.\end{aligned}$$

Todos esses resultados paradoxais reforçavam a suspeita associada à componente geométrica da crise. Cada novo resultado paradoxal que surgia funcionava como uma crítica: "Viu? Não disse que isso não tem sentido?".

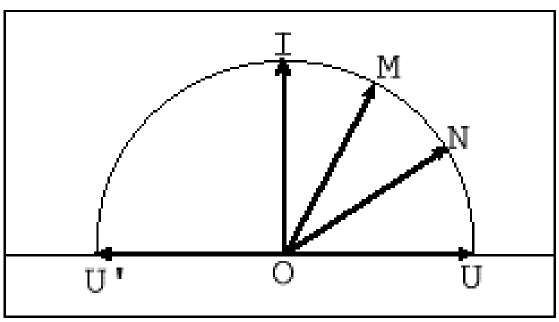
Componentes da Crise da Legitimidade	$\nearrow$	geométrica (solução: Argand, François, Mourey)
	$\searrow$	operacional (solução: Euler, Riemann, Ohm)

Adiante examinaremos alguns aspectos da componente operacional da Crise da Legitimidade, sendo que, por enquanto, nos limitaremos a expor algumas ideias básicas do trabalho que mais contribuiu para se resolver a componente geométrica dessa crise. Trata-se de uma pequena monografia de cerca de 80 páginas que o contador suiço Jean Robert Argand publicou em Genebra, em 1806: *Essai sur une manière de representer les quantités imaginaires dans les constructions géométriques.*

Em sua monografia, Argand conseguiu estender a tradicional teoria das proporções da Geometria Euclidiana para o que ele chamou de *grandezas dirigidas*. Essas nada mais eram do que o que hoje chamamos de vetores complexos e poderíamos chamar de segmentos orientados, sendo que ele explorava a existência de uma correspondência biunívoca entre estes vetores e os números complexos.

Podemos dizer que a extensão de Argand foi feita em três etapas. Ele inicia a primeira etapa interpretando os números reais como vetores sobre o eixo horizontal, onde o sentido positivo de orientação e a unidade de medida são dados por um vetor unitário $\overrightarrow{OU}$. Os números positivos são vistos como vetores de mesmo sentido que $\overrightarrow{OU}$ e os negativos como vetores de sentido oposto a este vetor unitário $\overrightarrow{OU}$. A seguir, ele estende a tradicional teoria das proporções de modo a incluir todos os números reais, inclusive os negativos. Em particular, ele dá interpretação para as proporções básicas $+1 : +1 = -1 : -1$ e $+1 : -1 = -1 : +1$, observando que elas seguem um mesmo padrão: quando os termos extremos (a e d em $a : b = c : d$) têm sinais opostos, o mesmo ocorre com os termos médios (c e d em $a : b = c : d$), e quando os termos extremos têm o mesmo sinal, o mesmo ocorre com os termos médios.

Na segunda etapa de seu trabalho, Argand trata de *achar uma interpretação de* $\sqrt{-1}$ *como segmento orientado.* Para tal, semelhantemente ao que tinha feito Wallis, ele inicia observando que a igualdade $x^2 = -1$ podia ser interpretada como dizendo que x é a média proporcional entre $+1$ e -1, ou seja: $+1 : x = x : -1$. A seguir, ele observa que essa última proporção não obedece ao padrão apresentado, pois os seus extremos, $+1$ e -1, têm sinais opostos, enquanto os termos médios, x e x, têm o mesmo sinal. Logo, é impossível que x represente a medida de um segmento no eixo horizontal, dos números reais. Para resolver o impasse, ele passa para o plano e interpreta a clássica construção euclidiana para determinação de médias proporcionais em termos de segmentos orientados. Relativamente à construção mostrada na figura a seguir, ele afirma que $\overrightarrow{OU} : \overrightarrow{OI} = \overrightarrow{OI} : \overrightarrow{OU'}$, pois essa proporcionalidade



vale tanto em termos dos comprimentos destes vetores quanto em termos de direções: o ângulo entre $\overrightarrow{OU}$ e $\overrightarrow{OI}$ é igual ao ângulo entre $\overrightarrow{OI}$ e $\overrightarrow{OU'}$. Evidentemente, ele passa a considerar o segmento orientado $\overrightarrow{OI}$ como a unidade i dos números complexos.

Na terceira etapa de sua extensão, Argand inicia mostrando que podemos inserir tantas médias proporcionais quantas quisermos entre as grandezas dirigidas, o que equivale a construir direções de ângulos $k\pi/2^n$. Feito isso, ele conclui que podemos indicar qualquer grandeza dirigida como um vetor de origem em O, caracterizado por seu comprimento e seu ângulo com o vetor unitário horizontal, $\overrightarrow{OU}$. Isso leva a duas representações de suas grandezas dirigidas, uma corresponde ao que chamamos de representação binomial $a + bi$, e a outra corresponde ao que chamamos de representação exponencial ou fasorial $\rho e^{i\theta}$. Finalmente, ele chega ao momento crítico de definir a razão $\overrightarrow{OM} : \overrightarrow{ON}$ entre duas grandezas dirigidas quaisquer, $\overrightarrow{OM}$ e $\overrightarrow{ON}$, o que ele faz definindo tanto a grandeza ou magnitude desta razão (dada pelo quociente entre seus comprimentos), como sua direção (dada pelo ângulo entre $\overrightarrow{OM}$ e $\overrightarrow{ON}$).

Com isso, finalmente, e depois de muito tempo, estava-se em condições de falar em proporções entre grandezas dirigidas, ou números complexos, quaisquer:

$$\overrightarrow{OM} : \overrightarrow{ON} = \overrightarrow{OP} : \overrightarrow{OQ}\,.$$

Como a monografia de Argand foi impressa às suas próprias custas, ela teve uma pequeníssima tiragem, coisa de menos de cem exemplares. Além disso, Argand esqueceu-se de colocar seu nome na capa do livro! Não fosse Jacques François, professor de matemática da École Impérial d 'Artillerie, em Paris, certamente suas ideias teriam passado desapercebidas pela comunidade. Com efeito, em 1813, quando Argand já tinha 50 anos, François publicou um trabalho, *Nouveaux principes de Géometrie de position et interpretation géométrique des symboles imaginaires,* onde divulgou as ideias de Argand, apresentou várias aplicações interessantes delas e dizia que tinha se baseado num livro do qual não podia se saber quem era o autor. Como o trabalho de François tinha sido publicado num jornal importante, no mesmo ano Argand acabou sabendo dele e identificou-se como o tal autor desconhecido, enviando a este jornal um resumo melhorado de sua monografia. Nos quatro anos seguintes, publicou na França vários outros artigos sobre números complexos, tornando-se um matemático bastante respeitado.

O toque de acabamento final nessas ideias foi dado por C. V. Mourey, ao publicar, em 1828, um livro de bastante sucesso, *La vrai théorie des quantités négatives et des quantités prétendues imaginaires.* Nesse, Mourey reescreveu as ideias de Argand de um modo muito mais rigoroso e num estilo bastante semelhante ao que hoje usamos, inclusive insistindo na definição estritamente geométrica da soma e produto de números complexos, bem como no estudo das propriedades destas operações, tais como sua associatividade, distributividade, etc.

Com isso – bem como com a publicação de trabalhos menores por Buée, Warren e outros –, por volta de 1830, o matemático mais respeitado da época, Karl F. Gauss, achou que, em vez de publicar mais uma justificativa geométrica para os números complexos, como ele há vários anos vinha prometendo, nada mais precisava ser feito, a não ser proclamar a derrota da Crise da Legitimidade. Assim, em 1831, num muito importante trabalho, *Teoria dos Resíduos Quadráticos*, e com todo o peso de sua autoridade científica, Gauss escreveu:

> "Fazia muito tempo que as quantidades imaginárias estavam baseadas na ficção, não sendo plenamente aceitas na Matemática e vistas como uma coisa a ser tolerada; elas estavam longe de ter o mesmo status que as quantidades reais. Agora não há mais justificativa para tal discriminação, uma vez que a metafísica dos números imaginários está plenamente esclarecida, e que se provou que eles têm um significado tão real quanto os números negativos".

A bem da verdade, di ga-se que a construção de uma teoria geométrica para os números complexos, bem de acordo com a tradição euclidiana, não foi a única responsável pelo término do preconceito que sofriam. Também muito contribuiram a importância de vários resultados estabelecidos usando números complexos pelo próprio Gauss (como o Teorema Fundamental da Álgebra e resultados sobre números primos), por Niels Abel e Carl Jacobi – acerca das chamadas integrais elípticas –, por Augustin Cauchy – sobre holomorfia e integração das funções da variável complexa –, bem como a resolução completa das dificuldades com a avaliação e manipulação dos radicais, logaritmos, exponenciais e funções trigonométricas, por Cauchy, Bernhard Riemann e Martin Ohm.

Enfim, lá por cerca de 1850, não havia mais nenhuma dúvida sobre a legitimidade dos números complexos, e estava bem clara sua importância fundamental no estudo da Matemática. Em particular, a denominação original –números sofísticos– foi totalmente abandonada e substituída pela denominação atual –números complexos– que havia sido introduzida por Gauss. Também foi abandonado o costume de se escrever esses números como $a + b\sqrt{-1}$ em favor da atual notação $a + bi$, que havia sido introduzida por Euler e adotada por Gauss. Incidentalmente, esta última troca estava motivada pela intenção de se procurar dissociar a noção de número complexo das propriedades operacionais dos radicais. Passou-se a preferir $ii = -1$ em vez de $\sqrt{-1}\sqrt{-1} = -1$.

Curiosamente, em paralelo com os esforços de Argand e companheiros, estava ocorrendo um desenvolvimento extremamente importante para a Matemática em geral, que acabou mostrando que todo esse trabalho não era realmente decisivo. Com efeito, naquela época foram descobertos pelo húngaro János Bolyai e pelo russo Nicholau Lobachevsky os primeiros exemplos de *geometrias não-euclidianas.* Inicialmente elas foram recebidas com suspeita, dado o caráter dominador e exclusivista que tinha a Geometria Euclidiana. Contudo, em 1868, Eugenio Beltrami provou que essas novas geometrias eram tão rigorosas e livres de contradição quanto a Geometria Euclidiana.

Com isso, os matemáticos convenceram-se de que os fundamentos da Matemática não podem se resumir às verdades da Geometria Euclidiana. Como decorrência, a teoria das proporções foi abandonada em favor da construção dos números reais a partir dos números racionais, e a dos números complexos a partir dos reais, como passou a ser feito por Weierstrass, Dedekind, Méray, Peano, etc.

Para encerrar estas observações acerca da dramática aceitação dos números complexos, precisamos mencionar que, em 1813, travou-se uma grande polêmica sobre a melhor maneira de se chegar a uma legitimação dos números complexos. De um lado estavam Argand e Jacques François, e do outro estava o matemático francês F. Servois. Este último acabou iniciando uma campanha em defesa de uma fundamentação estritamente algébrica para os números complexos. Os primeiros resultados sob esse ponto de vista, curiosamente, foram escritos simultaneamente por János Bolyai (em um outro trabalho, o *Responsito,* cujo título pode ser traduzido do latim como "Consultando" – trata-se de um texto encontrado entre as 14.000 páginas de matemática deixadas sem publicar por Bolyai, e que só foi divulgado em 1899, por Stäckel) e pelo irlandês William Hamilton (*Theory of conjugate functions, or algebraic couples,* publicado no Trans. Irish Academy). Tanto Bolyai quanto Hamilton introduziram os números complexos como pares ordenados de números reais. Seguiu-se um importante trabalho de Augustin Cauchy (publicado em 1847, num livro de grande sucesso: *Exercises d'Analyse*) que tratava os números complexos como classes de polinômios. Tanto a abordagem de Bolyai-Hamilton como a de Cauchy são muito populares, atualmente.

In tempo. É preciso insistir que a ocorrência do que denominamos Crise da Legitimidade dos números complexos está fortemente ligada aos valores de uma época, quando a aceitação e relevância de qualquer construção matemática ainda eram muito dependentes de uma validação "concreta" desta construção. Em outras palavras, considerava-se que os conceitos e construções da Matemática deveriam ser, indispensavelmente, a "tradução" de fatos observáveis no mundo físico.

Com o tempo, esse paradigma matemático acabou tornando-se insustentável; entre outras razões, por ficar cada vez mais evidente, na prática científica, a inviabilidade de se dispor de um "mundo real", único, subjacente a qualquer experiência científica. Na Matemática do nosso tempo, é considerado preponderantemente o *valor intrínseco* de cada problema matemático (valor este decidido pela própria comunidade matemática) e as pesquisas em Matemática se desenvolvem muito mais por esta do que por qualquer outra razão.

9.5 Representações analíticas dos números complexos

A definição dos números complexos como objetos do tipo $z = a + bi$, com a e b reais, sugere uma correspondência óbvia entre esses números e o conjunto de pares ordenados (a, b) de números reais:

$$a + bi \longleftrightarrow (a, b). \tag{9.9}$$

Considerando a relação de igualdade a que estão submetidos os complexos (a saber: $a + bi = c + di \iff a = c$ e $b = d$), bem como a similar relação de igualdade existente entre pares ordenados, fica evidente que a correspondência (9.9) entre $\mathbb{C}$ e $\mathbb{R} \times \mathbb{R}$ é biunívoca. Esse fato permite uma identificação entre os números complexos e o conjunto de pares ordenados de números reais, e permite ainda expressar as operações de adição, multiplicação, etc. de números complexos em termos de pares ordenados. Com efeito, tem-se

$$(a, b) \oplus (c, d) = (a + b, c + d) \tag{9.10}$$

$$(a, b) \odot (c, d) = (ac - bd, ad + bc). \tag{9.11}$$

Exercício 280 -

i). Certifique-se de que a adição e a multiplicação de pares ordenados de reais, determinadas pela correpondência (9.9), são dadas, de fato, por (9.10) e (9.11).

ii). Por meio da mesma correspondência, obtenha a expressão da divisão de números complexos na forma de pares ordenados, ou seja, obtenha a expressão de

$$\frac{(a, b)}{(c, d)},$$

quando $(c, d) \neq (0, 0)$.

Os pares ordenados de números reais, com as operações de adição e multiplicação definidas anteriormente, permitem uma outra visualização dos complexos e de suas operações, constituindo a chamada *representação cartesiana* dos números complexos. Costuma-se chamar de *representação binomial* a expressão usual $z = a + bi$ de um número complexo. A representação cartesiana foi introduzida, independentemente, por János Bolyai e William R. Hamilton, por volta de 1840 e, na verdade, não passa de uma "troca de roupagem" da representação binomial.

A representação cartesiana não tem muita utilidade, preferindo-se trabalhar com a representação binomial. No entanto, como veremos adiante, ambas se mostram desajeitadas para a realização de muitos cálculos, tais como os que envolvem radiciação e potenciação. Assim, mais do que conveniente, é necessário termos à mão representações alternativas, como a *representação trigonométrica* ou *polar*:

$$z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$$

e a *representação exponenencial* ou *fasorial*:

$$z = \rho e^{i\theta}\,.$$

Infelizmente, teremos que deixar para um texto mais avançado o estudo de tais representações alternativas, uma vez que elas necessitam do conhecimento de Trigonometria e da prova de um dos resultados mais importantes da Matemática: o Teorema de Euler, que afirma

$$e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta.$$

Vale a pena insistir que, ao nos limitarmos ao estudo das formas binomial e cartesiana, ficaremos incapazes de resolver muitos problemas básicos que ocorrem na própria teoria dos números complexos, bem como de abordar um sem número de aplicações nas ciências e na tecnologia.

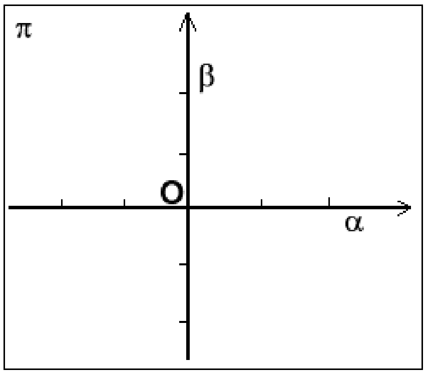
Deixamos para discutir a *representação vetorial* dos números complexos para a próxima seção, pois ela está relacionada com a representação geométrica dos mesmos.

9.6 Representações geométricas dos números complexos

O que segue é uma abordagem básica e rápida dos aspectos mais elementares da interpretação geométrica dos números complexos. Iniciaremos com a definição de sistema de coordenadas cartesianas do plano. Para melhor entendê-la, recomendamos que o leitor revise a primeira seção do Capítulo 7.

Definição 9.14 -

Um sistema cartesiano de eixos *do plano euclidiano (que denotaremos por π) consiste de dois eixos perpendiculares de π interceptando-se num ponto O, o qual é a origem de ambos. É tradicional, mas não obrigatório, que a unidade de medida desses eixos seja a mesma, e que eles tenham uma orientação relativa como mostrada na figura que segue.*[2]



Por plano cartesiano *entenderemos o plano euclidiano π, munido de um sistema cartesiano de eixos.*

Todo sistema de eixos determina um sistema de coordenadas cartesianas do plano euclidiano, entendendo-se por isso a seguinte correspodência biunívoca entre os pontos deste plano e o conjunto $\mathbb{R} \times \mathbb{R}$ dos pares ordenados de números reais:

- Dado um ponto $P \in \pi$, a paralela a β que passa por P intersepta o eixo α num ponto P',[3] cuja abscissa (relativamente ao eixo α), a, será denominada *abscissa de P*; por sua vez, a paralela a α que passa por P intersepta o eixo β num ponto P'', cuja abscissa (relativamente a β), b, será denominada *ordenada de P*. Desse modo, a cada ponto $P \in \pi$, associamos unívocamente um par ordenado de números reais: $(a, b) \in \mathbb{R} \times \mathbb{R}$. Os números a e b são denominados coordenadas cartesianas de P.

[2]Note que, para fazer o eixo α coincidir com β, precisamos girar α de 90° no sentido anti horário, ou sentido trigonométrico positivo, por isso dizemos que temos um sistema de eixos com orientação positiva; nada impede, contudo, que considerássemos um sistema com orientação negativa: ou seja, α tendo de girar 90° no sentido horário, para coincidir com β.

[3]Quem garante a existência dessa intersecção é a continuidade do plano euclidiano.

- Reciprocamente, dado um par $(a, b) \in \mathbb{R} \times \mathbb{R}$, usando o Teorema Fundamental da Geometria Analítica, localizamos um ponto $P' \in \alpha$, cuja abscissa (relativamente ao eixo α) seja a, e localizamos um ponto $P'' \in \beta$, cuja abscissa (relativamente a β) seja b. A perpendicular a α que passa por P' e a perpendicular a β que passa por P'' interceptam-se num único ponto P do plano euclidiano. Costuma-se escrever $P = P(a, b)$.

Devido a existência dessa correspondência, o eixo α de um sistema cartesiano de eixos é denominado **eixo das abscissas**, e β **eixo das ordenadas**.

O resultado que segue resume essas considerações.

Teorema 9.15 (*Teorema Fundamental da Geometria Analítica Plana*) -

Todo sistema cartesiano de eixos determina uma correspondência biunívoca entre π (o conjunto dos pontos do plano cartesiano) e $\mathbb{R} \times \mathbb{R}$ (o conjunto dos pares ordenados de números reais):

$$\pi \quad \overset{\text{sist.eixos}}{\longleftrightarrow} \quad \mathbb{R} \times \mathbb{R} .$$

Feitas essas preliminares, voltemos aos números complexos e tratemos de interpretá-los geométricamente.

Definição 9.16 -

A ***representação pontual*** *de um número complexo, $a + bi$, é o ponto do plano cartesiano que tem coordenadas (a, b).*

Observação 9.17 -

Observe que essa representação pontual depende, crucialmente, da escolha de um sistema cartesiano de eixos no plano euclidiano. Para que possamos nos lembrar dessa escolha, sempre que estivermos trabalhando com números complexos, passaremos a denominar o plano cartesiano de ***plano de Argand***.[4]

Com o conceito de representação pontual, podemos reescrever o último teorema:

[4] A associação com o nome de Argand serve apenas para ressaltar que estamos no contexto de números complexos. Em seus trabalhos, Argand nunca usou coordenadas cartesianas.

Teorema 9.18 -

Se a cada número complexo $a+bi$ associarmos sua representação pontual (a,b), estabeleceremos uma correspondência biunívoca entre o conjunto $\mathbb{C}$ dos números complexos e o plano de Argand.

Definição 9.19 -

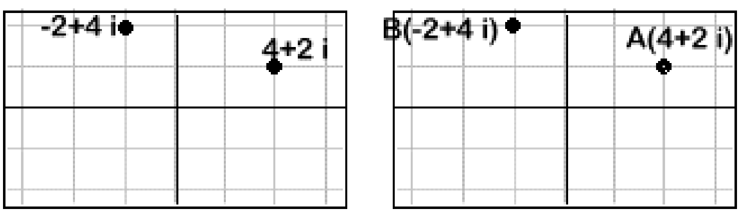
O eixo das abscissas do plano de Argand é denominado eixo real *deste plano, e o eixo das ordenadas é denominado* eixo dos imaginários puros.

Observação 9.20 -

Formalmente, temos as seguintes associações:

$$a+bi \in \mathbb{C} \longleftrightarrow (a,b) \in \mathbb{R}\times\mathbb{R} \longleftrightarrow P = P(a,b) \in \text{Argand}\,.$$

Contudo, embora $a+bi$, (a,b) e $P(a,b)$ sejam objetos matemáticos bem distintos –um número, um par e um ponto–, as correspondências biunívocas envolvidas permitem identificá-los, o que é uma prática comum, pois torna o trabalho mais simples, menos "pesado".
Essa identificação foi usada na figura a seguir, à esquerda, para representar pontualmente os números $4+2i$ e $-2+4i$; na figura à direita, temos uma notação mais precisa, indicando que A é o ponto representando $4+2i$, e B o ponto associado a $-2+4i$.



Resumo

– Planos que consideramos:

- plano euclidiano
- plano cartesiano
  = plano euclidiano + sistema de coordenadas cartesianas
- plano de Argand
  = plano euclidiano + sistema de coordenadas cartesianas + identificação pontual dos números complexos.

– Correspondências biunívocas que consideramos:

$$a + bi \in \mathbb{C} \longleftrightarrow (a, b) \in \mathbb{R} \times \mathbb{R} \longleftrightarrow P = P(a, b) \in \text{Argand}\,.$$

Passemos à uma segunda interpretacão geométrica muito utilizada dos números complexos, a chamada representação vetorial. A mesma estabelecerá uma biunivocidade entre os números complexos e os vetores do plano de Argand. Para tal, iniciaremos recordando o conceito de vetor do plano.

Indiquemos por O a origem do sistema de coordenadas do plano de Argand. Dado qualquer ponto P desse plano:

- caso $P \neq O$, escolhendo como sentido de percurso do segmento de reta OP o que vai de O para P, o segmento orientado resultante é o que chamamos de vetor de extremidade P, e que denotamos por $\overrightarrow{OP}$;

- caso $P = O$, o segmento de reta OP se reduz ao ponto O e, por extensão, é dito determinar o vetor nulo do plano, o qual é denotado por $\overrightarrow{OO}$.

O módulo do vetor $\overrightarrow{OP}$ é o comprimento do segmento de reta OP, e é denotado por $|\overrightarrow{OP}|$. Evidentemente, o vetor nulo tem módulo zero: $|\overrightarrow{OO}| = 0$.

Definição 9.21 -

Indiquemos por O a origem do sistema de coordenadas do plano de Argand. Para cada número complexo $z = a+bi$, indiquemos por $Z = (a, b)$ o correspondente ponto no plano de Argand. Dizemos que o vetor $\overrightarrow{OZ}$ é a representação vetorial do número complexo z.

As figuras apresentadas a seguir resumem e comparam os dois tipos de representação geométrica dos números complexos que introduzimos:

Definição 9.22 -

O módulo do número complexo z é denotado por $|z|$, e definido como sendo o módulo do vetor complexo que o representa.

Teorema 9.23 -

O módulo do número complexo $z = a + bi$ é dado por

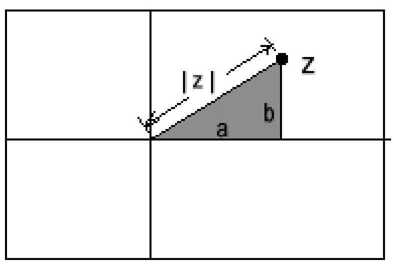
$$|z| = \sqrt{a^2 + b^2}\,,$$

o que pode ser reescrito como

$$|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}\,.$$

Prova:

É uma imediata aplicação do Teorema de Pitágoras (veja figura a seguir). CQD.



Exercício 281 -

Mostre que o módulo de um número real visto como número complexo coincide com o valor absoluto deste número. (Isto justifica utilizarmos a mesma notação para valor absoluto e módulo.)

Observação 9.24 -

Como $|i| = 1$, *fica justificada a denominação* unidade imaginária *introduzida por Gauss em 1831, no seu histórico trabalho Teoria dos Resíduos Quadráticos.*

Exercício 282 -

Mostre que, para cada número complexo z, *tem-se:*

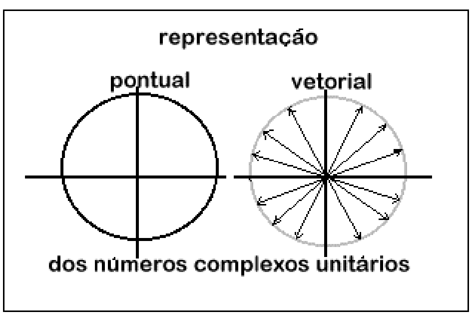
i). $|z| = 0$, *quando, e só quando,* $z = 0$;
ii). $|\operatorname{Re} z| \leqslant |z|$, *e a igualdade vale quando, e só quando,* z *for real;*
iii). $|\operatorname{Im} z| \leqslant |z|$, *e a igualdade vale quando, e só quando,* z *for imaginário puro.*

Exemplo 9.25 -

Nas mais diversas disciplinas, é muito importante o conjunto

$$U = \{z \in \mathbb{C},\ |z| = 1\}$$

dos números complexos de módulo unitário. Infelizmente, sua importância só pode ser melhor explicitada quando temos em mãos a representação trigonométrica dos números complexos. A representação pontual dos elementos do conjunto U *consiste do círculo unitário centrado em* O. *Por sua vez, a representação vetorial dos elementos de* U *consiste de todos os vetores complexos de comprimento um. Confira nas figuras a seguir.*



Proposição 9.26 -

Sendo z e w dois números complexos, então:

i). $|z.w| = |z||w|$ *;*
ii). se w é não nulo,

$$\left|\frac{z}{w}\right| = \frac{|z|}{|w|}\,.$$

Prova:

Para (i).
Adiante, com a noção de conjugado de um número complexo, poderemos dar uma prova mais rápida e simples para essa igualdade. No momento, temos que nos limitar ao uso da definição de módulo e explorar o fato de que basta mostrar que

$$|z.w|^2 = |z|^2|w|^2,$$

uma vez que todos os fatores envolvidos são números positivos. Ora, sendo $z = a+bi$ e $w = c+di$, temos

$$zw = (ac-bd)+(ad+bc)i,$$

e então

$$\begin{aligned}|z.w|^2 &= (ac-bd)^2+(ad+bc)^2\\ &= a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2\\ &= a^2(c^2+d^2)+b^2(c^2+d^2)\\ &= (a^2+b^2)(c^2+d^2)\\ &= |z|^2|w|^2\,.\end{aligned}$$

Para (ii).
Como podemos escrever $z = w(z/w)$, por *(i)* segue que

$$|z| = |w|\left|\frac{z}{w}\right|,$$

logo

$$\frac{|z|}{|w|} = \left|\frac{z}{w}\right|.$$

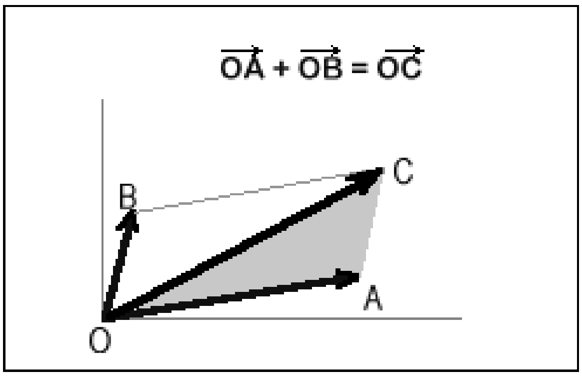
CQD.

9.7 Interpretação geométrica da adição e da multiplicação de números complexos

Começaremos definindo a adição de vetores, o que é assunto bem familiar para quem já estudou a composição de forças em Física:

Definição 9.27 -

A soma de dois vetores complexos, $\overrightarrow{OA}$ e $\overrightarrow{OB}$, é o vetor denotado por $\overrightarrow{OC} = \overrightarrow{OA} + \overrightarrow{OB}$, e determinado deslocando paralelamente $\overrightarrow{OB}$, de modo que sua origem venha coincidir com a extremidade A de $\overrightarrow{OA}$; o ponto C é a extremidade do vetor deslocado. Nos casos em que $\overrightarrow{OA}$ e $\overrightarrow{OB}$ não são colineares, também podemos ver $\overrightarrow{OC}$ como determinado pela diagonal do paralelogramo que tem como lados os segmentos OA e OB, conforme a figura a seguir.



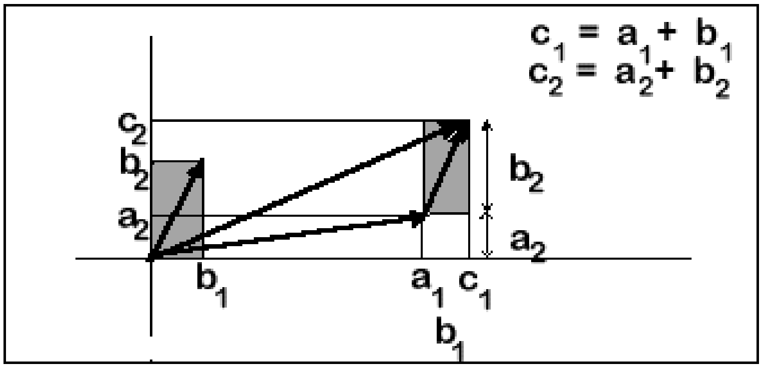
Teorema 9.28 -

A adição de números complexos corresponde à adição dos vetores complexos associados a esses números. Mais precisamente: dados quaisquer dois números complexos z e w, a soma $z + w$ tem como representação vetorial o vetor $\overrightarrow{OC}$, dado por $\overrightarrow{OC} = \overrightarrow{OA} + \overrightarrow{OB}$, onde $\overrightarrow{OA}$ é a representação vetorial de z , e $\overrightarrow{OB}$ é a representação vetorial de w.

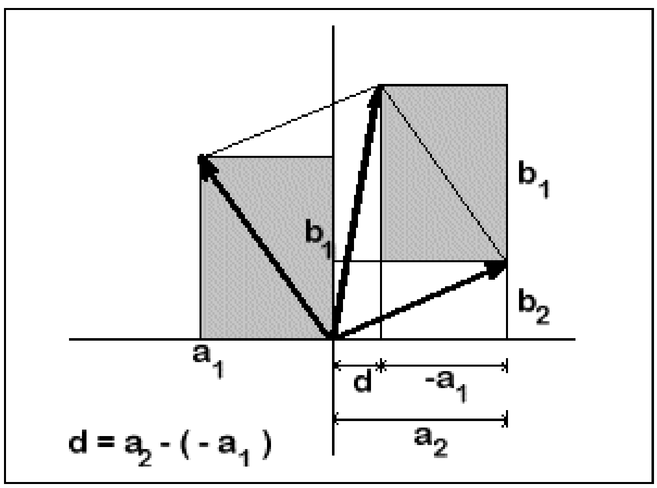
Prova:

Sendo $z = a_1 + b_1 i$ e $w = a_2 + b_2 i$, temos a seguir uma demonstração geométrica dividida em casos, cada um deles ilustrado por uma figura e que são complementados pelo Exercício 283. Pede-se ao leitor completar a demonstração por meio da resolução deste exercício.

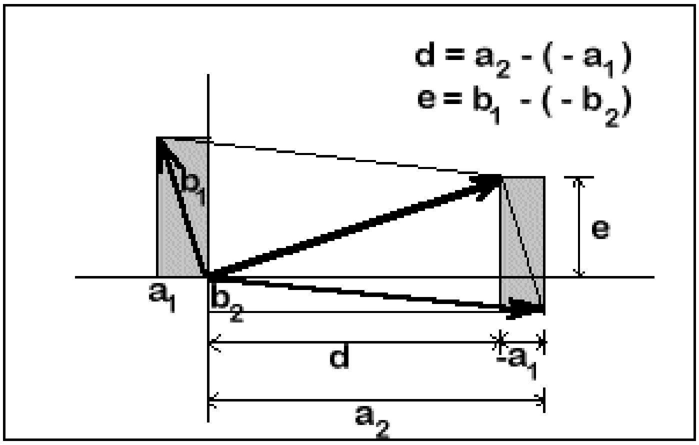
– Caso 1: todas as componentes são positivas.



– Caso 2: a_1 e a_2 têm sinais contrários, mas b_1 e b_2 têm mesmo sinal.



– Caso 3: a_1 e a_2, bem como b_1 e b_2, têm sinais contrários.



A prova ficará completa com resolução do exercício a seguir, que complementa todos os casos considerados aqui.

CQD.

Exercício 283 -

i). *Provar que $z+w$ tem como representação vetorial $\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{OB}$, para os demais casos em que os pares de números (a_1,a_2) e (b_1,b_2) são formados por pares de mesmo sinal.*

ii). *Provar que $z+w$ tem como representação vetorial $\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{OB}$, para os demais casos em que os pares de números (a_1,a_2) e (b_1,b_2) são tais que um par é formado por números de mesmo sinal, e o outro é formado por números de sinais contrários.*

iii). *Provar que $z+w$ tem como representação vetorial $\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{OB}$, para os demais casos em que os pares de números (a_1,a_2) e (b_1,b_2) são formados por números de sinais contrários.*

iv). *Provar que $z+w$ tem como representação vetorial $\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{OB}$, para o caso em que alguma coordenada é nula.*

v). *Provar que $z+w$ tem como representação vetorial $\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{OB}$, para o caso em que algum dos vetores (ou ambos) é nulo.*

vi). *Provar que $z+w$ tem como representação vetorial $\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{OB}$, para o caso em que os vetores $\overrightarrow{OA}$ e $\overrightarrow{OB}$ são colineares.*

Observação 9.29 -

Pelo Teorema anterior, costuma-se dizer que a correspondência biunívoca entre $\mathbb{C}$ e o conjunto dos vetores complexos preserva somas. Ou seja, a identificação de números de $\mathbb{C}$ com vetores complexos faz com que a soma de dois números complexos corresponda precisamente à soma dos vetores associados a tais números.

Exercício 284 -

Usando que a diferença entre dois complexos pode ser vista como uma soma (com efeito, $z - w = z + (-w)$), e que $-\overrightarrow{OZ}$ denota o vetor complexo de mesma direção e módulo que $\overrightarrow{OZ}$, mas com sentido oposto, pede-se interpretar geometricamente a diferença entre dois números complexos.

Faça uma figura onde sejam representadas tanto a soma como a diferença de dois números complexos dados.

Exercício 285 -

Dados dois números complexos, z e w, indiquemos por $\overrightarrow{OA}$ e por $\overrightarrow{OB}$ suas respectivas representações vetoriais. Como já sabemos, sendo $\overrightarrow{OC} = \overrightarrow{OA} + \overrightarrow{OB}$, a diagonal OC do paralelogramo $OACB$ tem comprimento igual a $|z + w|$. Como complementação a esse fato, pede-se:

i). mostrar que a outra diagonal do paralelogramo, o segmento de extremos A e B, tem comprimento igual a $|z - w| = |\overrightarrow{OA} - \overrightarrow{OB}|$;

ii). concluir que o número real $|z-w|$ pode ser interpretado como a distância entre as representações pontuais de z e w.

Exercício 286 -

Represente no plano de Argand o conjunto dos números complexos z verificando $|z - i| = 2$.

Exercício 287 -

Represente no plano de Argand o conjunto $A \cap B$, onde A é o conjunto dos números complexos z tais que $|z - 1| < 3$, e B é o conjunto dos números complexos z tais que $|z - 2i| < 2$.

Proposição 9.30 (*Desigualdade do Triângulo*) -

Para quaisquer $z, w \in \mathbb{C}$*:*

$$|z + w| \leqslant |z| + |w|.$$

Prova 1 (geométrica, para o caso de vetores de direções distintas):
podemos considerar esse resultado como óbvio, na medida em que $|z|$, $|w|$ e $|z+w|$ podem ser vistos como as medidas dos lados de um triângulo e, num triângulo, a soma dos comprimentos de dois lados é sempre maior ou igual do que o comprimento do terceiro lado. CQD

Prova 2 (algébrica):
como $|z+w|$, $|z|$ e $|w|$ são números positivos, basta mostrarmos que $|z+w|^2 \leqslant (|z|+|w|)^2$, ou seja: $|z+w|^2 \leqslant |z|^2 + 2|z||w| + |w|^2$. Ora, escrevendo $z = a + bi$ e $w = c + di$, essa desigualdade equivale a:

$$(a+c)^2 + (b+d)^2 \leqslant (a^2+b^2) + 2\sqrt{a^2+b^2}\sqrt{c^2+d^2} + (c^2+d^2),$$

que por sua vez equivale a

$$ac + bd \leqslant \sqrt{(a^2+b^2)(c^2+d^2)}. \tag{9.12}$$

Como $ac + bd \leqslant |ac+bd|$, se mostrarmos que

$$|ac + bd| \leqslant \sqrt{(a^2+b^2)(c^2+d^2)}, \tag{9.13}$$

teremos também (9.12). Ora,

$$0 \leqslant (ad - bc)^2 = a^2d^2 - 2abcd + b^2c^2,$$

logo

$$2abcd \leqslant a^2d^2 + b^2c^2,$$

portanto

$$a^2c^2 + 2abcd + b^2c^2 \leqslant a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2,$$

ou

$$(ac + bd)^2 \leqslant (a^2+b^2)(c^2+d^2),$$

que é a desigualdade (9.13), reescrita. CQD

Observação 9.31 -

É importante ressaltar que um dado enunciado matemático pode ser melhor entendido quando enfocado sob diferentes pontos de vista. Além disso, essa variedade de enfoques pode nos levar a conceber diversas demonstrações para o enunciado, umas mais simples ou mais elucidativas, do que outras. Reflita sobre essas observações considerando a proposição anterior.

– Interpretação geométrica da multiplicação de números complexos

Esta interpretação é bem menos simples e natural que a da adição. Com efeito, a dificuldade de se concebê-la foi uma das causas da demora da legitimação dos números complexos.

A representação geométrica da multiplicação de números complexos que mostraremos a seguir é devida a Argand, e consiste numa multiplicação vetorial.[5] Para que fique mais fácil entendermos o que será feito, tomaremos alguns casos particulares fáceis e naturais de interpretar. Iniciamos com o caso mais simples de todos, onde um dos fatores do produto é um número real.

Exercício 288 -

Inicialmente, apresente a representação vetorial dos números complexos z e rz, nos seguintes casos de r real:

i). quando $r = 2$
ii). quando $r = 1/2$
iii). quando $r = -3$.

Como você descreveria a representação vetorial do número complexo rz, no caso de r real qualquer?

Prossigamos, vendo o caso particular da representação de iz, para vários casos de z complexo.

[5] Nesse sentido, é importante alertarmos os leitores, principalmente aqueles que já estudaram Geometria Analítica, que a multiplicação vetorial que veremos aqui não é nenhuma das multiplicações vetoriais usuais (multiplicação escalar $\overrightarrow{u} \cdot \overrightarrow{v}$ e multiplicação vetorial $\overrightarrow{u} \times \overrightarrow{v}$). Em particular, o leitor não deve ficar surpreso em saber que existem outrar maneiras de se definir multiplicação vetorial além das conhecidas $\overrightarrow{u} \cdot \overrightarrow{v}$ e $\overrightarrow{u} \times \overrightarrow{v}$.

Exercício 289 -

Apresente a representação vetorial dos números complexos i, z e iz para várias escolhas de z.

O exercício a seguir apresenta uma propriedade geométrica comum nas representações vetoriais dos números z, i e iz.

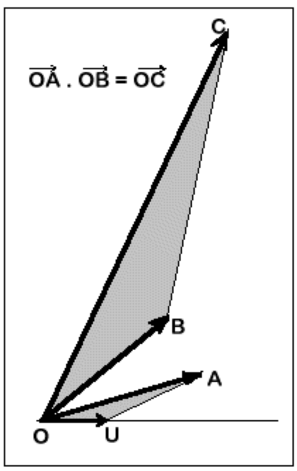
Exercício 290 -

Sejam $\overrightarrow{OU}$, $\overrightarrow{OA}$, $\overrightarrow{OB}$ e $\overrightarrow{OC}$ representações vetoriais de 1, i, z e iz, respectivamente, e suponha que z é tal que OBC é um triângulo. O que você pode afirmar sobre os triângulos OUA e OBC?

A propriedade apresentada no último exercício vale sempre, e nos permite interpretar geometricamente a multiplicação de números complexos. Confira:

Exercício 291 -

Sejam z e w números complexos, com z não real, e sejam $\overrightarrow{OU}$, $\overrightarrow{OA}$, $\overrightarrow{OB}$ e $\overrightarrow{OC}$ as representações vetoriais de 1, z, w e zw, respectivamente. Prove que os triângulos OUA e OBC são semelhantes.



Exercício 292 -

Dado um número complexo z não nulo, apresente a representação pontual de todos os números $i^n z$, onde $n \geqslant 1$ é um inteiro.

Exercício 293 -

Dado um número complexo w, não real, apresente a representação vetorial do número complexo $1/w$.

Exercício 294 -

Explorando a identidade

$$\frac{z}{w} = z \cdot \frac{1}{w}\,,$$

dar uma interpretação geométrica para a divisão dos números complexos z e w.

Observação 9.32 -

Quando for conhecida a representação trigonométrica dos números complexos, poderemos dar uma interpretação geométrica alternativa para o produto, interpretação esta que é mais simples e bem mais utilizada. (Infelizmente, questões trigonométricas terão de ser deixadas para um outro livro.)

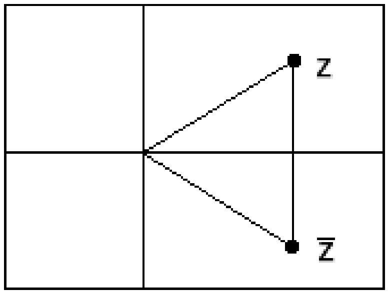
9.8 Conjugado de um número complexo

A noção de conjugado de um número complexo é tão útil que já foi explorada pelo próprio Bombelli. No que segue, observe, em particular, como ela nos permite simplificar o trabalho de divisão de números complexos. Num próximo capítulo, também veremos sua utilidade na enumeração das raízes de equações polinomiais.

Definição 9.33 -

O conjugado de um número complexo, $z = a + bi$, é o número $a - bi$.
O conjugado de z é denotado por $\overline{z}$.

A figura que segue indica a representação pontual do conjungado de z.



Proposição 9.34 -

Um número complexo é igual ao seu conjugado se, e só se, ele for um número real.

Prova:

$$a + bi = a - bi \iff b = -b \iff b = 0.$$

CQD.

Proposição 9.35 -

A operação de conjugação de complexos (isto é, de tomar o conjugado de um número complexo) é uma operação involutiva*, isto é:*

$$\overline{\overline{z}} = z\,,\ \forall z \in \mathbb{C}.$$

Exercício 295 -

Prove a Proposição 9.35.

Definição 9.36 -

Por números conjugados *entendemos quaisquer dois números complexos, tais que um deles é igual ao conjugado do outro.*

Proposição 9.37 -

Para cada número complexo z, temos

$$\operatorname{Re} z = \frac{z + \overline{z}}{2} \qquad e \qquad \operatorname{Im} z = \frac{z - \overline{z}}{2}.$$

Prova:

Basta calcular $z \pm \overline{z}$, usando $z = a + bi$. CQD.

Exercício 296 -

Prove em detalhe a Proposição 9.37.

Proposição 9.38 (*Propriedades básicas da conjugação*) -

A operação de conjugação é:

i). aditiva: $\overline{z+w} = \overline{z} + \overline{w} \quad (\forall\, z, w \in \mathbb{C})$;

ii). subtrativa: $\overline{z-w} = \overline{z} - \overline{w} \quad (\forall\, z, w \in \mathbb{C})$;

iii). multiplicativa: $\overline{z \cdot w} = \overline{z} \cdot \overline{w} \quad (\forall\, z, w \in \mathbb{C})$;

iv). divisiva: $\overline{z/w} = \overline{z}/\overline{w} \quad (\forall\, z, w \in \mathbb{C}$, *com* $w \neq 0)$.

Prova:

Os quatro casos têm uma demonstração semelhante. Por exemplo, no caso da multiplicação, partimos de $z = a + bi$ e $w = c + di$, e com essas representações calculamos $z \cdot w$ e depois o resultado $\overline{z \cdot w}$; a seguir, calculamos $\overline{z} \cdot \overline{w} = (a - bi) \cdot (c - di)$ e verificamos que o resultado obtido coincide com o primeiro.

CQD.

Exercício 297 -

Prove a Proposição 9.38 em detalhe.

Exercício 298 -

Sendo z complexo, prove que para todos os n inteiros positivos:

$$\overline{z^n} = \left(\overline{z}\right)^n .$$

Qual o resultado correspondente para n inteiro negativo?

Corolário 9.39 -

Seja $p(X)$ um polinômio com coeficientes reais. *Então, para cada número complexo z, temos:*

$$\overline{p(z)} = p(\overline{z}).$$

Prova:

Seja $p(X) = a_n X^n + \ldots + a_2 X^2 + a_1 X + a_0$, onde os coeficientes são números reais. Dado um $z \in \mathbb{C}$, temos sucessivamente, pelos resultados anteriores:

$$\begin{aligned}
\overline{p(z)} &= \overline{a_n z^n + \ldots + a_2 z^2 + a_1 z + a_0} \\
&= \overline{a_n z^n} + \ldots + \overline{a_2 z^2} + \overline{a_1 z} + \overline{a_0} && [propr.\ aditiva] \\
&= \overline{a_n}\,\overline{z^n} + \ldots + \overline{a_2}\,\overline{z^2} + \overline{a_1}\,\overline{z} + \overline{a_0} && [propr.\ multiplicativa] \\
&= \overline{a_n}\,\overline{z}^{\,n} + \ldots + \overline{a_2}\,\overline{z}^{\,2} + \overline{a_1}\,\overline{z} + \overline{a_0} && [Exerc.\ 298] \\
&= a_n \overline{z}^n + \ldots + a_2 \overline{z}^2 + a_1 \overline{z} + a_0 && [coefic.\ reais] \\
&= p(\overline{z})\,.
\end{aligned}$$

CQD.

Corolário 9.40 -

Seja $p(X)$ um polinômio com coeficientes reais. *Um número complexo $a + bi$ é raiz da equação $p(x) = 0$ se, e só se, o conjugado $a - bi$ também for raiz desta equação. Ou seja:*

$$p(z) = 0 \iff p(\overline{z}) = 0\,.$$

Exercício 299 -

Mostre, por substituição direta, que a equação polinomial

$$x^2 + (2i - 3)x + 5 - i = 0$$

admite $z = 1 + i$ e $z = 2 - 3i$ como raízes, mas não admite seus conjugados como raízes. Compare essa conclusão com a do corolário anterior.

Exercício 300 -

Seja $p(X)$ um polinômio com coeficientes reais. Dado $z = a + bi$, com a e b reais, escrevamos o valor de $p(a + bi)$ em termos de sua parte real e sua parte imaginária, *ou seja:*

$$p(a+bi) = u + iv\,,$$

onde u e v são reais. Prove que

$$p(a-bi) = u - iv\,.$$

Exercício 301 -

Prove que o produto $z \cdot \overline{z}$ de um número complexo por seu conjugado é um número real, enquanto que o produto $z{\cdot}\overline{w}$ pode não ser real, se z e w forem números complexos quaisquer.

Exercício 302 -

Mostre que, para quaisquer $z, w \in \mathbb{C}$:

$$|z+w|^2 = |z|^2 + |w|^2 + 2\,\mathrm{Re}(z\overline{w}) \quad e \quad |z-w|^2 = |z|^2 + |w|^2 - 2\,\mathrm{Re}(z\overline{w})\,.$$

Na prática, é muito usada a seguinte versão do Exercício 301:

Teorema 9.41 (*Teorema do produto de conjugados*) -

Para cada $z \in \mathbb{C}$ temos: $z \cdot \overline{z} = |z|^2$.

Exercício 303 -

Prove o Teorema 9.41.

Corolário 9.42 -

Sendo a, b, c e d reais, $z = a+bi$, e $w = c+di \neq 0$, temos:

$$\frac{a+bi}{c+di} = \frac{z}{w} = \frac{z.\overline{w}}{|w|^2} = \frac{(a+bi)\,(c-di)}{c^2+d^2}\,.$$

Prova:

O crucial é observar que

$$\frac{z}{w} = \frac{z.\overline{w}}{w.\overline{w}} = \frac{z.\overline{w}}{|w|^2}\,.$$

CQD.

Exercício 304 *Qual a utilidade do resultado estabelecido nesse corolário? Apresente alguns exemplos que comprovem tal utilidade.*

Corolário 9.43 -

Dado $z \in \mathbb{C}$ não nulo, tem-se

$$\frac{1}{z} = \frac{\overline{z}}{z \cdot \overline{z}} = \frac{\overline{z}}{|z|^2}\,.$$

Prova:

imediata do corolário anterior. CQD.

Exercício 305 -

Refaça o Exercício 293, agora utilizando o último corolário.

Corolário 9.44 -

Dado $z \in \mathbb{C}$ de módulo unitário, tem-se

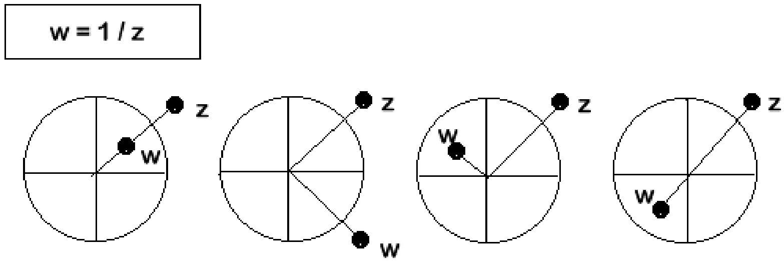
$$\frac{1}{z} = \overline{z}\,.$$

Prova:

basta aplicar o último corolário, usando que $|z| = 1$. CQD.

Exercício 306 -

Nas figuras a seguir, o círculo desenhado é o círculo unitário. Pede-se mostrar que todas elas são representações geométricas incorretas de $w = 1/z$. Feito isso, desenhe as representações corretas.



Exercício 307 -

Usando o teorema do produto de conjugados, mostre que

$$|z \cdot w| = |z| \cdot |w| \, .$$

Compare sua demonstração com a feita na Proposição 9.26.

Observação 9.45 -

Uma utilidade do teorema do produto de conjugados é nos permitir afirmar que o produto $z\overline{z}$ é um número real, e até mesmo não negativo. Contudo, em geral, um produto $z_1\overline{z_2}$ pode não ser real, conforme mostrado no Exercício 301.

Exercício 308 -

Usando o teorema do produto de conjugados, descreva o conjunto de números complexos z que satisfazem

$$\left| \frac{z-3}{z+3} \right| < 2 \, .$$

Exercício 309 -

Mostre que

$$|z - w| = |1 - \overline{z}w| \; ,$$

sempre que $z, w \in \mathbb{C}$ satisfizerem ao menos uma das condições $|z| = 1$ e $|w| = 1$.

Exercício 310 -

Sendo x, y reais e $z = x + iy$, pede-se

i). reescrever a equação $2x + y = 5$ como uma equação envolvendo apenas z e $\overline{z}$;
ii). mostrar que a equação de qualquer círculo do plano pode ser reescrita como

$$az\overline{z} + \beta z + \overline{\beta}\,\overline{z} + c = 0\,,$$

para convenientes $a, c \in \mathbb{R}$, e $\beta \in \mathbb{C}$.

9.9 Operação de radiciação com números complexos

A extensão das operações aritméticas (adição, multiplicação, subtração e divisão) dos números reais para os números complexos não trouxe nenhuma novidade algébrica. A única restrição operatória encontrada até o momento foi a divisão por zero, que ocorre em qualquer campo numérico. Essas semelhanças operatórias poderiam nos levar a esperar que é igualmente fácil estender a operação de radiciação para os números complexos. A seguir, veremos que isso está longe de ser verdade. Com efeito, embora não existam maiores dificuldades na extensão da operação de extração de raízes quadradas, a definição de raízes de ordem maior ou igual a 3, no campo dos complexos, é um problema inviável de ser resolvido em contexto puramente algébrico.

– Cálculo das raízes quadradas de um número complexo

Veremos a seguir que, trabalhando com a representação binomial, não teremos grandes dificuldades em calcular as raízes quadradas complexas de qualquer número complexo dado e, em particular, de reais negativos.

Teorema 9.46 -

Todo número complexo admite pelo menos uma raiz quadrada que é um número complexo. Mais precisamente: para cada $w \in \mathbb{C}$, existe pelo menos um $z \in \mathbb{C}$, tal que $z^2 = w$.

Prova:

Escrevamos w como $w = a + bi$. Se indicarmos z por $z = x + iy$, com x e y a determinar, podemos transformar a equação complexa $z^2 = w$ em duas equações reais, da seguinte forma:

$$z^2 = w \iff (x + yi)^2 = a + bi \iff x^2 - y^2 + 2xyi = a + bi\,,$$

ou seja:

$$\exists z \in \mathbb{C}, \text{tal que } z^2 = w \iff \exists x, y \in \mathbb{R} \text{ tais que } x^2 - y^2 = a \text{ e } 2xy = b\,.$$

Assim, precisamos provar que o sistema de equações

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

tem solução em $\mathbb{R}$; após encontrá-las, teremos garantido que $z = x + iy$ é tal que $z^2 = a + bi = w$.

Passamos então a considerar dois casos: w real, ou não real.

– Caso 1: w é um número real.

Neste caso, $b = 0$, e o sistema se resume a

$$\begin{cases} x^2 - y^2 = a \\ 2xy = 0\,. \end{cases} \tag{9.14}$$

Pela segunda equação deduzimos que, se tal sistema tiver solução, então $x = 0$ ou $y = 0$. Daí, comparando com a primeira equação:

$$\begin{array}{l} a > 0 \Rightarrow y = 0 \Rightarrow x = \pm\sqrt{a} \text{ e } y = 0 \Rightarrow z = x + yi = \pm\sqrt{a} \\ a < 0 \Rightarrow x = 0 \Rightarrow y = \pm\sqrt{-a} \Rightarrow z = x + yi = \pm i\sqrt{-a} \\ a = 0 \Rightarrow x^2 = y^2 \Rightarrow x = 0 = y \Rightarrow z = x + yi = 0 + 0i\,. \end{array}$$

É fácil agora comprovar que de fato todos esses candidatos são efetivamente soluções do sistema (9.14); podendo-se concluir, então, que sempre existe pelo menos uma solução complexa para a equação $z^2 = w$, no caso em que w é um número real, e existindo exatamente duas quando w for um número real não nulo.

– Caso 2: w não é um número real, isto é, $b \neq 0$.

Neste caso, se o sistema

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

tiver solução, a segunda equação mostra que necessariamente $x \neq 0$ e $y \neq 0$. Ademais, da primeira equação obtemos

$$x^2 - y^2 = a \;\Rightarrow\; x^2 = a + y^2 \;\Rightarrow\; 2x^2 = a + x^2 + y^2 = a + |z|^2\,.$$

Mas, se esse sistema tiver solução, então $z = x + yi$ é tal que $z^2 = w$ logo $|z|^2 = |w| = \sqrt{a^2 + b^2}$, de modo que x e y serão soluções do sistema

$$\begin{cases} 2x^2 = a + \sqrt{a^2 + b^2} \\ 2xy = b\,. \end{cases}$$

Resolvendo esse sistema, obtemos:

$$x = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}$$

$$y = \pm\frac{b}{2\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}} = \pm\frac{b}{\sqrt{2}\sqrt{a + \sqrt{a^2 + b^2}}}\,,$$

sendo x e y de mesmo sinal se $b > 0$, e de sinais opostos se $b < 0$.

(Note que, mesmo que a seja negativo, o número $a + \sqrt{a^2 + b^2}$ sempre será estritamente positivo, pois

$$\sqrt{a^2 + b^2} \overset{b\neq 0}{>} \sqrt{a^2} = |a| \Rightarrow a + \sqrt{a^2 + b^2} > a + |a| \geqslant 0\ .)$$

Concluímos assim que, quando w não é real, só existem dois candidatos a soluções para a equação $z^2 = w$:

$$z = \pm\left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + i\frac{b}{\sqrt{2}\sqrt{a + \sqrt{a^2 + b^2}}}\right).$$

Afirmamos que ambos são efetivamente soluções dessa equação. Com efeito, em qualquer caso, fazendo $d = \sqrt{a + \sqrt{a^2 + b^2}}$ para facilitar a escrita, temos:

$$
\begin{aligned}
z^2 &= \left(\frac{d}{\sqrt{2}} + i \frac{b}{d\sqrt{2}} \right)^2 \\
&= \left(\frac{d}{\sqrt{2}} \right)^2 - \left(\frac{b}{d\sqrt{2}} \right)^2 + 2i \frac{d}{\sqrt{2}} \frac{b}{\sqrt{2}d} \overset{d^2 = a + \sqrt{a^2+b^2}}{=} \\
&= \frac{a + \sqrt{a^2 + b^2}}{2} - \frac{b^2}{2\left(a + \sqrt{a^2 + b^2}\right)} + bi \\
&= \frac{\left(a + \sqrt{a^2 + b^2}\right)^2 - b^2}{2\left(a + \sqrt{a^2 + b^2}\right)} + bi \\
&= \frac{a^2 + 2a\sqrt{a^2 + b^2} + a^2 + b^2 - b^2}{2\left(a + \sqrt{a^2 + b^2}\right)} + bi \\
&= \frac{a^2 + 2a\sqrt{a^2 + b^2}}{\left(a + \sqrt{a^2 + b^2}\right)} + bi \\
&= \frac{2a\left(a + \sqrt{a^2 + b^2}\right)}{2\left(a + \sqrt{a^2 + b^2}\right)} + bi = a + bi = w\,,
\end{aligned}
$$

o que completa a demonstração do teorema. CQD.

Resumamos os resultados importantes dessa demonstração:

> **Corolário 9.47** -
>
> *Se $w = a + bi$ e $z^2 = w$, então:*
>
> - $z = 0 + 0i$, *se* $w = 0 + 0i$;
> - $z = \pm\sqrt{a}$, *se* $w = a + 0i$ *com* $a > 0$;
> - $z = \pm i\sqrt{a}$, *se* $w = a + 0i$ *com* $a < 0$;
> - $z = \pm \left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + i \frac{b}{\sqrt{2}\sqrt{a + \sqrt{a^2 + b^2}}} \right)$, *se* $w = a + bi$ *com* $b \neq 0$.

Exercício 311 -

Determine todos os possíveis $z \in \mathbb{C}$, *tais que* $z^2 = 1 + 2i$. *Faça isso de duas* *maneiras:*

i). utilizando diretamente as fórmulas do corolário anterior;

ii). particularizando o raciocínio da demonstração do teorema anterior para o caso $w = 1 + 2i$.

Observação 9.48 -

O cálculo da raiz de grau $\geqslant 3$ *de um número complexo é praticamente inviável de ser feito usando a representação binomial. Para se convencer da imensa dificuldade envolvida, o leitor está convidado a tentar resolver o sistema de duas equações nas incógnitas* x *e* y *provenientes da equação*

$$(x + iy)^3 = a + bi\,.$$

Tendo aprendido a calcular todos os possíveis números complexos, cujo quadrado é um número complexo dado, é natural procurarmos usar isto para calcular todas as soluções de qualquer equação polinomial do segundo grau e com coeficientes complexos. O exercício a seguir mostra que a fórmula de Bhaskara continua válida nesses casos.

Exercício 312 -

Prove que a equação quadrática geral de coeficientes complexos, $az^2 + bz + c = 0$ *admite*

i). exatamente uma solução quando $b^2 - 4ac = 0$, *a saber:* $-b/2a$;

ii). exatamente duas soluções quando $b^2 - 4ac \neq 0$, *a saber:*

$$\frac{-b+w}{2a} \quad e \quad \frac{-b-w}{2a}$$

(onde w *é um número complexo cujo quadrado é* $b^2 - 4ac$ *).*

iii). Confirme que as duas expressões de (ii) dão as soluções da equação, qualquer que seja a escolha que se faça para w .

Passemos a tratar do cálculo da raiz quadrada de números complexos. Para isso, iniciemos recordando que, quando estudamos os números reais, introduzimos um símbolo (a raiz quadrada aritmética ou principal) que nos permitiu representar algebricamente todas as eventuais raízes quadradas de um dado número real. Recordemos brevemente o que lá foi feito.

- A raiz quadrada aritmética ou principal é definida para todos os números reais $x \geqslant 0$, e é caracterizada como sendo o único número real $y \geqslant 0$, tal que $y^2 = x$. Notação: $y = \sqrt{x}$.
- O número real $x = 0$ tem exatamente uma raiz quadrada, e ela é dada por $y = \sqrt{0}$.
- Cada número real $x > 0$ tem exatamente duas raízes quadradas, e elas são dadas por $y = +\sqrt{x}$ e $y = -\sqrt{x}$.
- Nenhum número real $x < 0$ tem raiz quadrada.

Vejamos como adaptar esses resultados para o caso das raízes quadradas de números complexos. Iniciamos observando que, uma vez que $\mathbb{C}$ não é um corpo ordenado, não faz sentido falarmos em "número complexo positivo" e nem em "número complexo negativo". Contudo, o que realmente precisamos é ter um *critério* de escolha única da raiz quadrada. Isso, a rigor, já foi feito no caso $w \in \mathbb{R}$. Com efeito, nesse caso, $\sqrt{w}$ é o único real do semi-eixo $[0, +\infty)$, cujo quadrado vale w. De modo que nossa questão é: quando $w \in \mathbb{C}$, será possível adotar um critério semelhante, escolhendo uma região do plano de Argand na qual um único valor de z verifique $z^2 = w$?

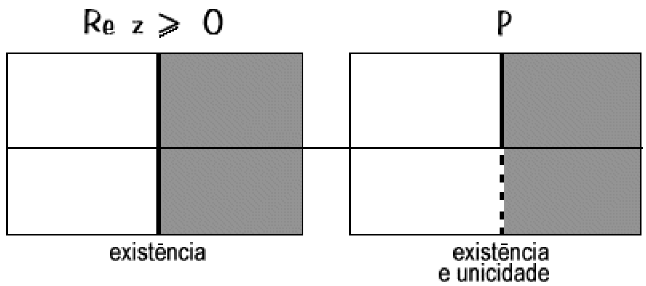
A partir do Corolário 9.47, vemos que é sempre possível encontrar uma solução z com $\operatorname{Re} z \geq 0$. No entanto, para nossos fins, a existência não é bastante, precisamos também ter unicidade. Ora, o único caso em que não temos unicidade satisfazendo essa condição é quando w for um real negativo, situação que nos leva a duas soluções que são imaginários puros: $i\sqrt{-w}$ e $-i\sqrt{-w}$. Logo, para termos unicidade, tudo o que precisamos fazer é cortar da região $\operatorname{Re} z \geqslant 0$, por exemplo, os $z \in \mathbb{C}$ verificando, simultâneamente, $\operatorname{Re} z = 0$ e $\operatorname{Im} z < 0$. Em termos concretos, temos o seguinte resultado:

Teorema 9.49 -

Definindo

$$\mathcal{P} = \{z \in \mathbb{C} \,|\, \operatorname{Re} z > 0\} \cup \{z \in \mathbb{C} \,|\, \operatorname{Re} z = 0 \text{ e } \operatorname{Im} z \geqslant 0\},$$

temos que, para todo número complexo w, existe um único número complexo $z \in \mathcal{P}$, verificando $z^2 = w$.



Definição 9.50 -

Para cada $w \in \mathbb{C}$, o símbolo $\sqrt{w}$ denota a única solução z da equação $z^2 = w$ que pertence ao conjunto $\mathcal{P}$; solução esta que é denominada **determinação principal da raiz quadrada de** w *ou* **raiz quadrada principal** *de w.*

Exercício 313 -

Mostre que $\{z \in \mathbb{C} \,|\, z = a + 0i, a \geqslant 0\} \subset \mathcal{P}$.
Ademais, verifique que a determinação principal da raiz quadrada de $w \geqslant 0$ coincide com a raiz quadrada aritmética de $w \geqslant 0$. Ou seja: a extensão da raiz quadrada aritmética para o campo dos números complexos é feita pela determinação principal da raiz quadrada. Em particular, não há perigo de confusão ao usarmos o símbolo $\sqrt{w}$, seja no sentido real, seja no sentido complexo!

Podemos resumir todas essas colocações com o seguinte teorema:

Teorema 9.51 -

Todo número complexo w tem uma, e somente uma, raiz quadrada principal. Seu valor, $\sqrt{w}$, é dado por:

- $\sqrt{w} = \sqrt{a + 0i} = \sqrt{a}$, *se* $a \geqslant 0$;
- $\sqrt{w} = \sqrt{a + 0i} = i\sqrt{a}$, *se* $a < 0$;
- $\sqrt{w} = \sqrt{a + bi} = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\frac{b}{\sqrt{2}\sqrt{a+\sqrt{a^2+b^2}}}$, *se* $b \neq 0$ *e* a *é real.*

Exercício 314 -

Expresse na forma $a + bi$ o valor das seguintes raízes quadradas principais:

i). $\sqrt{i}$
ii). $\sqrt{1+i}$.

Exercício 315 -

Comprove que $\sqrt{-15-8i} = 1 - 4i$. *A seguir, expresse na forma $a + bi$ todas as raízes quadradas de $-15 - 8i$.*

Exercício 316 -

Sem usar fórmulas, refaça o exercício anterior.

Exercício 317 -

Os cálculos a seguir mostram que a regra $\sqrt{a}\sqrt{b} = \sqrt{ab}$ somente vale para reais $\geqslant 0$. Pede-se explicar o absurdo obtido.

$$\begin{aligned}\sqrt{6} &= \sqrt{(-2)(-3)}\\ &= \sqrt{-1}\sqrt{2}\sqrt{-1}\sqrt{3}\\ &= i\sqrt{2}i\sqrt{3}\\ &= i^2\sqrt{6} = -\sqrt{6}\,.\end{aligned}$$

Agora, podemos melhorar o Exercício 312, dando a solução das equações quadráticas, de coeficientes complexos, ao estilo de Bhaskara:

Proposição 9.52 -

As raízes complexas da equação $ax^2 + bx + c = 0$ (com $a, b, c \in \mathbb{C}$, e $a \neq 0$) são precisamente os números complexos

$$z_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad e \quad z_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}\,,$$

onde $\sqrt{b^2 - 4ac}$ denota a raiz quadrada principal do número complexo $b^2 - 4ac$.

Exercício 318 -

Usando a fórmula (a rigor, as fórmulas) de Bhaskara, e o resultado do Exercício 315, resolva a equação quadrática:

$$z^2 + (2i-3)z + 5 - i = 0\,.$$

A seguir, confira por substituição direta na equação que as raízes são $z_1 = 1+i$ *e* $z_2 = 2-2i$.

Exercício 319 -

Determine todas as raízes da equação

$$(1+i)z + 3i\,\overline{z} - (2+i) = 0\,.$$

Exercício 320 -

Dados z_1 *e* z_2 *números complexos quaisquer,*

i). *mostre que ambos são raízes da equação polinomial*

$$z^2 - (z_1+z_2)z + z_1 z_2 = 0\,;$$

ii). *mostre que se* z_1 *e* z_2 *forem tais que* $z_1 + z_2 \in \mathbb{R}$ *e* $z_1 z_2 \in \mathbb{R}$, *então* z_1 *e* z_2 *ou são ambos reais, ou são ambos complexos conjugados.*

O exercício a seguir mostra que o conjunto $\mathcal{P}$ anteriormente definido não serve para determinar com unicidade o que seria $\sqrt[3]{w}$.

Exercício 321 -

Mostre que

$$-1, \qquad \frac{1}{2} + \frac{\sqrt{3}}{2}i, \qquad \frac{1}{2} - \frac{\sqrt{3}}{2}i$$

são todas raízes cúbicas de -1, *mas que não é verdade que exatamente uma delas está em* $\mathcal{P}$.

CAPÍTULO 10

OS TEOREMAS FINAL DA ARITMÉTICA E FUNDAMENTAL DA ÁLGEBRA

Antes de tudo, fixemos a terminologia: onde aqui utilizarmos a palavra "aritmética" estaremos nos referindo às propriedades das operações entre números reais ou complexos. Reservamos as palavras "álgebra" e "algébrica" para quando estivermos tratando de problemas de equações polinomiais.

Conforme insistido no capítulo anterior, os números complexos foram introduzidos como uma extensão dos números reais viabilizando "destravar" o cálculo das raízes reais das chamadas cúbicas irredutíveis. Com o passar do tempo, gradativamente foi se percebendo que essa extensão tinha capacidades que iam muito além do citado "destravamento". Por exemplo, logo se descobriu que os números complexos possibilitavam realizar vários tipos de cálculos aritméticos, até então totalmente impensáveis, bem como elucidavam muitos fenômenos algébricos, tais como os que envolvem relações entre quantidade de raízes de equações polinomiais e o grau do respectivo polinômio. É exatamente dessas surpreendentes capacidades que trata este capítulo.

Mais detalhadamente, este capítulo tem dois grandes objetivos:

– Primeiro: mostrar que com os números complexos chegamos, finalmente, a um campo numérico que *é plenamente satisfatório sob o ponto de vista aritmético*. Essa demonstração será concretizada com o Primeiro Teorema Fundamental da Aritmética.
– Segundo: mostrar que o campo dos números complexos também é *plenamente satisfatório sob o ponto de vista algébrico*. Essa segunda demonstração será concretizada por meio do Teorema Fundamental da Álgebra, em suas várias versões.

Para que nosso texto fique autossuficiente, faremos um estudo básico das relações entre polinômios e raízes de equações polinomiais em corpos numéricos. Sendo que por *corpo numérico* entenderemos qualquer campo $[\mathbb{K}, +, \times]$ que tenha estrutura de corpo, ocorra $\mathbb{K} \subseteq \mathbb{C}$ e as operações de adição e multiplicação sejam as usuais. [1]

Esse ponto de vista, mais geral do que a abordagem usual do Ensino Fundamental e Médio, nos permitirá perceber que a plenitude da simplicidade e utilidade das relações mencionadas anteriormente – entre polinômios e as raízes das respectivas equações polinomiais – encontra-se no maior dos corpos numéricos: o corpo $\mathbb{C}$ dos números complexos. Essa descoberta será sintetizada por meio de um grupo de teoremas assemelhados, todos chamados de Teorema Fundamental da Álgebra (TFA) por serem logicamente equivalentes.

[1]Na terminologia mais precisa da Álgebra: $[\mathbb{K}, +, \times]$ é um subcorpo do corpo dos números complexos.

10.1 O primeiro Teorema Final da Aritmética

A fim de entendermos a suficiência do corpo dos complexos sob o ponto de vista aritmético, explicitemos uma hierarquia das operações com números:

– *Nível 1*:
as quatro operações aritméticas ou operações algébricas racionais: adição, subtração, multiplicação e divisão de números.
– *Nível 2*:
as operações de radiciação ou operações algébricas irracionais: extração de raiz quadrada, cúbica, quártica, etc. de números.

operações algébricas

– *Nível 3*:
as operações transcendentes elementares: exponenciação, logaritmação e avaliação das funções trigonomé - tricas circulares (diretas e inversas).
– *Nível 4*:
avaliação das funções transcendentais outras que as do nível 3, estudadas em cursos avançados.

operações transcendentais

Com essa hierarquia, podemos dizer que, no capítulo anterior – sobre números complexos – vimos que as cúbicas irredutíveis expuseram de maneira clara a necessidade de se poder atribuir sentido às operações de nível 2, mesmo para reais negativos. O campo dos reais é obviamente insuficiente para isso. Ainda naquele capítulo, vimos que os números complexos não apresentam essa deficiência, sendo plenamente capazes de atribuir sentido a todas as operações de nível 2, embora as regras operatórias dos radicais de números complexos requeiram maiores discussões do que as encontradas no campo dos reais.

Assim, resta-nos examinar se o campo dos números complexos também é suficiente para darmos sentido às operações transcendentais elementares, ou operações de nível 3. Por exemplo, será possível dar sentido numérico, bem como regras operacionais satisfatórias, para cálculos como

$$(-2)^{\pi}, \ \log(-2), \ \sqrt{-1}^{\sqrt{-1}} \ ?$$

Essas perguntas podem ser respondidas afirmativamente com o conhecimento das representações exponencial e trigonométrica dos números complexos. Remetemos o leitor curioso a [Ne]. Aqui, nos limitamos a apresentar o enunciado de um teorema que diz que todas as insuficiências aritméticas exibidas pelos números reais ficam sanadas com os números complexos:

Teorema 10.1 (*Primeiro Teorema Final da Aritmética*) -

Do ponto de vista aritmético, não é preciso ampliar o campo dos números complexos, pois ele é suficiente para dar sentido a todas as operações aritméticas (ou algébricas racionais), algébricas irracionais e as operações transcendentais elementares.

10.2 Conceitos e terminologia iniciais da teoria dos polinômios

Convenção 1:
a partir daqui, usaremos a denominação *corpo numérico* para denotar qualquer campo $[\mathbb{K}, +, \times]$ que tenha estrutura de corpo, sendo $\mathbb{K} \subseteq \mathbb{C}$, e onde as operações de adição e multiplicação sejam as usuais. Como as operações estarão fixas, usaremos a abreviação $\mathbb{K}$ para $[\mathbb{K}, +, \times]$. Também salientamos que, além dos corpos $\mathbb{K} = \mathbb{Q}$ e $\mathbb{K} = \mathbb{R}$, podemos considerar outras possibilidades, tais como $[\mathbb{Q}, \sqrt{2}]$ ou $\mathbb{K} = [\mathbb{Q}, \sqrt{2}, \sqrt{3}]$ (veja exercícios 222, 223), bem como o caso "limite" $\mathbb{K} = \mathbb{C}$ (o de maior interesse neste capítulo).

Definição 10.2 -

Por polinômio *com coeficientes num corpo numérico $\mathbb{K}$ entende-se toda expressão da forma*

$$a_n X^n + \cdots + a_1 X + a_0,$$

onde $a_0, \ldots, a_n$ são constantes pertencentes a $\mathbb{K}$, ditas coeficientes do polinômio e onde X é um símbolo chamado de indeterminada *do polinômio.*
É comum não valer a pena explicitarmos os termos de um polinômio, casos em que o denotaremos por $p(X)$, ou notação semelhante. Por isso, também é comum denotarmos um polinômio por $p(X) = a_n X^n + \cdots + a_1 X + a_0$.

Convenção 2:
No caso de um polinômio ter coeficientes $a_k = 1$, é costume não escrevê-los; ademais, também se costuma não escrever os termos de coeficiente nulo, o que significa dizer que se faz identificações tais como:

$$0X^5 + 1X^4 + 0X^3 - 5X^2 + 0X - 1 = X^4 - 5X^2 - 1\,.$$

Aprofundemos essas ideias, tratando da imprescindível noção de igualdade geral de polinômios. Devido à existência do que chamaremos polinômio nulo, a mesma envolve alguns cuidados.

Definição 10.3 -

Denominaremos qualquer expressão da forma $0X^n + \cdots + 0X + 0$ *de* polinômio nulo *e, pela convenção anterior, escreveremos:*

$$0 = 0X = 0X + 0 = 0X^2 = 0X^2 + 0 = 0X^2 + 0X + 0 = \dots\ .$$

Definição 10.4 -

Dois polinômios, $p(X)$ *e* $q(X)$*, são ditos* polinômios iguais *se, e só se, quando colocados na forma* $p(X) = a_nX^n + \cdots + a_1X + a_0$ *e* $q(x) = b_nX^n + \cdots + b_1X + b_0$ *(depois de possivelmente usarmos coeficientes nulos), tivermos que vale* $a_k = b_k$*, para todos os* $0 \leqslant k \leqslant n$*. Em tal caso, escreveremos* $p(X) = q(X)$ *e, também,* $a_nX^n + \cdots + a_1X + a_0 = b_nX^n + \cdots + b_1X + b_0$ *.*

Exemplo 10.5 -

Um polinômio $p(X)$ *é* igual ao polinômio nulo *(o que escreveremos como* $p(X) = 0$ *) se, e só se, todos os coeficientes de* $p(X)$ *forem nulos. Por exemplo:*

$$aX^2 + bX + c = 0 \iff a = b = c = 0\,.$$

Por outro lado, polinômio não nulo *é todo polinômio que não é igual ao identicamente nulo. Ou seja: é todo polinômio que tem ao menos um coeficiente diferente de zero.*

Exemplo 10.6 -

Vale a igualdade polinomial $X^2 + 3X - 4 = X^2 + bX - 4 \iff b = 3$*.*
Semelhantemente, temos:

$$\begin{aligned} X^2 + 1 = aX^3 + bX^2 + cX + d &\iff 0X^3 + 1X^2 + 0X + 1 = aX^3 + bX^2 + cX + d \\ &\iff a = 0,\, b = 1,\, c = 0,\, d = 1\,. \end{aligned}$$

Exercício 322 -

Verifique que a Definição 10.4 inclui a Convenção 2.

Exercício 323 -

Verifique que a Definição 10.4 equivale à seguinte:
"Dois polinômios, $a_nX^n+\cdots+a_1X+a_0$ e $b_mX^m+\cdots+b_1X+b_0$, são iguais quando, e somente quando, para todos os valores de k: $a_k \neq 0$ ou $b_k \neq 0 \ \Rightarrow\ a_k = b_k$."

Definição 10.7 -

Por equação polinomial *de* incógnita *x, e com coeficientes num corpo numérico $\mathbb{K}$, entende-se toda equação que pode ser escrita na forma*

$$a_nx^n + \cdots + a_1x + a_0 = 0,$$

onde $n \geqslant 1$, $a_n \neq 0$ e $a_0, \ldots, a_n$ são constantes pertencentes ao corpo numérico $\mathbb{K}$. Por raízes *de uma tal equação entende-se suas soluções que estão em $\mathbb{K}$. Na eventualidade de querermos tratar apenas das soluções que estão em algum conjunto $A \subseteq \mathbb{K}$, falaremos nas* raízes em A *de tal equação.*

Exemplo 10.8 -

Atente o leitor que polinômio e equação polinomial são objetos conceitualmente distintos, embora a literatura elementar tenda a tratá-los como iguais. Assim, $X^3 + 1$ é um polinômio, enquanto que $x^3 + 1 = 0$ é uma equação polinomial.

Exemplo 10.9 -

Note que não há nenhuma ambiguidade na afirmação: "A equação $x^2 + 1 = 0$ não tem nenhuma raiz real, mas tem duas raízes complexas: $x = i$ e $x = -i$."
Contudo, a pergunta: "Quantas raízes tem a equação $x^2 + 1 = 0$?" precisa ser clarificada, dando-se o corpo numérico envolvido (por exemplo: $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$).

Observação 10.10 -

Sendo $n \geqslant 1$ e $a_n \neq 0$, a todo polinômio de coeficientes em um corpo $\mathbb{K}$ e da forma

$$p(X) = a_nX^n + \cdots + a_1X + a_0,$$

está associada a seguinte equação polinomial em $\mathbb{K}$:

$$a_nx^n + \cdots + a_1x + a_0 = 0,$$

a qual pode ser denotada simplesmente por:

$$p(x) = 0.$$

Reciprocamente, toda equação polinomial

$$a_n x^n + \cdots + a_1 x + a_0 = 0\,,$$

determina um polinômio associado, *o qual é* $a_n X^n + \cdots + a_1 X + a_0$.

A seguir, frequentemente trataremos de questões em que não é relevante explicitar o corpo numérico envolvido; nestes casos ficará então subentendido que a discussão se aplica a polinômios ou equações polinomais com coeficientes em qualquer corpo numérico.

A título de um breve lembrete:

- polinômio: expressão envolvendo uma indeterminada;
- equação polinomial: uma relação de igualdade expressa com o uso de um polinômio, e envolvendo números e uma incógnita.

Definição 10.11 -

Por grau de um polinômio não nulo

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

entende-se o maior expoente de X *com coeficiente não nulo na expressão do polinômio. (Aqui devemos ver o termo constante como acompanhado da indeterminada com expoente zero:* $a_0 = a_0 X^0$ *.)*
Semelhantemente, o grau de uma equação polinomial é o grau do polinômio a ela associado.

Exemplo 10.12 -

A equação polinomial $5x^3 - 5x = 2x^2 + 9$*, ou seja,* $5x^3 - 2x^2 - 5x - 9 = 0$*, é de grau 3, pois o polinômio associado,* $5X^3 - 2X^2 - 5X - 9$*, tem grau* 3*.*

O polinômio $p(X) = 3$ *é um polinômio de grau zero, e qualquer outro polinômio constante, desde que não nulo, também tem grau zero.*

10.3 A afirmativa sobre a existência de raízes de equações polinomiais: TFA-existencial

Como já mencionado na introdução deste capítulo, existem vários teoremas semelhantes que são denominados Teorema Fundamental da Álgebra (TFA). Nesta seção trataremos do mais importante deles, o qual trata da *existência de raízes* para equações polinomiais de coeficientes num campo numérico. Na seção a seguir, logo veremos que a combinação adequada de alguns resultados básicos sobre polinômios com esse TFA-existencial nos permitirá determinar a quantidade de raízes das equações polinomiais.

Atrás da simplicidade da afirmação do TFA-existencial também escondem-se muitas sutilezas. Como exemplo, vejamos duas peculiaridades notáveis:

i). Todas as demonstrações até hoje produzidas para esse teorema envolvem argumentos baseados na noção de *continuidade topológica* , o que não apenas foge do âmbito da Álgebra, como do âmbito deste texto.
Nesse sentido, vale comentar que, assim como existem fórmulas algébricas para a resolução das equações polinomiais gerais de grau um a quatro, mas não para as de grau cinco ou superior, também existem demonstrações estritamente algébricas do TFA para equações de grau até quatro, mas não para as de grau cinco ou maior do que cinco. Isso sugere fortemente que há enorme alteração nas propriedades das equações polinomiais ao passarmos de equações de grau até quatro para equações de grau cinco ou maior.

ii). Embora os corpos numéricos que estamos considerando sejam sempre subconjuntos de $\mathbb{C}$, não se pode descartar completamente a possibilidade de existência de conjuntos numéricos "maiores" do que $\mathbb{C}$ que também sejam corpos, ou seja, corpos que contenham $\mathbb{C}$. Relacionado a essa possibilidade, mencionamos o seguinte fato pouco conhecido sobre o TFA: as primeiras tentativas de demonstração do TFA davam como óbvia a existência de raízes das equações polinomiais (raízes estas que estariam em algum corpo numérico, eventualmente maior do que $\mathbb{C}$) e que tudo o que se tinha de demonstrar era que tais raízes estão obrigatoriamente no campo dos números complexos.
Coube ao talento de Karl F. Gauss apontar que a existência de raízes não é um fato óbvio, e que é ilógico se querer deduzir propriedades de um objeto matemático cuja existência ainda não foi provada.

Exercício 324 -

O raciocínio que se segue incorre no mesmo erro lógico que Gauss detectou. Pede-se criticá-lo cuidadosamente:

> *"Mostremos que 1 é o maior inteiro positivo. Com efeito, seja N o maior inteiro positivo. Temos então duas possibilidades: ou $N = 1$, ou $N > 1$. Ora, como a segunda alternativa não é verdadeira (pois ela nos levaria a $N^2 = \text{inteiro} > N = $maior inteiro positivo), segue que tem que valer a primeira opção, ou seja, $N = 1$."*

Teorema 10.13 (*TFA–versão existencial*) -

Toda equação polinomial com coeficientes no corpo dos números complexos tem ao menos uma raiz neste corpo.

Em termos mais completos, a proposição "toda equação polinomial com coeficientes em um corpo $\mathbb{K}$ tem ao menos uma raiz em tal corpo" é verdadeira em um único corpo numérico: $\mathbb{K} = \mathbb{C}$.

A demonstração mais conhecida desse teorema é a primeira entre as várias dadas por Gauss, lá por cerca de 1800, mas dela poderemos apresentar apenas a ideia básica.

Ideia da prova.
Dado um polinômio $p(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$, de coeficientes complexos e grau $n \geqslant 1$, mostremos que a equação $p(z) = 0$ admite uma raiz no corpo dos números complexos. Como a incógnita é um número complexo, será preferível representá-la na forma binomial $z = x + iy$, com $x, y \in \mathbb{R}$. Assim, a equação a resolver fica:

$$\begin{aligned} 0 &= p(z) = p(x+iy) \\ &= a_n(x+iy)^n + a_{n-1}(x+iy)^{n-1} + \cdots + a_1(x+iy) + a_0 . \end{aligned}$$

Se também escrevermos os coeficientes na forma binomial

$$a_k = c_k + id_k ,$$

e separarmos os termos da equação que estão multiplicados por i dos termos que não estão multiplicados por i, veremos que ela pode ser escrita na forma:

$$u(x,y) + iv(x,y) = 0 ,$$

onde $u(X,Y)$ e $v(X,Y)$ são polinômios em duas indeterminadas[2] e de coeficientes reais. Essa "descomplexificação" da equação original mostra que

$$p(x+iy)=0$$

tem raiz se, e só se, existir um par de números reais (x,y) verificando o sistema de equações reais:

$$\begin{cases} u(x,y)=0 \\ v(x,y)=0\,. \end{cases} \tag{10.1}$$

Neste ponto é que entram as contribuições de Gauss. Ele iniciou observando que $u(x,y)=0$ e $v(x,y)=0$ podem ser vistas como equações de curvas do plano cartesiano. Consequentemente, mostrar a existência de uma raiz no campo dos números complexos de nossa equação polinomial equivale a mostrar que as duas curvas, $u(x,y)=0$ e $v(x,y)=0$, têm uma intersecção, ao menos.

Apliquemos essa ideia no caso particular em que a equação $p(z)=0$ tem grau um, ou seja: $az+b=0$. É claro que nesse caso temos uma óbvia solução: $z=-b/a$. Contudo, queremos neste momento apenas ilustrar e explicar a ideia usada por Gauss, e essa situação particular cumpre, significativamente bem, este objetivo.

Escrevendo $a=a_1+ia_2$, e $b=b_1+ib_2$, a equação $az+b=0$ faz com que (10.1) se transforme no sistema linear:

$$\begin{cases} a_1x-a_2y=b_1 \\ a_2x+a_1y=b_2\,. \end{cases} \tag{10.2}$$

Nesse caso particular, mostrar que as curvas $u(x,y)=0$ e $v(x,y)=0$ têm ao menos uma intersecção significa mostrar que as retas $a_1x-a_2y=b_1$ e $a_2x+a_1y=b_2$ se cortam. Ora, isto é o que efetivamente ocorre, porque o determinante da matriz principal

$$A=\begin{bmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{bmatrix}$$

do sistema (10.2) é não nulo. Com efeito: $\det A=a_1^2+a_2^2=|a|^2\neq 0$, pois $a\neq 0$.

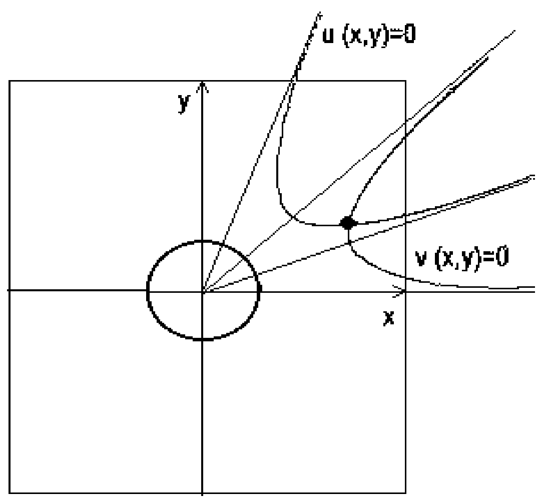
No caso em que o grau de $p(X)$ é maior ou igual a 2, a prova de existência de um ponto de intersecção das curvas $u(x,y)=0$ e $v(x,y)=0$ é muito mais difícil, mesmo

[2]Um polinômio nas indeterminadas X e Y, e com coeficientes em um corpo numérico $\mathbb{K}$, é uma expressão da forma $a_0+a_{11}XY+\cdots+a_{ij}X^iY^j+\cdots+a_{mn}X^mY^n$, onde m e n são naturais, e $a_0,a_{11},\ldots,a_{ij},\ldots,a_{mn}$ são elementos de $\mathbb{K}$.

no caso de o grau de $p(X)$ valer 2. Faremos no que se segue uma argumentação heurística, resumindo as ideias de Gauss. O ponto crucial do seu argumento consiste em olhar o aspecto das curvas $u(x, y) = 0$ e $v(x, y) = 0$ bem longe da origem do sistema de coordenas cartesianas.

Notando que a curva $u(x, y) = 0$ foi originada por uma equação polinomial complexa de grau $n \geqslant 2$, e que, bem longe da origem, o comportamento de curvas polinomiais é decidido pelos termos de maior grau, Gauss não teve dificuldades maiores para mostrar que a curva $u(x, y) = 0$ tem um ramo (ou "pedaço" contínuo) um dos lados do qual é assintótico [3] a uma reta fazendo um ângulo de $\alpha = 180/2n$ graus com o eixo x, e o outro lado do ramo é assintótico a uma reta fazendo um ângulo de 3α graus com o mesmo eixo. Confira na figura a seguir.

Semelhantemente, ele mostrou que a curva $v(x, y) = 0$ tem um ramo que de um lado é assintótico a uma reta fazendo um ângulo de 2α graus com o eixo x, e do outro lado é assintótico ao mesmo eixo. Ora, conforme mostra a figura, a continuidade desses ramos, aliada com seus comportamentos assintóticos, faz com que os mesmos tenham de se interceptar, conforme queríamos mostrar.



[3]Os termos *assintótico* e *assíntota* têm um significado preciso que pode ser enunciado de forma rigorosa usando a noção de limite, estudada em cursos de Cálculo Infinitesimal. Entretanto, ainda que aqui não tenhamos como abordar de maneira completa essa noção, a situação acima descrita fica intuitivamente clara observando-se o correspondente desenho.
(Nos exercícios que seguem, o leitor terá a oportunidade de trabalhar com casos concretos da noção de assíntota.)

CQD.

Exercício 325 -

Mostre que, para x real muito grande, os valores de $p(x) = x^2 + 1000x + 500$ e $q(x) = x^2$ tendem a se confundir.
Sugestão: estude o comportamento de seu quociente.

Exercício 326 -

Para o polinômio complexo $p(Z) = Z^2 + 1$, pede-se:

i). determinar os polinômios $u(X,Y)$ e $v(X,Y)$ mencionados na última demonstração;

ii). desenhar as curvas $u(x,y) = 0$ e $v(x,y) = 0$, e verificar se elas têm assíntotas como foram caracterizadas na demonstração do último teorema;

[*Sugestão: use que $\sqrt{1+x^2} \simeq |x|$, para x muito grande.*]

iii). determinar as intersecções das curvas $u(x,y) = 0$ e $v(x,y) = 0$, e conferir se elas correspondem aos valores esperados: $\pm i$.

iv). Uma crítica que se faz ao rigor da prova de Gauss, anteriormente mencionada, insiste que a intersecção das curvas $u(x,y) = 0$ e $v(x,y) = 0$ não precisa ocorrer muito distante da origem; pede-se examinar isso.

Exercício 327 -

No caso de $p(Z) = Z^3 - 2i$, mostre que os polinômios $u(X,Y)$ e $v(X,Y)$ mencionados na última demonstração são dados por

$$u(X,Y) = X^3 - 3XY^2 \ \ e \ \ v(X,Y) = 3X^2Y - Y^3 - 2.$$

Observação 10.14 -

Já sabemos que existem equações polinomiais de coeficientes reais que não têm nenhuma raiz real, como é o caso de $x^2 + 1 = 0$. Contudo, tais equações sempre têm raízes no corpo dos números complexos; no caso de $x^2 + 1 = 0$, essas raízes são $x = i$ e $x = -i$.

É um exercício interessante o leitor verificar se existe algum corpo, intermediário entre $\mathbb{R}$ e $\mathbb{C}$, contendo as raízes dessa equação.

10.4 Resultados iniciais sobre igualdade e fatoração de polinômios

Convenções

Todos os polinômios desta seção são considerados como tendo coeficientes num mesmo corpo numérico $\mathbb{K}$.

A seguir, definiremos as operações aritméticas com polinômios, assunto que não deve ser novidade para o leitor. Para facilitar essas definições – dados dois polinômios, talvez, de graus distintos – usaremos o expediente de escrever termos nulos, tipo $0X^k$, para fazer com que os polinômios tenham as mesmas potências de X. Exemplo: X^2+1 e X^3-X^2+X ficarão, respectivamente: $0X^3+X^2+0X+1$ e X^3-X^2+X+0.

Definição 10.15 (*Operações com polinômios*) -

Dados polinômios $p(X) = a_nX^n + \cdots + a_0$ *e* $q(X) = b_nX^n + \cdots + b_0$ *definimos*

– *a soma de* $p(X)$ *com* $q(X)$ *como sendo o polinômio*

$$(a_n + b_n)X^n + \cdots + (a_0 + b_0),$$

que denotaremos por $p(X) + q(X)$ *;*

– *a diferença entre* $p(X)$ *e* $q(X)$ *como sendo o polinômio*

$$(a_n - b_n)X^n + \cdots + (a_0 - b_0),$$

que denotaremos por $p(X) - q(X)$.

– *o produto de* $p(X)$ *com* $q(X)$ *; como sendo o polinômio*

$$c_{2n}X^{2n} + c_{2n-1}X^{2n-1} + \cdots + c_0,$$

que denotaremos por $p(X) \cdot q(X)$, *ou mesmo* $p(X)q(X)$, *onde cada coeficiente* c_k, *para* $k \in \{0, \ldots, 2n\}$ *, é dado por*

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0\,.$$

Note que, pelo fato de estarmos trabalhando num corpo numérico, temos garantido que os polinômios soma, diferença e produto ainda estão com coeficientes neste corpo numérico.

Exemplo 10.16 -

Tratemos de somar e multiplicar $p(X) = 3X^2 + 5X$ *e* $q(X) = 5X^3 - 2X^2 + 9$*. Para isso, iniciamos pensando em* $p(X) = 0X^3+3X^2+5X+0$ *e* $q(X) = 5X^3-2X^2+0X+9$ *e, então, calculamos:*

$$\begin{aligned} p(X) + q(X) &= (0+5)X^3 + (3+(-2))X^2 + (5+0)X + (0+9) \\ &= 5X^3 + X^2 + 5X + 9, \end{aligned}$$

enquanto que

$$\begin{aligned} p(X)q(X) &= (3\times 5)X^5 + (3\times(-2) + 5\times 5)X^4 + (3\times 0 + 5\times(-2))X^3 + \\ &\quad (3\times 9 + 5\times 0 + 0\times(-2))X^2 + (5\times 9 + 0\times 0)X + 0\times 9 \\ &= 15X^5 + 19X^4 - 10X^3 + 27X^2 + 45X. \end{aligned}$$

Exercício 328 -

Mostre que dois polinômios são iguais se, e só se, a diferença entre eles for o polinômio nulo.

Exercício 329 -

Prove, a partir da Definição 10.15, que

$$X^r X^s = X^{r+s}\,.$$

Exercício 330 -

Mostre que a multiplicação de polinômios com coeficientes num corpo numérico $\mathbb{K}$ *tem a propriedade da integridade. Ou seja, sendo* $p(X)$ *e* $q(X)$ *dois polinômios, então* $p(X)q(X)$ *é o polinômio nulo se, e somente se, algum deles for o polinômio nulo. Em particular:*

$$p(X)q(X) = 0 \;\text{ e }\; p(X) \neq 0 \Rightarrow q(X) = 0\,.$$

Exercício 331 (*anel dos polinômios*) -

Prove que, como estamos lidando com coeficientes num corpo numérico, as operações de adição e multiplicação de polinômios satisfazem as seguintes propriedades:

i). a adição é comutativa, é associativa, tem elemento neutro e admite simétricos;

ii). a multiplicação é comutativa, é associativa, tem elemento neutro e é distributiva em relação à adição.

Exercício 332 -

Indicando por $\mathbb{K}[X]$ *o conjunto de todos os polinômios de indeterminada* X *e de coeficientes em* $\mathbb{K}$*, e usando os resultados dos dois exercícios anteriores, verifique que* $[\,\mathbb{K}[X], +\,, \cdot\,]$*, semelhantemente ao que foi mostrado no Capítulo 2 para* $[\mathbb{Z}, +\,, \times\,]$*, tem estrutura de anel de integridade.*

Sabendo operar com polinômios, podemos estabelecer algumas importantes *identidades polinomiais* envolvendo fatoração.

Proposição 10.17 -

Sempre $X - a$ *é um fator de* $X^n - a^n$*, quaisquer que sejam* $n \geqslant 2$ *inteiro e* $a \in \mathbb{K}$*. Ou seja, existe um polinômio* $q(X)$*, com coeficientes também em* $\mathbb{K}$*, tal que:*

$$X^n - a^n = (X - a) \cdot q(X)\ .$$

Prova:

Basta verificarmos, por multiplicação direta, as seguintes identidades (note que as mesmas já dão explicitamente a expressão do polinômio $q(X)$):

$$\begin{aligned}
X^2 - a^2 &= (X - a)(X + a)\\
X^3 - a^3 &= (X - a)(X^2 + aX + a^2)\\
X^4 - a^4 &= (X - a)(X^3 + aX^2 + a^2X + a^3)\\
&\cdots\\
X^n - a^n &= (X - a)(X^{n-1} + aX^{n-2} + a^2X^{n-3} + \cdots + a^{n-2}X + a^{n-1})\,.
\end{aligned} \tag{10.3}$$

CQD.

Exercício 333 -

Complete os detalhes da prova da Proposição 10.17.

Como as regras para operar com a indeterminada X são as mesmas que para operar com um número qualquer b do corpo numérico $\mathbb{K}$, segue que as identidades polinomiais (10.3) geram igualdades numéricas verificadas para quaisquer $a, b \in \mathbb{K}$. Por exemplo:

$$b^3 - a^3 = (b-a)(b^2 + ab + a^2)\,,\ \forall a, b \in \mathbb{K}.$$

Também é imediato ver que vale o seguinte resultado mais geral:

Teorema 10.18 -

Sendo $p(X)$ e $q(X)$ dois polinômios com coeficientes em um mesmo corpo numérico, se vale a igualdade polinomial $p(X) = q(X)$, então valerá a igualdade numérica $p(a) = q(a)$, para todos os infinitos valores de a no corpo numérico.

A recíproca desse teorema será enunciada mais adiante (veja Corolário 10.27).

Teorema 10.19 (*teorema da fatoração*) -

Trabalhando em corpos numéricos, sempre que uma equação polinomial $p(x) = 0$ tiver uma raiz α, o respectivo polinômio $p(X)$ admitirá o polinômio $X - \alpha$ como fator. Ou seja, para um apropriado polinômio $q(X)$, também com coeficientes neste corpo numérico, vale a identidade polinomial:

$$p(X) = (X - \alpha)q(X).$$

Prova:

Suponhamos

$$p(X) = a_n X^n + \cdots + a_0.$$

Ora, sendo α raiz da equação $p(x) = 0$, temos $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Daí, podemos escrever:

$$\begin{aligned} p(X) &= p(X) - 0 \\ &= (a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0) - (a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\ &= a_n(X^n - \alpha^n) + a_{n-1}(X^{n-1} - \alpha^{n-1}) + \cdots + a_1(X - \alpha). \end{aligned}$$

Resta observar que, pela Proposição 10.17, cada parênteses do segundo membro da última igualdade pode ser fatorado por $(X - \alpha)$.

CQD.

Teorema 10.20 -

Num corpo numérico, sempre que um polinômio $p(X)$ puder ser fatorado como $p(X) = (X - \alpha)q(X)$, para um apropriado número α do corpo e um polinômio $q(X)$ de coeficientes neste corpo, poderemos afirmar que α é uma raiz da equação polinomial $p(x) = 0$. Ou seja:

$$p(X) = (X - \alpha)q(X) \Rightarrow p(\alpha) = 0\,.$$

Além disso, essa fatoração nos permite reduzir o trabalho da determinação das eventuais outras raízes de $p(x) = 0$ à determinação das raízes de $q(x) = 0$. Mais precisamente: o conjunto das raízes da equação $p(x) = 0$ tem como elementos α e as eventuais raízes da equação $q(x) = 0$.

Prova:

É imediato que α é raiz de $p(x) = 0$. Por outro lado, a fatoração dada nos permite ver que toda raiz de $q(x) = 0$ tem de ser raiz de $p(x) = 0$. Reciprocamente, se um $\beta \neq \alpha$ for raiz de $p(x) = 0$, teremos $0 = p(\beta) = (\beta - \alpha)q(\beta)$. Simplificando o fator $(\beta - \alpha) \neq 0$, segue que $q(\beta) = 0$.

CQD.

Exemplo 10.21 -

No caso do polinômio $p(X) = X^3 + 5X^2 + 17X$, é imediato que

$$p(X) = X(X^2 + 5X + 17),$$

e portanto, 0 é uma raiz da equação polinomial $p(x) = 0$. Para determinarmos as demais raízes reais dessa equação cúbica, basta resolvermos a equação quadrática:

$$x^2 + 5x + 17 = 0\,.$$

Teorema 10.22 (*teorema da fatoração repetida*) -

Trabalhando num corpo numérico, sempre que conhecermos uma sequência de raízes (distintas) $\alpha_1, \alpha_2, \dots, \alpha_k$ de uma mesma equação polinomial $p(x) = 0$, valerá uma fatoração de $p(X)$ da forma

$$p(X) = (X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_k)q(X),$$

para algum polinômio $q(X)$.

Prova:

Pelo teorema da fatoração, temos $p(X) = (X - \alpha_1)q_1(X)$, para algum polinômio $q_1(X)$ apropriado. Pelo Teorema 10.20, $\alpha_2, \ldots, \alpha_k$ têm de ser raízes de $q_1(x) = 0$.

Uma nova aplicação do teorema da fatoração, agora ao polinômio $q_1(X)$, mostra que $q_1(X) = (X - \alpha_2)q_2(X)$, para um polinômio $q_2(X)$ apropriado. Consequentemente, podemos escrever

$$p(X) = (X - \alpha_1)(X - \alpha_2)q_2(X)$$

e afirmar, por nova aplicação do raciocínio da prova do Teorema 10.20, que $\alpha_3, \ldots, \alpha_k$ têm de ser raízes de $q_2(x) = 0$. O argumento pode ser repetido até chegarmos à raiz α_k. CQD.

Teorema 10.23 (*teorema da enumeração finita*) -

Toda equação polinomial, de grau $n \geqslant 1$ e coeficientes num corpo numérico $\mathbb{K}$, ou não tem nenhuma raiz em $\mathbb{K}$, ou tem de uma a n raízes em $\mathbb{K}$.

Prova:

Seja $p(x) = 0$ a equação dada. Mostremos que, se a mesma tiver raízes, a quantidade delas não pode ser maior do que n. Com efeito, por absurdo, se a equação admitisse $n+1$, ou mais, raízes, $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$, o teorema da fatoração repetida nos permitiria escrever:

$$p(X)(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)(X - \alpha_{n+1})q(X)\,.$$

Ora, temos duas alternativas:

- ou o polinômio $q(X)$ é nulo, e isto implica $p(X)$ nulo: absurdo;
- ou $q(X)$ não é nulo, e isto faz que o produto da direita seja um polinômio de grau $\geqslant n+1$, logo maior do que o grau de $p(X)$: absurdo.

CQD.

Exemplo 10.24 -

Para a equação de grau $n = 2$: $x^2 - 2 = 0$, pode-se afirmar:
– A equação não tem raízes no corpo numérico $\mathbb{K} = \mathbb{Q}$.
– No corpo numérico $\mathbb{K} = \mathbb{R}$, é imediato verificar que a equação tem duas raízes:

$\sqrt{2}$ e $-\sqrt{2}$; então, pelo teorema, ela só pode ter estas raízes. Com efeito, podemos confirmar diretamente que $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Observação 10.25 -

Não deixe o leitor de observar que o teorema anterior não aborda as equações triviais, $p(x) = 0$, com $p(X)$ polinômio constante. Se um tal polinômio for uma constante não nula, a equação $p(x) = 0$ não tem nenhuma raiz; se for o polinômio nulo, a equação tem infinitas raízes.

Corolário 10.26 -

Sempre que a equação polinomial

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

admitir $n + 1$ ou mais raízes, poderemos afirmar que $a_n = \ldots = a_1 = a_0 = 0$.

Exercício 334 -

Prove o Corolário 10.26.

O corolário a seguir é a recíproca do Teorema 10.18:

Corolário 10.27 -

Sejam $p(X)$ e $q(X)$ dois polinômios de coeficientes num mesmo corpo numérico, ambos não nulos e graus $\leqslant n$. Se valer a igualdade numérica $p(a) = q(a)$, para $n + 1$ valores distintos de a no corpo, então $p(X) = q(X)$.

Prova:

Valendo a igualdade numérica $p(a) = q(a)$ para $n + 1$ valores distintos de a em um corpo numérico, teremos que a equação polinomial $p(x) - q(x) = 0$ terá mais de n raízes neste corpo. Ora, isso – segundo o Teorema da enumeração finita – só pode ocorrer quando $p(X) - q(X) = 0$, ou seja: quando os polinômios $p(X)$ e $q(X)$ forem iguais.

CQD.

Exercício 335 -

Pede-se apontar o erro no raciocínio a seguir, e então corrigí-lo.

"Suponha que $a + bx = c + dx + ex^2$, para todos os valores de x no corpo numérico dos coeficientes a, b, c, d, e. Fazendo $x = 0$, obtemos $a = c$. Daí, ficamos com $a+bx = a+dx+ex^2$, para todos os valores de x. Consequentemente, $bx = dx+ex^2$, para todos os valores de x. Simplificando, obtemos $b = d+ex$. Novamente tomando $x = 0$, obtemos dessa última igualdade que $b = d$. Consequentemente, a igualdade inicial pode ser reescrita como $a + bx = a + bx + ex^2$. Dela, sai que $ex^2 = 0$, para todos os x. Tomando $x = 1$, obtemos $e = 0$. Resumindo: $a = c$, $b = d$, $e = 0$."

Exercício 336 -

Simplifique ao máximo que puder a seguinte expressão algébrica, sabendo que a, b, c são números reais, distintos dois a dois:

$$\frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-c)(x-a)}{(b-c)(b-a)}\,.$$

10.5 O problema da enumeração das raízes de equações polinomiais: TFA-enumerativo

Convenção:
no que segue, nosso interesse estará focado no estudo das equações polinomiais e não nos polinômios em si, por isso convencionaremos que:

> quando falarmos em *equação polinomial*, sempre estaremos supondo que a mesma corresponda a um polinômio que não seja constante, tendo, então, grau $\geqslant 1$.

Por si só, os resultados anteriores ainda são bastante pobres em utilidade prática. Por exemplo, se formos defrontados com a equação $x^5 - x - 1 = 0$, por enquanto, tudo o que podemos dizer é que ela terá de uma a cinco raízes no campo dos números complexos. Obviamente, seria muito mais útil se pudessemos afirmar a quantidade exata de raízes dessa equação. Para chegarmos a isso, será fundamental abrirmos a possibilidade de, para certos casos especiais que caracterizaremos cuidadosamente adiante, pudermos contar uma mesma raiz mais de uma vez. A maneira que faremos isso é baseada na seguinte:

Definição 10.28 -

Dizemos que um número α é **raiz de multiplicidade** *s de uma equação polinomial $p(x) = 0$ se, e só se, valer uma fatoração do tipo*

$$p(X) = (X - \alpha)^s q(X)\,,$$

onde $q(X)$ é um polinômio verificando $q(\alpha) \neq 0$.
Quando $s = 1$ dizemos que a raiz é **simples**, *e quando $s = 2, 3, 4, \ldots$, dizemos que a raiz é, respectivamente,* **dupla**, **tríplice**, **quádrupla** , *etc.*

Exemplo 10.29 -

Relativamente à equação $x^3 - 4x^2 + 5x - 2 = 0$, como vale a fatoração

$$X^3 - 4X^2 + 5X - 2 = (X - 1)^2(X - 2)\,,$$

segue que ela tem uma raiz dupla ($x = 1$) e uma raiz simples ($x = 2$).

Lema 10.30 -

Se para todos os valores de x num corpo numérico tivermos uma igualdade do tipo:

$$(x - \alpha)^{s_1} q_1(x) = (x - \alpha)^{s_2} q_2(x) \tag{10.4}$$

onde $q_1(X)$ e $q_2(X)$ são polinômios, e s_1 e s_2 são números verificando $s_1 < s_2$, então α é raiz da equação $q_1(x) = 0$. Ademais, para todos os valores de x, inclusive $x = \alpha$, vale

$$q_1(x) = (x - \alpha)^{s_2 - s_1} q_2(x).$$

Prova:

Dividindo ambos os lados de (10.4) por $(x - \alpha)^{s_1}$, para $x \neq \alpha$, ficamos com $q_1(x) = (x - \alpha)^{s_2 - s_1} q_2(x)$, para todos os $x \neq \alpha$. Resta aplicarmos o Corolário 10.27.

CQD.

O resultado a seguir é esperado e poderia parecer que é de demonstração óbvia. Contudo, isto não ocorre, pois precisamos evitar divisões por zero (recorde o Exercício 335).

Teorema 10.31 -

Em corpos numéricos, a cada raiz de uma equação polinomial fica atribuído um único grau de multiplicidade.

Prova:

– Existência do grau de multiplicidade.
Pela convenção feita quanto ao uso da expressão "equação polinomial", estamos tratando com um polinômio $p(X)$ de grau $n \geqslant 1$, e a hipótese nos diz que existe um número α que é raiz da equação polinomial $p(x) = 0$. Pelo teorema da fatoração, temos

$$p(X) = (X - \alpha)p_1(X),$$

onde $p_1(X)$ tem de ser um polinômio de grau $n - 1$.

Se $p_1(\alpha) \neq 0$, temos $s = 1$. Se $p_1(\alpha) = 0$, como $p_1(X)$ não pode ser o polinômio identicamente nulo (pois a fatoração mencionada faria com que também $p(X)$ fosse identicamente nulo), o teorema da fatoração nos diz que tem de valer uma igualdade

$$p_1(X) = (X - \alpha)p_2(X),$$

e então

$$p(X) = (X - \alpha)^2 p_2(X),$$

para algum polinômio não identicamente nulo $p_2(X)$.

Daí, se $p_2(\alpha) \neq 0$, temos $s = 2$. Se $p_2(\alpha) = 0$, repetimos com $p_2(X)$ o raciocínio feito com $p_1(X)$, e assim sucessivamente. Desse modo, produziremos uma sequência de polinômios não identicamente nulos $p_1(X), p_2(X), \ldots$ de graus diminuindo gradativamente: $n-1, n-2, \ldots$. Fica fácil vermos que o mais longe que esse processo poderá ir é até $p_n(X)$, que tem de ser um polinômio de grau zero, isto é, constante não nulo ($p_n(X) = c \neq 0$), o que nos daria a fatoração

$$p(X) = (X - \alpha)^n p_n(X) = c\,(X - \alpha)^n,$$

a qual implicaria $s = n$. Consequentemente, a cada raiz α da equação $p(x) = 0$, podemos atribuir uma multiplicidade s, que será um valor entre 1 e n.

– Unicidade do grau de multiplicidade.
Iniciamos observando que se ocorresse $(x - \alpha)^{s_1} q_1(x) = p(x) = (x - \alpha)^{s_2} q_2(x)$ para

todos os valores de x no tal corpo – supondo $s_1 < s_2$ e $q_1(\alpha) \neq 0, q_2(\alpha) \neq 0$ – bastaria aplicar o Lema 10.30 para concluirmos que

$$q_1(x) = (x-\alpha)^{s_2-s_1} q_2(x),$$

para todos os valores de x, inclusive $x = \alpha$, e isso nos levaria ao absurdo $q_1(\alpha) = 0$.

CQD.

Exemplo 10.32 -

Para a equação $x^3 - 4x^2 + 5x - 2 = 0$ do exemplo 10.29, podemos dizer que temos uma raiz dupla ($x = 1$) e uma raiz simples ($x = 2$). Por isso, dizemos que esta equação tem três raízes reais: $x = 1$ (que é contada duas vezes) e $x = 2$.

Exemplo 10.33 -

Como a equação $(x-1)^3 = 0$ tem uma raiz tríplice, dizemos que ela tem três raízes iguais.

Exemplo 10.34 -

As equações $(x-1)(x-2)(x-3) = 0$, $(x-1)^2(x-2) = 0$ e $(x-1)^3 = 0$ têm, todas elas, três raízes. Com efeito, elas têm, respectivamente: três raízes simples; uma dupla e uma simples; e uma tríplice. Também dizemos que elas têm, respectivamente, três, duas e uma raízes distintas.

Teorema 10.35 (*TFA - versão enumerativa*) -

Toda equação polinomial de grau $n \geqslant 1$, e coeficientes no corpo dos números complexos, tem exatamente n raízes neste corpo, entendendo-se que contamos cada raiz tantas vezes quanto valer sua multiplicidade.

Prova:

Escrevamos o polinômio associado à equação dada como $p(X)$. Pelo TFA-versão existencial, a equação $p(x) = 0$ admite ao menos uma raiz α_1 no corpo dos números complexos. Consequentemente, pelo teorema da fatoração (Teorema 10.19), podemos escrever, para algum polinômio $q_1(X)$ de grau $n-1$,

$$p(X) = (X - \alpha_1) q_1(X).$$

Se tal $q_1(X)$ não for um polinômio constante, uma aplicação do TFA-versão existencial à equação $q_1(x) = 0$, combinada com o Teorema 10.19, nos garante a existência de um número complexo α_2, que é raiz tanto de $q_1(x) = 0$ como de $p(x) = 0$, bem como garante uma fatoração para $p(X)$ da forma

$$p(X) = (X - \alpha_1)(X - \alpha_2)q_2(X),$$

para algum polinômio $q_2(X)$ de grau $n - 2$.

Se tal $q_2(X)$ não for um polinômio constante, repetimos com ele o que fizemos com $q_1(X)$, bem como com os polinômios $q_3, q_4, \ldots$ que irão surgindo com a repetição do raciocínio. É fácil vermos que esse processo de sucessivas reduções de grau só parará com a obtenção de um polinômio $q_k(X)$ constante, o que só vai ocorrer quando $k = n$. Nesta última etapa teremos:

$$p(X) = (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n)q_n(X) = c(X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n)\,,$$

onde c é o valor do polinômio constante $p_n(X)$.

Comparando os termos de grau n da esquerda e da direita da última igualdade, vemos que: $a_nX^n = cX^n$, logo $c = a_n$; ou seja, tem de valer a fatoração:

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0 = a_n(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)\,.$$

Em particular, está provado que a equação $p(x) = 0$ tem n raízes, possivelmente repetidas.

Resta provarmos que cada raiz é repetida tantas vezes quanto for o valor de sua multiplicidade. Para demonstrarmos isso, iniciemos denotando por $\beta_1, \beta_2, \ldots, \beta_m$ os valores *distintos* das raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ (em particular, $m \leqslant n$), e agrupando os fatores iguais, reescrevamos a nova fatoração como:

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0 = a_n(X - \beta_1)^{s_1}(X - \beta_2)^{s_2}\cdots(X - \beta_m)^{s_m}\,.$$

Assim, tudo o que nos resta fazer é provar que cada s_k é a multiplicidade da raiz β_k. Ora, isso é imediato, pois a fatoração nos diz que: $p(X) = (X - \beta_k)^{s_k}q_k(X)$, onde $q_k(\beta_k) \neq 0$, e então basta apelarmos para a definição de multiplicidade para podermos afirmar que β_k é raiz de multiplicidade s_k.

CQD.

Exemplo 10.36 -

Embora a equação real $x^2 + 1 = 0$ não tenha nenhuma raiz no corpo dos números reais, o TFA garante que ela tem exatamente duas raízes no corpo dos complexos. Com efeito, elas são $x = i$ e $x = -i$, pois $(X - i)(X + i) = X^2 - i^2 = X^2 + 1$.

10.6 O problema da fatoração de polinômios: TFA-fatoração

A investigação da possibilidade de se fatorar polinômios iniciou somente por cerca de 1700, quando se passou a tratar da integração das frações racionais, $p(x)/q(x)$ (assunto estudado em Cálculo Integral). Com efeito, tendo-se descoberto como fazer a integração das frações racionais da forma $1/(ax+b)$ e $1/(ax^2+bx+c)$, onde os coeficientes a, b, c são números reais, viu-se que ficaria fácil fazer a integração das frações mais gerais, da forma $p(x)/q(x)$, *desde que* se soubesse fatorar, em termos de fatores lineares e/ou quadráticos reais, qualquer polinômio de coeficientes reais, Esse problema mostrou-se ser nada trivial, pois garantir a existência desse tipo de fatoração – conforme veremos – equivale a provar uma outra versão do Teorema Fundamental da Álgebra: a chamada "versão fatoração"do TFA.

É importante o leitor observar que falamos nas frações $1/(ax+b)$ e $1/(ax^2+bx+c)$, e não apenas nas do primeiro tipo, pois pode ocorrer (como é o que o acontece com x^2+1) que ax^2+bx+c não possa ser redutível a um produto de fatores lineares *reais*. Ter de incluir as frações $1/(ax^2+bx+c)$ era um preço a pagar em todo aquele tempo em que os números complexos foram vistos com muita suspeita e pouca legitimidade.

Assim, historicamente – e, ainda hoje, em alguns problemas – o grande desafio era escrever qualquer polinômio real como um produto de fatores reais com o menor grau possível. A versão do TFA que passaremos a examinar mostra que isso sempre é possível com fatores reais de no máximo grau dois.

Exercício 337 -

No início dessa investigação, o conhecimento dos números complexos ainda estava tão precário que nada menos do que Leibniz acabou concluindo que $p(X) = X^4 + 1$ *não teria uma fatoração real com fatores de no máximo grau dois. Passaram-se* 50 *anos até que Euler mostrou que Leibniz estava errado, uma vez que vale:*

$$X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1).$$

A partir da decomposição acima, é um exercício fácil, que deixamos para o leitor, mostrar que o polinômio dado não tem fatoração linear real, embora tenha fatoração linear complexa.

Teorema 10.37 (*TFA–versão fatoração linear*) -

O conhecimento de todas as raízes (talvez repetidas), $\alpha_1, \alpha_2, \ldots, \alpha_n$, de uma equação polinomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$, de grau n e cujos coeficientes são números complexos, nos permite escrever a fatoração do polinômio associado:

$$\begin{aligned} &a_n X^n + a_{n-1}X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0 \\ &= a_n (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n). \end{aligned}$$

Equivalentemente, indicando por $\beta_1, \beta_2, \ldots, \beta_m$ os valores distintos das raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ e agrupando os fatores iguais, podemos reescrever a fatoração anterior como

$$\begin{aligned} &a_n X^n + a_{n-1}X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0 \\ &= a_n (X - \beta_1)^{s_1}(X - \beta_2)^{s_2}\cdots(X - \beta_m)^{s_m}, \end{aligned}$$

onde $s_1, s_2, \ldots, s_m$ são as multiplicidades das raízes.

Prova:

Podemos ver o TFA–versão enumerativa como uma abreviação do presente teorema, sendo que a prova daquela versão cobre perfeitamente bem tudo o que aqui está sendo afirmado. CQD.

Observação 10.38 -

Esse teorema mostra mais claramente o significado da ideia de raiz múltipla. O leitor, quando tiver estudado a noção de limite, poderá obter um entendimento ainda maior, sendo capaz de ver que, por exemplo, uma raiz dupla é o que resulta quando duas raízes simples aglutinam-se. Uma outra maneira de captarmos o significado de raiz múltipla é através do gráfico cartesiano da função polinomial associada. Os detalhes disso tudo são vistos no Cálculo Diferencial.

Exercício 338 -

Mostre que 2 *é uma raiz para a equação polinomial*

$$x^7 - 11x^6 + 49x^5 - 115x^4 + 160x^3 - 152x^2 + 112x = 48.$$

A seguir, determine a multiplicidade de 2 *como raiz de tal equação.*

Com a noção de múltiplicidade de raiz, melhoremos o enunciado do Corolário 9.40:

Teorema 10.39 -

Se uma equação polinomial de coeficientes reais *tiver uma raiz complexa* $a + bi$, *ela admitirá também o complexo conjugado* $a - bi$ *como raiz e ambas terão a mesma multiplicidade.*

Prova:

Sendo $p(X)$ o polinômio associado, como seus coeficientes são reais, o Corolário 9.39 implica a igualdade $p(\bar{z}) = \overline{p(z)}$, para todos os números complexos z. De modo que

$$\begin{aligned} z \text{ é raiz de } p(x) = 0 &\iff \\ p(z) = 0 &\iff \\ \overline{p(z)} = 0 &\iff \\ p(\bar{z}) = 0 &\iff \\ \bar{z} \text{ é raiz de } p(x) = 0, & \end{aligned}$$

como queríamos demonstrar. CQD.

Corolário 10.40 -

Todo polinômio de coeficientes reais, cuja equação associada tenha raízes complexas, tem fator quadrático real.

Prova:

Esse resultado é conseqüência do teorema anterior e da identidade:

$$[X - (a + bi)][X - (a - bi)] = X^2 - 2aX + (a^2 + b^2)\,.$$

CQD.

Teorema 10.41 (*TFA–versão fatoração real*) -

Qualquer polinômio $p(X)$ de coeficientes reais pode ser fatorado no corpo dos números reais, em termos de fatores reais lineares e/ou fatores reais quadráticos.

Prova:

É uma consequência do TFA–versão fatoração linear. Com efeito, por esse teorema, cada raiz real dá origem a um *fator linear real*. Quanto às raízes complexas, como o polinômio é suposto ter coeficientes reais, elas ocorrem em pares conjugados e, pelo Corolário 10.40, os respectivos fatores lineares *complexos* dão origem a um *fator quadrático real*. CQD.

Exemplo 10.42 -

Do Exercício 337, temos que o polinômio X^4+1 admite a fatoração quadrática real:

$$X^4+1=(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)\,,$$

a qual não pode ser reduzida a fatores lineares reais.

Exercício 339 -

Determinar a fatoração quadrática real do polinômio X^4+1, partindo da identidade $X^4+1=(X^2+1)^2-2X^2$.

Exercício 340 -

Determinar uma fatoração real linear/quadrática para o polinômio

$$p(X)=1+X+X^2+X^3\,.$$

10.7 Relação entre coeficientes e raízes de equações polinomiais

Cardano descobriu que em certas cúbicas a soma das raízes iguala o negativo do coeficiente do termo quadrático. Logo se conseguiu mostrar que a soma dos produtos dos pares dessas raízes dava o coeficiente do termo linear. Isso levou a se pensar na possibilidade de se relacionar somas de produtos de raízes com os coeficientes das equações polinomiais quaisquer. Ora, essa possibilidade depende de um resultado mais básico: toda equação polinomial de grau n deve ter o mesmo número n de raízes. Essa afirmação, conforme já vimos, corresponde à versão enumerativa do Teorema Fundamental da Álgebra e implica a adoção da ideia de multiplicidade de uma raiz.

As relações gerais que estamos por enunciar e demonstrar estão associadas aos nomes de Viète e Newton, e requerem um certo cuidado notacional. Para que possamos perceber claramente as ideias envolvidas, iniciemos com o caso particular das equações quadráticas e cúbicas.

Teorema 10.43 (*Fórmulas de Newton-Viète (caso grau 2)*) -

Indicando por α_1, α_2 as raízes (reais ou complexas, distintas ou não) de uma equação quadrática de coeficientes reais ou complexos, $ax^2 + bx + c = 0$, temos que valem as relações

$$\alpha_1 + \alpha_2 = -b/a \quad e \quad \alpha_1\alpha_2 = c/a.$$

Prova:

Pelo TFA–versão fatoração linear:

$$aX^2 + bX + c = a(X - \alpha_1)(X - \alpha_2),$$

de modo que, efetuando os produtos envolvidos no membro da direita, obtemos:

$$aX^2 + bX + c = aX^2 - a(\alpha_1 + \alpha_2)X + a\alpha_1\alpha_2.$$

Resta usar a caracterização de igualdade polinomial em termos da igualdade entre os correspondentes coeficientes estabelecida na Definição 10.4. CQD.

Teorema 10.44 (*Fórmulas de Newton-Viète (caso grau 3)*)-

Indicando por α_1, α_2, α_3 as raízes (reais ou complexas, distintas ou não) de uma equação cúbica de coeficientes reais ou complexos, $ax^3 + bx^2 + cx + d = 0$, temos *que valem as relações:*

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= -b/a \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= c/a \\ \alpha_1\alpha_2\alpha_3 &= -d/a. \end{aligned}$$

Prova:

Pelo TFA–versão fatoração linear:

$$aX^3 + bX^2 + cX + d = a(X - \alpha_1)(X - \alpha_2)(X - \alpha_3),$$

de modo que, efetuando os produtos envolvidos no membro da direita, obtemos:

$$\begin{aligned} &aX^3 + bX^2 + cX + d \\ &= aX^3 - a(\alpha_1 + \alpha_2 + \alpha_3)X^2 + a(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)X - a(\alpha_1\alpha_2\alpha_3). \end{aligned}$$

Resta aplicar a Definição 10.4. CQD.

O caso de equações polinomiais de grau $n \geqslant 1$ é provado por indução.

Teorema 10.45 (*Fórmulas de Newton-Viète* (*caso grau* $n \geqslant 1$)) -

Indicando por α_1, α_2, $\alpha_3, \ldots, \alpha_n$ *as raízes (reais ou complexas) de uma equação polinomial de coeficientes reais ou complexos,* $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, *temos que valem as relações:*

$$\begin{aligned} -a_{n-1}/a_n &= \alpha_1 + \alpha_2 + \cdots + \alpha_n \\ a_{n-2}/a_n &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \cdots + \alpha_2\alpha_n + \cdots + \alpha_{n-1}\alpha_n \\ -a_{n-3}/a_n &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_1\alpha_2\alpha_n \\ &\quad + \alpha_2\alpha_3\alpha_4 + \cdots + \alpha_2\alpha_3\alpha_n + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n \\ &\cdots \\ (-1)^n a_0/a_n &= \alpha_1\alpha_2\alpha_3 \ldots \alpha_n\,. \end{aligned}$$

Muito cuidado!
Fique o leitor alertado que, em vez de nossa notação

$$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 = 0\,,$$

alguns autores usam

$$a_0 x^n + \cdots + a_{n-2}x^2 + a_{n-1}x + a_n = 0\,,$$

o que implica numa radical modificação notacional das relações mencionadas.

Exercício 341 -

i). *Sejam* $\sigma_1 = \alpha_1 + \alpha_2$ *e* $\sigma_2 = \alpha_1 \alpha_2$. *Prove que* α_1 *e* α_2 *são as raízes da equação:* $x^2 - \sigma_1 x + \sigma_2 = 0$.

ii). *Sejam* $\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3$, $\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$, *e* $\sigma_3 = \alpha_1\alpha_2\alpha_3$. *Prove que* α_1, α_2 *e* α_3 *são as raízes da equação:* $x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 = 0$.

Exercício 342 -

Resolver a equação $x^3 - 10x^2 + 31x - 30 = 0$, *sabendo que uma de suas raízes é a soma das outras.*

Exercício 343 -

Mostre que ao menos um dentre a soma e produto de dois números transcendentes tem de ser irracional.

Exercício 344 -

Sejam $\alpha_1, \alpha_2, \alpha_3$ *e* α_4 *as raízes, talvez repetidas, da equação* $x^4 + \alpha x^2 + \beta x + \gamma = 0$, *e sejam*

$$u = \frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3} + \frac{1}{\alpha_4}\,,$$

$$v = \frac{1}{\alpha_1^2} + \frac{1}{\alpha_2^2} + \frac{1}{\alpha_3^2} + \frac{1}{\alpha_4^2}\,.$$

Pede-se expressar u *e* v *em termos de* α, β, γ.

Exercício 345 -

Resolver o sistema de equações:

$$x + y + z = 1$$

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$$

$$x^2 + y^2 + z^2 = -1.$$

CAPÍTULO 11

EXISTEM NÚMEROS ALÉM DOS ESTUDADOS ATÉ AGORA?

Tendo-se em vista os resultados expressos pelo Primeiro Teorema Final da Aritmética (Teorema 10.1) e pelas várias versões do Teorema Fundamental da Álgebra, seria até razoável pensar que não há nada de útil, numericamente falando, além do campo dos números complexos. Afinal, com o mesmo, todas as deficiências geométricas, aritméticas e algébricas clássicas que surgiram com o desenvolvimento da Matemática foram sanadas.

Contudo, a partir de pontos de vista matemáticos bem mais sofisticados do que os que encontramos até aqui, foram concebidos vários outros campos numéricos que têm se mostrado úteis na resolução de problemas matemáticos e científicos. Isso é o caso dos números p-ádicos e dos reais não-standard, por exemplo. Infelizmente, o estudo desses campos requer um grau de maturidade matemática bem maior do que o exigido por este livro, e sua utilidade só é evidenciada em problemas bem distintos dos que aqui estudamos.

Por outro lado, é natural e fácil generalizarmos os números complexos com o mero ato de aceitar "várias unidades imaginárias". Desse modo, obtemos os chamados *números hipercomplexos*, o exemplo mais conhecido dos quais sendo o dos *quatérnios*. Apesar desses números não formarem um campo com estrutura de corpo, eles têm o grande mérito de nos permitir, fácil e rapidamente, entender melhor a importância dos números complexos, bem como destacar claramente as propriedades estruturais que viabilizam a existência dos teoremas fundamentais da Álgebra. Será exatamente dessas questões que trataremos neste capítulo.

11.1 Números hipercomplexos

Com o propósito de definir o que chamaremos de números hipercomplexos, generalizaremos a construção que fizemos para construir os números complexos a partir dos reais. Naquela ocasião, introduzimos um novo símbolo, denotado por i, para representar uma nova entidade numérica distinta de qualquer número real, e com ele consideramos o conjunto $\mathbb{C}$ dos "números" da forma $a + bi$ com $a, b \in \mathbb{R}$. A generalização desse procedimento produz a seguinte definição:

Definição 11.1 -

Números hipercomplexos são os objetos numéricos da forma

$$z = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + \cdots + a_n i_n\,,$$

onde $a_0, a_1, \ldots, a_n \in \mathbb{R}$ e $i_1, i_2, i_3, \ldots, i_n$ são elementos distintos entre si e fora do universo dos números reais; chamaremos estes i_k de "unidades imaginárias".

A igualdade entre dois números hipercomplexos é escrita como

$$a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + \cdots + a_n i_n = b_0 + b_1 i_1 + b_2 i_2 + b_3 i_3 + \cdots + b_n i_n\,,$$

e vale se, e só se, tivermos simultaneamente: $a_0 = b_0,\ a_1 = b_1, \ldots, a_n = b_n$.

Exemplo 11.2 -

Os números complexos constituem o caso particular dos números hipercomplexos que têm apenas uma unidade imaginária $(n = 1)$ *e ela verifica* ${i_1}^2 = -1$ *.*
(Notação abreviada tradicional: $i = i_1$*, de modo que* $i^2 = -1$ *.)*

Passemos a transformar o conjunto dos hipercomplexos num campo numérico. Para tal, introduziremos uma adição e uma multiplicação que estendem as dos números complexos:

Definição 11.3 (*Operações entre números hipercomplexos*) -

– *A adição de hipercomplexos é definida por:*

$$\begin{aligned} z + z' &= (a_0 + a_1 i_1 + \cdots + a_n i_n) + (b_0 + b_1 i_1 + \cdots + b_n i_n) \\ &= (a_0 + b_0) + (a_1 + b_1) i_1 + (a_2 + b_2) i_2 + \cdots + (a_n + b_n) i_n \,. \end{aligned}$$

– *A multiplicação de hipercomplexos é definida por:*

$$\begin{aligned} zz' &= (a_0 + a_1 i_1 + \cdots + a_n i_n).(b_0 + b_1 i_1 + \cdots + b_n i_n) \\ &= a_0 b_0 + a_0 b_1 i_1 + \cdots + a_0 b_n i_n \\ &\quad + a_1 b_0 i_1 + a_1 b_1 i_1 i_1 + a_1 b_2 i_1 i_2 \cdots + a_1 b_n i_1 i_n + \cdots \\ &\quad \cdots + a_n b_0 i_n + a_n b_1 i_n i_1 + a_n b_2 i_n i_2 + \cdots + a_n b_n i_n i_n \,, \end{aligned}$$

sendo que, de modo a podermos dizer que efetivamente zz' *é um hipercomplexo, fazemos mais duas suposições:*

- ⋆ *consideraremos válidas as propriedades associativa e comutativa da adição, bem como a distributividade da multiplicação;*
- ⋆ *a cada produto de unidades imaginárias* $i_p i_q$ *(para* $p, q \in \{1, 2, \ldots, n\}$*) é atribuído um valor hipercomplexo, ou seja, um valor da forma* $\alpha + \beta i_1 + \gamma i_2 + \cdots + \omega i_n$ *(onde os* $\alpha, \beta, \ldots, \omega \in \mathbb{R}$*) .*

Exercício 346 -

Mostre que a suposição de associatividade e comutatividade da adição, bem como a distributividade da multiplicação, nos permitem afirmar que sempre podemos levar o produto zz' *de hipercomplexos para a forma oficial:*

$$zz' = c_0 + c_1 i_1 + c_2 i_2 + \ldots + a_n i_n \,.$$

Note o leitor que, em todos os campos numéricos que já estudamos, a multiplicação tem várias propriedades básicas. Recordando:

- no campo dos números inteiros a multiplicação, além de ser distributiva, é associativa e comutativa; vimos que este campo tem uma estrutura de anel de integridade;

- nos campos dos números racionais, reais e complexos a multiplicação, além de ser distributiva, é associativa, comutativa e todo número não nulo tem recíproco; estes campos têm estrutura de corpo.

Por outro lado, num campo hipercomplexo genérico, a única propriedade da multiplicação que é obrigatória é sua distributividade. Assim, pela primeira vez, estamos encontrando campos numéricos onde *não estão* sendo exigidas as propriedades da associatividade e comutatividade da multiplicação, e nem a existência de recíprocos (para números não nulos). Façamos alguns comentários iniciais sobre essa novidade.

– A associatividade nos hipercomplexos

A associatividade é uma propriedade tão essencial que é de causar espanto que a mesma não tenha sido exigida na definição de multiplicação nos campos de hipercomplexos. O exemplo mais importante de campo onde a associatividade da multiplicação *não vale* é o dos chamados octônios[1], os quais são hipercomplexos formados de sete unidades imaginárias e mais a unidade real; omitiremos maiores detalhes, pois não faremos uso desse campo (ver: Okubo – *Introduction to Octonion and Other Non-Associative Algebras in Physics.* Cambridge UP, 1995). Contudo, é de se acrescentar que na vasta maioria dos exemplos essa propriedade é válida.

– A comutatividade da multiplicação de hipercomplexos

Como a definição de multiplicação de hipercomplexos não fixou os valores dos parâmetros em

$$i_p i_q = \alpha + \beta i_1 + \gamma i_2 + \cdots + \omega i_n \,,$$

estão abertas as portas para a possibilidade de propriedades operacionais que ainda não encontramos neste texto. Por exemplo, a princípio, pode muito bem ocorrer que algum $i_p i_q$ difira em valor de $i_q i_p$, possibilidade esta que caracterizará uma multiplicação não comutativa. Os quatérnios constituem o exemplo mais importante.

[1] Também chamados de números de Cayley, pois por ele introduzidos em 1845.

Exemplo 11.4 (*Os quatérnios*) -

São os mais importantes números hipercomplexos de três unidades imaginárias. Eles foram inventados por W. R. Hamilton em 1843, depois de anos de tentativas frustradas na busca de uma versão 3-dimensional dos números complexos (isto é, procurando um corpo comutativo com duas unidades imaginárias).

Os quatérnios têm a forma $a + bi + cj + dk$, *onde* $a, b, c, d \in \mathbb{R}$, *e as unidades imaginárias* i, j, k *verificam:*

$i^2 = -1$	$ij = \ \ k$	$ik = \ \ j$
$ji = -k$	$j^2 = -1$	$jk = \ \ i$
$ki = \ \ j$	$kj = -i$	$k^2 = -1$

Uma das principais características desse conjunto de números é a não comutatividade da multiplicação. Com efeito, a tabela nos diz que, por exemplo:

$$k = ij \neq ji = -k, \ \ i = jk \neq kj = -i, \ \ j = ki \neq ik = -j.$$

É de se acrescentar que os anos de frustração de Hamilton são justificados, na medida em que naquela época era inconcebível que um campo numérico não fosse comutativo.

Exercício 347 -

Mostre que toda a tabela de produtos das unidades imaginárias dos quatérnios pode ser deduzida dos seguintes casos básicos:

$$i^2 = j^2 = k^2 = ijk = -1\,.$$

Sugestão: para provar $ij = -ji = k$, *multiplique* $ijk = -1$ *à esquerda por* i, *e à direita por* k.

– Recíprocos e integridade nos hipercomplexos

Quando introduzimos os campos dos números inteiros, racionais, reais e complexos, nos capítulos anteriores, sempre se observou que o respectivo campo tinha a propriedade da *integridade.* Ou seja, nesses campos numéricos básicos, é impossível encontrarmos um produto nulo no qual nenhum dos fatores seja nulo; ou resumidamente: eles não têm *divisores de zero.* Contudo, veremos que a integridade pode não ocorrer em campos hipercomplexos. Dada a importância disso, vale a pena explicitarmos uma definição formal:

Definição 11.5 -

Um número hipercomplexo $z \neq 0$ é dito ser um divisor de zero *se valer $zz' = 0$ ou $z'z = 0$, para algum hipercomplexo $z' \neq 0$.*
Um campo de hipercomplexos onde não exista nenhum divisor de zero é dito ter integridade.

A existência de divisores de zero é fonte de muitas patologias operacionais. Por exemplo, ocorrendo $ab = 0$ e $a \neq 0$, não podemos garantir que $b = 0$.

Um exemplo importante de número que não é divisor de zero é todo número que tem recíproco.

Definição 11.6 -

Num campo de hipercomplexos, um número $z \neq 0$ é dito ter recíproco *(ser um* divisor da unidade *ou ter* inverso multiplicativo*) se existir algum hipercomplexo não nulo, z', tal que $zz' = z'z = 1$. Nesse caso, costuma-se escrever $z' = 1/z$.*

Exercício 348 -

Mostre que, em campos de hipercomplexos nos quais a multiplicação é associativa (é o que ocorre nos casos importantes, como o dos quatérnios), vale:

$$z \neq 0 \text{ tem recíproco} \Rightarrow z \text{ não é divisor de zero.}$$

Sugestão: raciocine por absurdo.

Exercício 349 -

Mostre que todos os quatérnios não nulos têm recíproco e que, portanto, não existem divisores de zero entre os quatérnios.
Dica: calcule o produto $(a + bi + cj + dk)(a - bi - cj - dk)$.

Exercício 350 -

Conforme vimos em capítulo anterior, o campo dos números reais tem estrutura de corpo ordenado. Contudo, à medida que formos considerando campos mais gerais, a estrutura vai "empobrecendo". Com efeito, verifique, ou recorde, que:

- *o campo dos complexos ainda é corpo, mas não ordenado;*
- *o campo dos quatérnios "é corpo", exceto pela não validade da comutatividade da multiplicação.*

11.2 Hipercomplexos com uma unidade imaginária

Como o campo dos quatérnios não tem divisores de zero, concluímos que a incomodativa existência de eventuais divisores de zero não é devida à multiplicidade de unidades imaginárias, mas à maneira como forem definidos os produtos de pares de unidades imaginárias. Com efeito, veremos nesta seção que divisores de zero podem ocorrer mesmo entre os campos com uma única unidade imaginária.

Para mostrar isso claramente, examinemos em termos bem gerais o caso dos hipercomplexos de uma única unidade imaginária, ou seja, dos hipercomplexos da forma $a + bI$ (para simplificar a notação, usaremos I no lugar de i_1).

Como I^2 também tem de ser um hipercomplexo de uma unidade imaginária, ele tem de ter a forma $I^2 = \alpha + \beta I$, com $\alpha, \beta \in \mathbb{R}$. Com isso, o produto de dois hipercomplexos de uma unidade imaginária tem de ter a forma:

$$\begin{aligned}(a + bI)(c + dI) &= (ac + bdI^2) + (ad + bc)I \\ &= (ac + bd\alpha) + (ad + bc + bd\beta)I.\end{aligned}$$

Examinemos três exemplos importantes de escolha para α e β. Eles são as chamadas *formas canônicas* dos números hipercomplexos com uma unidade imaginária:

· **números complexos :** temos $I^2 = -1 = -1 + 0I$, o que nos dá

$$(a + bI)(c + dI) = (ac - bd) + (ad + bc)I\,;$$

· **números duais :** temos $I^2 = 0 = 0 + 0I$, o que nos dá

$$(a + bI)(c + dI) = ac + (ad + bc)I\,;$$

· **números hiperbólicos:** temos $I^2 = 1 = 1 + 0I$, o que nos dá

$$(a + bI)(c + dI) = (ac + bd) + (ad + bc)I\,.$$

O quadro a seguir põe em destaque a diferença de comportamento desses três campos canônicos no que toca à existência de divisores de zero (recorde o Exercício 348):

campo numérico	é divisor de zero?	
	I	$1+I$
complexos ($I^2=-1$)	não	não
duais ($I^2=0$)	sim	não
hiperbólicos ($I^2=1$)	não	sim

Exercício 351 -

Prove as afirmações contidas no quadro anterior. Construa, além disso, um quadro correspondente que discuta a existência dos recíprocos de I e $1+I$.

Exercício 352 -

Sejam dois números hiperbólicos, $z \neq 0$ e $z' \neq 0$. Mostre que $zz'=0 \iff$

- *ou $z=\alpha+\alpha i$ e $z'=\alpha-\alpha i$, para um mesmo α real não-nulo,*
- *ou $z=\alpha-\alpha i$ e $z'=\alpha+\alpha i$, para um mesmo α real não-nulo.*

Exercício 353 -

Sejam dois números duais, z e z'. Imitando o que foi feito no exercício anterior, encontre uma caracterização do tipo $\iff$ para a ocorrência de $zz'=0$.

Já que encontramos a patologia dos divisores de zero, nossa próxima tarefa será descobrir uma caracterização estrutural que nos permita evitar campos hipercomplexos que tenham esse tipo de números. No caso mais simples, a saber, o caso dos hipercomplexos com uma unidade imaginária, essa caracterização é fácil de ser achada:

Teorema 11.7 (*formas canônicas*) -

Todo campo de números hipercomplexos de uma unidade imaginária I pode ser reduzido, mediante uma mudança de variável adequada, a uma das seguintes três formas canônicas:

i). a dos números complexos, ou seja, dos hipercomplexos com $I^2=-1$;
ii). a dos números duais, ou seja, dos hipercomplexos com $I^2=0$;
iii). a dos números hiperbólicos, ou seja, dos hipercomplexos com $I^2=1$.

Prova:

Indiquemos por $a+bI$ os números do campo dado, e escrevamos $I^2=\alpha+\beta I$. Nosso objetivo é mostrar que existe um $J=a+bI$, tal que o valor de J^2 é -1, 0 ou 1, conforme os valores de α e β. Para tal, precisaremos considerar as três seguintes possibilidades:

– caso (i): $\beta^2+4\alpha<0$

neste caso, iniciamos observando que está bem definido o número hipercomplexo

$$J=\frac{\beta}{\sqrt{-\beta^2-4\alpha}}+\frac{-2}{\sqrt{-\beta^2-4\alpha}}I,$$

e a seguir verificamos diretamente que $J^2=-1$;

– caso (ii): $\beta^2+4\alpha>0$

semelhantemente, iniciamos observando que está bem definido o número hipercomplexo

$$J=\frac{\beta}{\sqrt{\beta^2+4\alpha}}+\frac{-2}{\sqrt{\beta^2+4\alpha}}I\,,$$

e a seguir verificamos diretamente que $J^2=1$.

– caso (iii): $\beta^2+4\alpha=0$:

agora, introduzimos o hipercomplexo

$$J=\beta-2I\,,$$

e verificamos que $J^2=(\beta-2I)(\beta-2I)=\beta^2-4\beta I+4I^2=\beta^2-4\beta I+4(\alpha+\beta I)=\beta+4\alpha=0$. CQD.

Teorema 11.8 -

Nos campos de números hipercomplexos de uma unidade imaginária, sempre valem a associatividade e a comutatividade da multiplicação. Ademais, entre eles:

- *os campos que têm como forma canônica os números duais ou os números hiperbólicos sempre têm divisores de zero;*
- *os campos que têm como forma canônica os números complexos ($I^2=-1$) nunca têm divisores de zero.*

Prova:

É imediata consequência do teorema anterior. CQD.

Exercício 354 -

É sabido que a identidade numérica $(a+b)(a-b) = a^2 - b^2$ *vale no campo dos números complexos, ou seja: ela vale para todos os* $a, b \in \mathbb{C}$*. Pede-se estudar sua validade no campo dos números duais e no dos hiperbólicos.*

11.3 Revisitando o Teorema Final da Aritmética

Voltamos nesta seção a considerar os hipercomplexos com várias unidades imaginárias. Vamos usá-los para enunciar e discutir uma nova versão do Teorema Final da Aritmética.

Começamos observando que o Teorema 11.8 nos mostra que é muito fácil fugirmos dos campos de hipercomplexos de apenas uma unidade imaginária, mas com divisores de zero: basta trabalharmos apenas com os campos onde $i_1^2 = -1$. Infelizmente, no caso dos campos com mais de uma unidade imaginária, a solução não é tão simples, pois podemos ter coisas como $i_1^2 = \alpha i_2 + \beta i_3$, e também precisamos nos preocupar com os produtos mistos $i_p i_q$. Contudo, mostra-se que é suficiente nos restringirmos aos chamados hipercomplexos normalizados, a saber:

Definição 11.9 -

Um campo de números hipercomplexos,

$$z = a + bi_1 + ci_2 + di_3 + \cdots + wi_n \,,$$

de n *unidades imaginárias, é dito ser* normalizado *quando valer* $i_k^2 = -1$*, para* $k = 1, 2, \ldots, n$*.*

Exemplo 11.10 -

É imediato se constatar que o campo dos números complexos e o dos quatérnios são campos normalizados.

Exercício 355 -

Verifique que entre os campos hipercomplexos canônicos de uma única unidade imaginária, o único normalizado é o que não tem divisores de zero.

O teorema a seguir é devido a Weierstrass:

Teorema 11.11 (*Segundo Teorema Final da Aritmética*) -

Existe apenas um campo normalizado de números hipercomplexos cuja multiplicação é associativa, comutativa e não tem divisores de zero. Este campo é o dos números complexos.

Prova:

Já sabemos que o resultado vale para o caso dos campos com apenas uma unidade imaginária. Assim, resta examinarmos os casos onde temos duas, ou mais, unidades imaginárias.

a). Caso de campo com 2 unidades imaginárias

Os números de um tal campo podem ser escritos na forma $a+bj+ck$, onde $a, b, c \in \mathbb{R}$, e as duas unidades imaginárias verificam $j^2 = k^2 = -1$.

Escrevamos o produto jk na forma oficial: $jk = a + bj + ck$. Multiplicando essa igualdade por j, e usando as propriedades usuais da adição –bem como a associatividade, distributividade e comutatividade da multiplicação, que estamos supondo válidas–, obtemos:

$$\begin{aligned} -k = jjk &= aj - b + cjk \\ &= aj - b + c(a + bj + ck) \\ &= (-b + ac) + (a + bc)j + c^2 k \,, \end{aligned}$$

ou seja,

$$-k = (-b + ac) + (a + bc)j + c^2 k \,,$$

o que implica termos as igualdades:

$$\begin{cases} -b + ac = 0 \\ a + bc = 0 \\ c^2 = -1. \end{cases}$$

Ora, esse sistema não tem solução, pois é impossível um número real c verificar $c^2 = -1$.

b). Caso de campo com 3 unidades imaginárias

Agora, os números do campo têm a forma: $a + bj + ck + dl$, com a, b, c, d reais. Consequentemente, os produtos jk, kl, lj podem ser escritos como:

$$\begin{aligned} jk &= a_1 + b_1 j + c_1 k + d_1 l \\ kl &= a_2 + b_2 j + c_2 k + d_2 l \\ lj &= a_3 + b_3 j + c_3 k + d_3 l\,. \end{aligned} \tag{11.1}$$

Como já fizemos no caso de 2 unidades, mostraremos que essas igualdades são incoerentes com as propriedades supostas para a adição e multiplicação dos números de um tal campo. Como novidade, os detalhes serão mais extensos e, agora, também precisaremos usar que não é permitido que um produto de fatores não nulos seja nulo. O início da prova é semelhante ao caso anterior: multiplicaremos cada uma das três igualdades em (11.1) por j, k, l , respectivamente. Vejamos.

Multiplicando a primeira igualdade por j:

$$\begin{aligned} -k &= jjk \\ &= j(a_1 + b_1 j + c_1 k + d_1 l) \\ &= a_1 j - b_1 + c_1 jk + d_1 jl \\ &= a_1 j - b_1 + c_1(a_1 + b_1 j + c_1 k + d_1 l) \\ &+ d_1(a_3 + b_3 j + c_3 k + d_3 l) \\ &= (-b_1 + a_1 c_1 + a_3 d_1) + j(a_1 + b_1 c_1 + b_3 d_1) \\ &+ k(c_1^2 + c_3 d_1) + l(c_1 d_1 + d_1 d_3), \end{aligned}$$

o que nos leva às equações:

$$\begin{cases} 0 = -b_1 + a_1 c_1 + a_3 d_1 \\ 0 = a_1 + b_1 c_1 + b_3 d_1 \\ -1 = c_1^2 + c_3 d_1 \\ 0 = c_1 d_1 + d_1 d_3\,. \end{cases}$$

Multiplicando a segunda igualdade de (11.1) por k:

$$\begin{aligned} -l = kkl = k(a_2 + b_2 j + c_2 k + d_2 l) &= a_2 k + b_2 jk - c_2 + d_2 kl \\ &= a_2 k + b_2(a_1 + b_1 j + c_1 k + d_1 l) - c_2 + d_2(a_2 + b_2 j + c_2 k + d_2 l) \\ &= (a_1 b_2 - c_2 + a_2 d_2) + j(b_1 b_2 + b_2 d_2) \\ &+ k(a_2 + b_2 c_1 + c_2 d_2) + l(b_2 d_1 + d_2^2), \end{aligned}$$

o que nos leva às equações:

$$\begin{cases} 0 = a_1b_2 - c_2 + a_2d_2 \\ 0 = b_1b_2 + b_2d_2 \\ 0 = a_2 + b_2c_1 + c_2d_2 \\ -1 = b_2d_1 + d_2^2 \,. \end{cases}$$

Multiplicando a terceira igualdade de (11.1) por l:

$$\begin{aligned} -j = llj &= l(a_3 + b_3j + c_3k + d_3l) = a_3l + b_3lj + c_3kl - d_3 \\ &= a_3l + b_3(a_3 + b_3j + c_3k + d_3l) + c_3(a_2 + b_2j + c_2k + d_2l) - d_3 \\ &= (a_3b_3 + a_2c_3 - d_3) + j(b_3^2 + b_2c_3) \\ &+ k(b_3c_3 + c_2c_3) + l(a_3 + b_3d_3 + c_3d_2), \end{aligned}$$

o que nos leva às equações:

$$\begin{cases} 0 = a_3b_3 + a_2c_3 - d_3 \\ -1 = b_3^2 + b_2c_3 \\ 0 = b_3c_3 + c_2c_3 \\ 0 = a_3 + b_3d_3 + c_3d_2 \,. \end{cases}$$

Desses três conjuntos de quatro equações, nos bastará tomar as equações que tenham duas parcelas no membro direito. Elas estão agrupadas a seguir:

$$\begin{cases} -1 = c_1^2 + c_3d_1 & \quad 0 = c_1d_1 + d_1d_3 \\ -1 = d_2^2 + b_2d_1 & \quad 0 = b_1b_2 + b_2d_2 \\ -1 = b_3^2 + b_2c_3 & \quad 0 = b_3c_3 + c_2c_3 \,. \end{cases} \tag{11.2}$$

Para atingirmos o nosso objetivo, passaremos a simplificar as equações desse sistema. Inicialmente, iremos simplificar as equações da segunda coluna de (11.2) (as equações que têm zero como membro esquerdo). Para isso, basta observar que como o quadrado de um número real nunca pode ser negativo, as equações da primeira coluna do sistema (11.2) nos dizem que, respectivamente:

$$c_3d_1 \neq 0,\ b_2d_1 \neq 0,\ b_2c_3 \neq 0\,,$$

de modo que $b_2 \neq 0, c_3 \neq 0, d_1 \neq 0$, e isso nos permite dizer que as equações do sistema (11.2) podem ser simplificadas para:

$$\begin{cases} 0 = c_1 + d_3 \\ 0 = b_1 + d_2 \\ 0 = b_3 + c_2\,, \end{cases} \tag{11.3}$$

ou seja:

$$c_1 = -d_3,\ b_1 = -d_2,\ b_3 = -c_2.$$

Passemos à simplificação das equações da primeira coluna do sistema (11.2) (as que têm membro esquerdo igual a -1). Para conseguirmos isso, a ideia será montar igualdades deduzidas das várias maneiras de calcularmos o produto jkl.

Nesse sentido, dada a comutatividade e associatividade do produto, temos três possibilidades de reescrita:

$$\begin{cases} (jk)l = j(kl) \\ (jk)l = k(lj) \\ (kl)j = k(lj)\,. \end{cases}$$

– No caso $(jk)l = j(kl)$, temos:

$$\begin{aligned}(jk)l &= (a_1 + b_1 j + c_1 k + d_1 l)l = a_1 l + b_1 jl + c_1 kl - d_1 \\ &= -d_1 + a_1 l + b_1(a_3 + b_3 j + c_3 k + d_3 l) + c_1(a_2 + b_2 j + c_2 k + d_2 l) \\ &= (-d_1 + a_3 b_1 + c_1 a_2) + j(b_1 b_3 + c_1 b_2) \\ &+ k(b_1 c_3 + c_1 c_2) + l(a_1 + b_1 d_3 + c_1 d_2),\end{aligned}$$

e

$$\begin{aligned}j(kl) &= j(a_2 + b_2 j + c_2 k + d_2 l) = a_2 j - b_2 + c_2 jk + d_2 lj \\ &= a_2 j - b_2 + c_2(a_1 + b_1 j + c_1 k + d_1 l) + d_2(a_3 + b_3 j + c_3 k + d_3 l) \\ &= (-b_2 + c_2 a_1 + d_2 a_3) + j(a_2 + c_2 b_1 + d_2 b_3) \\ &+ k(c_2 c_1 + d_2 c_3) + l(c_2 d_1 + d_2 d_3).\end{aligned}$$

Comparando os coeficientes de ambos os membros da igualdade $(jk)l = j(kl)$, vemos que o mais promissor de analisar é o coeficiente de k, o qual nos permite escrever

$$b_1 c_3 + c_1 c_2 = c_2 c_1 + d_2 c_3,$$

de onde tiramos $c_3(b_1 - d_2) = 0$.

Ora, já sabemos que $c_3 \neq 0$, de modo que $b_1 - d_2 = 0$, ou $b_1 = d_2$. Mas, as equações de (11.3) nos dizem que $b_1 = -d_2$. Consequentemente, pela simultaneidade de $b_1 = d_2$ e $b_1 = -d_2$, somos forçados a concluir que $b_1 = d_2 = 0$.

– No caso $(jk)l = k(lj)$, faremos análogo:

$$\begin{aligned} k(lj) &= k(a_3 + b_3 j + c_3 k + d_3 l) = a_3 k + b_3 jk - c_3 + d_3 kl \\ &= -c_3 + a_3 k + b_3(a_1 + b_1 j + c_1 k + d_1 l) + d_3(a_2 + b_2 j + c_2 k + d_2 l) \\ &= (-c_3 + b_3 a_1 + d_3 a_2) + j(b_3 b_1 + d_3 b_2) + k(a_3 + b_3 c_1 + d_3 c_2) \\ &+ l(b_3 d_1 + d_3 d_2). \end{aligned}$$

Comparando os membros de $(jk)l = k(lj)$, vemos que o único coeficiente que é dado por apenas duas parcelas, em ambos os membros, é o coeficiente de j. Trabalhando com ele, temos,

$$b_1 b_3 + c_1 b_2 = b_3 b_1 + d_3 b_2,$$

ou $b_2(c_1 - d_3) = 0$. Ora, já sabemos que $b_2 \neq 0$, de modo que $c_1 - d_3 = 0$, ou $c_1 = d_3$. Por outro lado, a primeira equação de α_2 nos diz que $c_1 = -d_3$. Consequentemente: $c_1 = d_3 = 0$.

– Resta examinar o caso $(kl)j = k(lj)$.

Ambos esses produtos já foram calculados anteriormente, tendo sido obtido:

$$\begin{aligned} (kl)j = j(kl) &= (-b_2 + c_2 a_1 + d_2 a_3) + j(a_2 + c_2 b_1 + d_2 b_3) \\ &+ k(c_2 c_1 + d_2 c_3) + l(c_2 d_1 + d_2 d_3), \end{aligned}$$

e

$$\begin{aligned} k(lj) &= (-c_3 + b_3 a_1 + d_3 a_2) + j(b_3 b_1 + d_3 b_2) \\ &+ k(a_3 + b_3 c_1 + d_3 c_2) + l(b_3 d_1 + d_3 d_2). \end{aligned}$$

Comparando os membros de $(kl)j = k(lj)$, novamente vemos que há só um coeficiente que é dado por apenas duas parcelas, em ambos os membros, que é o coeficiente de l. Trabalhando com ele, temos

$$c_2 d_1 + d_2 d_3 = b_3 d_1 + d_3 d_2\,,$$

de onde $d_1(c_2 - b_3) = 0$. Como já sabemos que $d_1 \neq 0$, concluímos que $c_2 - b_3 = 0$, ou $b_3 = c_2$. Por outro lado, a terceira equação de (11.3) nos diz que $b_3 = -c_2$. Consequentemente, somos obrigados a concluir que $b_3 = c_2 = 0$.

Resumindo, temos que

$$b_1 = d_2 = c_1 = d_3 = b_3 = c_2 = 0.$$

Essas nulidades nos permitem, finalmente, simplificar as equações da primeira coluna do sistema (11.2), obtendo:

$$\begin{cases} -1 = c_3 d_1 \\ -1 = b_2 d_1 \\ -1 = b_2 c_3 \,. \end{cases}$$

Se multiplicarmos entre si essas três igualdades, obteremos, finalmente:

$$-1 = (b_2 c_3 d_1)^2,$$

o que é uma impossibilidade para números reais.

c). Caso de campo com $\geqslant 4$ unidades imaginárias

Dado o aumento do grau de complexidade da prova ocorrido ao passarmos de 2 para 3 unidades imaginárias, é de se esperar que, para campos com $\geqslant 4$ unidades imaginárias, a demonstração fique muito mais complicada. Assim, nos contentaremos em remeter o leitor interessado nessas provas para o trabalho de E. Study e Élie Cartan, mencionado na bibliografia. CQD.

Exercício 356 -

Examine novamente a demonstração do Segundo Teorema Final da Aritmética, agora, procurando ver onde se usou que o produto de reais não nulos nunca pode ser zero.

Observação 11.12 -

A importância do Segundo Teorema Final da Aritmética está no fato de que ele nos diz que, se insistirmos na obediência ao Princípio da Permanência de Hankel, a extensão do campo dos números reais para um campo envolvendo um número finito de unidades imaginárias inicia e termina com o dos números complexos.

Embutida nessa "terminalidade" do campo dos números complexos está a proibição de existirem divisores de zero. Essa proibição é tão forte que mesmo que abríssemos mão de outras propriedades algébricas básicas, tais como a associatividade e comutatividade da multiplicação, conseguiríamos muito poucos campos hipercomplexos além de $\mathbb{C}$. Com efeito, em 1957, os matemáticos John Milnor, Raull Bott e Michel Kervaire mostraram que:

mesmo que não exijamos a associatividade e a comutatividade da multiplicação, os únicos possíveis campos de números hipercomplexos normalizados ocorrerão para $n = 1$ (números complexos), $n = 3$ (quatérnios) e $n = 7$ (octônios).

11.4 Polinômios e equações nos hipercomplexos

O objetivo desta seção é mostrar que a comutatividade e a integridade da multiplicação (ou seja: a inexistência de divisores de zero) em um campo de números hipercomplexos são decisivas na validade de propriedades básicas dos polinômios e equações associadas. Mostraremos isso usando exemplos envolvendo equações comuns de encontrarmos em problemas práticos. Na seção seguinte, reexaminaremos a situação sob o ponto de vista do Teorema Fundamental da Álgebra.

Visando nosso objetivo, a primeira coisa a ser observada é que poderíamos dizer que não há mais nada realmente interessante a dizer sobre polinômios. Com efeito, os mesmos foram definidos sobre um corpo numérico, e o Segundo Teorema Final da Aritmética diz que não existem campos hipercomplexos (normalizados) que tenham estrutura de corpo, além de $\mathbb{C}$.

Contudo, de maneira igual à feita em cursos de Álgebra Abstrata, podemos estender a noção de polinômio para os casos em que seus coeficientes estão num campo onde valham as propriedades características dos corpos, com *exceção* da comutatividade e da integridade da multiplicação, bem como não se garanta a existência do recíproco dos números não nulos.[2] A adição e multiplicação desses tipos mais gerais de polinômios são definidas do mesmo modo como fizemos para o caso clássico de polinômios sobre um corpo numérico (vide Definição 10.15, no capítulo anterior). É sob essa convenção que iremos trabalhar, no que segue.

– A importância da comutatividade da multiplicação

O mais conhecido e importante campo de hipercomplexos no qual a multiplicação *não é* comutativa é o campo dos quatérnios (vide Exemplo 11.4). Assim, consideremos nesse campo a equação quadrática $x^2 + 1 = 0$.

[2]Na terminologia da Álgebra, um campo com essas propriedades é chamado de anel. No Capítulo 2, quando caracterizamos a estrutura algébrica dos inteiros, mostramos que eles formam um anel *de integridade*, ou seja: um anel no qual a multiplicação é comutativa e tem integridade.

Primeira surpresa:
a equação $x^2 + 1 = 0$ tem *infinitas raízes* no campo dos quatérnios.

Com efeito, por exemplo, todos os números da forma $x = aj + bk$, onde $a^2 + b^2 = 1$, são raízes, pois nos quatérnios vale $(aj+bk)^2 = -a^2-b^2$, como o leitor pode verificar imediatamente. Em particular, $x = j$, $x = -j$, $x = k$ e $x = -k$ são quatro dessas infinitas raízes.

Vejamos outro fato surpreendente. Como $x = j$ é raiz, deveríamos esperar ser verdadeira uma fatoração da forma (sendo α um número dos quatérnios):

$$X^2 + 1 = (X - j)q(X) = (X - j)(X + \alpha)\,.$$

Mostremos que ela efetivamente existe. Para isso, recordemos que pela definição de produto de polinômios, mesmo que o campo dos coeficientes a e b não seja comutativo, temos:

$$(X + a)(X + b) = X^2 + (a + b)X + ab, .$$

Consequentemente, $(X - j)(X + \alpha) = X^2 + (-j + \alpha)X + (-j)\alpha$. Disso segue:

$$X^2+1 = (X-j)q(X) = (X-j)(X+\alpha) \iff X^2+0X+1 = X^2+(-j+\alpha)X+(-j)\alpha\,.$$

Ou seja: $0 = -j + \alpha$ e $1 = (-j)\alpha$. Ora, é imediato verificar que $\alpha = j$ é a solução dessas equações. Resumindo, temos a igualdade polinomial:

$$X^2 + 1 = (X - j)q(X) = (X - j)(X + j)\,.$$

Apesar disso, compare com:

Segunda surpresa:
a igualdade polinomial sobre os quatérnios $X^2 + 1 = (X - j)(X + j)$
não se traduz numa *identidade numérica*, ou seja:

$$\text{é falso que } x^2 + 1 = (x - j)(x + j),\ \forall x \in \text{quatérnios}\,.$$

Com efeito, vendo x como um número quatérnio, e não como uma indeterminada, como a multiplicação de quatérnios não é comutativa:

$$(x - j)(x + j) = x^2 + xj + (-j)x - j^2 = x^2 + [xj + (-j)x] + 1\,,$$

de modo que a identidade numérica mencionada é equivalente a dizer que $xj = jx$, para todo x dos quatérnios. Evidentemente, isso é falso: basta tomar $x = k$.

Exercício 357 -

Encontrar infinitos exemplos de números quatérnios para os quais é falsa a igualdade numérica: $x^2 + 1 = (x - j)(x + j)$.

Vale a pena resumir:

- como produto de *polinômios* sobre o campo dos quatérnios, temos:

$$(X - j)(X + j) = X^2 + (-j + j)X - j^2 = X^2 + 0X + 1 = X^2 + 1\,;$$

- como produto de *expressões analíticas* temos, para x número quatérnio:

$$(x - j)(x + j) = x^2 + xj + (-j)x - j^2 = x^2 + [xj + (-j)x] + 1 \overset{\text{em geral}}{\neq} x^2 + 1\,.$$

Exercício 358 -

i). Mostre que mesmo em campos hipercomplexos cuja multiplicação não seja comutativa, vale a identidade polinomial:

$$X^n - \alpha^n = (X - \alpha)(X^{n-1} + \alpha X^{n-2} + \alpha^2 X^{n-3} + \cdots + \alpha^{n-2} X + \alpha^{n-1}).$$

ii). Mostre que em tais campos não comutativos, a identidade polinomial acima não se traduz em uma identidade numérica.

Exercício 359 -

Seja $p(X)$ um polinômio (não nulo) sobre um campo de hipercomplexos, e suponhamos que a equação $p(x) = 0$ tenha uma raiz α neste campo. Mostre que pode ocorrer que não exista um polinômio $q(X)$ sobre este campo e para a qual valha a identidade numérica:

$$p(x) = (x - \alpha)q(x), \quad \forall x \in \textit{ao campo}.$$

Exercício 360 -

Em campos hipercomplexos, a multiplicação de polinômios segue regras distintas das da multiplicação de expressões polinomiais? Responda, justificando.

– Importância da inexistência de divisores de zero

Já muito enfatizamos que em todo corpo numérico a multiplicação tem integridade. Ou seja: um corpo nunca tem divisores de zero, o que significa que, sendo α e β números deste corpo:

$$\alpha\beta = 0 \Rightarrow \text{ ao menos um dos fatores será nulo.}$$

Contudo, muitos campos de hipercomplexos têm divisores de zero. Isso já ocorre com campos de uma única unidade imaginária, como é o caso dos números duais. Entre os campos com duas unidades imaginárias, um dos mais interessantes é o campo dos números biduais, que passamos a definir.

Definição 11.13 -

Os números biduais são os números hipercomplexos da forma $z = a + bj + ck$ (onde $a, b, c \in \mathbb{R}$), tais que as unidades imaginárias verificam as relações

$$j^2 = k^2 = jk = kj = 0. \tag{11.4}$$

As relações 11.4 mostram que a multiplicação de biduais não tem integridade. Elas também estão declarando que o produto das unidades é comutativo, com o que é imediato vermos que o produto de biduais quaisquer é comutativo.

Tendo exemplos de campos hipercomplexos nos quais a multiplicação não tem integridade, passemos a examinar as consequências disto.

Iniciamos verificando se os defeitos (as surpresas 1 e 2) que identificamos no caso dos campos onde a multiplicação não é comutativa ainda continuam existindo.

> Primeira surpresa (versão campo sem integridade):
> a equação $x^2 - 2x + 1 = 0$ tem *infinitas raízes* no campo dos biduais.

Com efeito, como esse campo é comutativo na multiplicação, a equação pode ser escrita na forma: $(x-1)^2 = 0$. Isto mostra que $x = 1$ é uma raiz. Mas existem infinitas outras, todas as da forma $x = 1 + bj + ck$, com quaisquer $b, c \in \mathbb{R}$, pois:

$$x^2 - 2x + 1 = (x-1)^2 = (bj + ck)^2 = b^2j^2 + bcjk + cbkj + c^2k^2 \overset{(11.4)}{=} 0\,.$$

Segunda surpresa (versão campo sem integridade):
no campo dos biduais – bem como em qualquer campo hipercomplexo sem integridade, mas com multiplicação comutativa – continua valendo que toda igualdade polinomial se traduz numa identidade numérica em todo o campo.

Passemos, finalmente, a investigar o principal incômodo provocado por uma multiplicação *sem* integridade: a falta de unicidade em fatorações. Vejamos o que isso significa e porque ocorre. Tomemos dois divisores de zero, a e b; ou seja: nenhum deles é o elemento zero do campo, mas $ab = 0$. Assim sendo, teremos que cada elemento a' do campo nos permite construir um outro elemento a'', de modo a termos $a'b = a''b$. Com efeito, definindo $a'' = a + a'$:

$$a''b = (a + a')b = ab + a'b = 0 + a'b = a'b\,.$$

Isso nos leva a crer que, num campo sem integridade, fatorações $p(X) = (X - \alpha)q(X)$ possam não ser únicas. Com efeito, isto realmente pode ocorrer:

Terceira surpresa:
em campos hipercomplexos sem integridade (como no campo dos números biduais), fixado α, podem existir infinitos fatores $q(X)$ para

$$p(X) = (X - \alpha)q(X).$$

Quarta surpresa:
em campos hipercomplexos sem integridade, como no campo dos números biduais, não são quaisquer duas raízes, α e β da equação $x^2 - 2x + 1 = 0$ que nos permitem obter a fatoração:

$$X^2 - 2X + 1 = (X - \alpha)(X - \beta)\,.$$

Com efeito, existem muitas maneiras de $(X - \alpha)(X - \beta)$ não ser igual ao polinômio associado à equação, mesmo no caso de α e β serem duas raízes:

$$\begin{aligned}(X - 1 - bj)(X - 1 - ck) &= X^2 - (2 + bj + ck)X + (1 + bj + ck)\\ &= X^2 - 2X + 1 \iff bj + ck = 0 \iff b = c = 0\,,\end{aligned}$$

como também existem infinitas maneiras desta igualdade polinomial se verificar, por exemplo, para todos os reais b:

$$\begin{aligned}(X-1-bj)(X-1+bj) &= X^2-2X-(1+bj)(-1+bj)\\ &= X^2-2X-(-1+b^2j^2) = X^2-2X+1\,.\end{aligned}$$

– Resumindo:

- num campo hipercomplexo onde a multiplicação não é comutativa ou não tem integridade, podemos encontrar equações polinomiais com infinitas raízes;
- em todo campo hipercomplexo vale o Teorema da Fatoração:

  $$p(X) = (X-\alpha)q(X)\,,$$

  porém, se a multiplicação não for comutativa, esta igualdade polinomial não precisa se transformar numa identidade numérica $p(x) = (x-\alpha)q(x)$, válida para todos os números x do campo;
- num campo hipercomplexo sem integridade, o conhecimento de n raízes $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ de uma equação polinomial

  $$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

  não implica que seja válida a fatoração:

  $$a_n X^n + \cdots + a_2 X^2 + a_1 X + a_0 = a_n(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)\,.$$

Exercício 361 -

Determine a quantidade de raízes da equação $x^2+1=0$:

i). em cada um dos corpos numéricos clássicos: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$;

ii). no campo hipercomplexo não comutativo dos quatérnios;

iii). no campo hipercomplexo sem integridade dos números biduais.

Exercício 362 -

Estude a equação $x^2+1=0$ nos campos hipercomplexos de uma unidade imaginária. Em particular, mostre que nos três campos canônicos – complexos, duais e hiperbólicos – ela tem raízes apenas no campo dos números complexos.

11.5 Revisitando o Teorema Fundamental da Álgebra

Iniciemos recordando que vimos três versões do Teorema Fundamental da Álgebra (TFA), para uma equação polinomial, $p(x) = 0$, sobre o corpo dos números complexos:

- o *TFA-existencial* (que garante a existência de raiz para toda equação polinomial neste corpo);
- o *TFA-enumerativo* (que dá o número exato de raízes de uma tal equação);
- o *TFA-fatoração* (que mostra que o polinômio associado $p(X)$ pode ser obtido pelo produto dos fatores $X - \alpha$, com α raiz da tal equação).

Observemos, ademais, que essas três versões do TFA foram estabelecidas na seguinte ordem lógica:

$$\text{TFA-existencial} \Rightarrow \text{TFA-enumerativo} \Rightarrow \text{TFA-fatoração}.$$

Também precisamos observar que a prova do TFA-existencial não é estritamente algébrica, pois usa crucialmente a *continuidade topológica* de $\mathbb{C}$. Por sua vez, os outros TFA dependem do resultado do primeiro, mas usam um *argumento algébrico*, baseado em identidades polinomiais e identidades numéricas associadas.

Questão 1:
podemos generalizar o TFA–existencial para campos hipercomplexos?

Resposta simples: não para todos esses campos! Pois, por exemplo, $x^2 + 1 = 0$ é uma equação sem nenhuma raiz no campo dos números hiperbólicos e nem no dos números duais.
Resposta mais sofisticada: nada vimos, por enquanto, que possa impedir de valer esse TFA em *algum* campo hipercomplexo. Com efeito, Ivan Niven mostrou que esse teorema vale no campo dos quatérnios (vide seu artigo: "Equations in quaternions", *Amer. Math. Monthly*, vol. 48 (1941), pp. 654-661).

Questão 2:
podemos generalizar o TFA–enumerativo para campos hipercomplexos?

Como este teorema é obtido a partir do TFA–existencial, mais identidades polinomiais e respectivas identidades numéricas, precisamos examinar a validade destas em campos hipercomplexos. Ora, como o Segundo Teorema Final da Aritmética diz que existe apenas um campo de números hipercomplexos normalizado, comutativo e sem divisores de zero – o dos números complexos –, segue que precisamos examinar a validade de tais identidades em campos onde não houver comutatividade ou não houver integridade da multiplicação.

Ora, na seção anterior, vimos que basta *não valer* uma propriedade dentre a integridade e comutatividade da multiplicação para que tenhamos equações polinomiais com infinitas raízes. Isso tira a possibilidade de expressarmos a quantidade de raízes de uma equação polinomial, num tal campo, em termos do grau da equação.

Questão 3:
podemos generalizar o TFA–fatoração para campos hipercomplexos?

Este teorema depende crucialmente das igualdades polinomiais da forma $p(X) = (X-\alpha)q(X)$, as quais vimos que não se traduzem em termos de identidades numéricas $p(x) = (x-\alpha)q(x)$, se a multiplicação do campo não for comutativa ou não tiver integridade.

Com efeito, mais uma vez, tomemos a equação $x^2-2x+1=0$, no campo hipercomplexo dos números biduais, a qual admite $x = 1 + bj + ck$ como raízes, $\forall\, b, c \in \mathbb{R}$. No caso, podemos fatorar o polinômio associado de infinitas maneiras:

$$(X-1-bj)(X-1+bj) = X^2-2X-(-1+b^2j^2) = X^2-2X+1\,,\ \forall b \in \mathbb{R}\ .$$

Mas, também ocorre que o conhecimento de suas duas raízes não produza uma fatoração:

$$\begin{aligned}(X-1-bj)(X-1-ck) &= X^2-(2+bj+ck)X+(1+bj+ck)\\ &= X^2-2X+1 \iff bj+ck=0 \iff b=c=0\,.\end{aligned}$$

RESPOSTAS E SUGESTÕES AOS EXERCÍCIOS

Capítulo 1.

Exercício 1.
Um possível padrão é "Para qualquer natural ímpar n, tem-se $n^2 - n = (n-1)^2 + (n-1)$". Esta afirmação é verdadeira, e uma demonstração para ela pode ser obtida apenas desenvolvendo-se a expresão $(n-1)^2 + (n-1)$.
A mesma demonstração serve para o padrão "Para qualquer natural n, tem-se $n^2 - n = (n-1)^2 + (n-1)$".

Exercício 2.
Um possível padrão é "Para qualquer natural n, tem-se $(10n + 25)^2 = 1000n + 25$. Esta afirmação, é no entanto, falsa. Uma maneira de comprovar isto é apresentando um contraexemplo: para $n = 1$, temos $35^2 = 1225 \neq 1025$.

Exercício 3.
Lembre que um número par é da forma $2 \times \textit{inteiro}$, e um número ímpar é da forma $\textit{par} + 1$.

Exercício 4.
Divida em dois casos: n par e n ímpar.

Exercício 7.
Escreva x na forma $x = a/b$, com $a, b \in \mathbb{Z}$ e $b > 0$; para uma prova por contraposição, sugere-se utilizar a seguinte propriedade válida para inteiros c e d quaisquer: se $c \geqslant d \geqslant 0$, então $c^2 \geqslant d^2$.

Exercício 8.
i) V *ii)* F.

Exercício 9.
i) F *ii)* V.

Exercícios 10 e 11.
Imite o procedimento do Exemplo 1.55.

Exercício 12.
Expresse todos os termos da PG em função do primeiro termo e da razão.

Exercícios 13, 14, 15.
Verifique cuidadosamente se todos os passos de uma prova por indução estão bem enunciados.

Exercício 16.
Você deve usar que $169 = 13^2$.

Capítulo 2.

Exercício 17.
Por exemplo, para $A = \mathbb{Z}$:
$\forall x \in A, x > 0$ é F; $\exists x \in A, x > 0$ é V; $\exists! x \in A, x > 0$ é F; $\nexists x \in A, x > 0$ é F.

Exercício 18.
Use a definição de subtração e as propriedades já provadas da adição.

Exercício 21.
i) Use duas vezes a compatibilidade da ordem com a adição. *ii)* Use duas vezes a compatibilidade da ordem com a multiplicação.

Exercício 22.
Basta encontrar um contraexemplo.

Exercício 23.
ii) Use a definição de divisor em cada uma das hipóteses.

Exercício 24.
Use a definição de divisor.

Exercício 25.
F. Encontre um contraexemplo.

Exercício 26.
Conte o número de divisores de 0 e de ± 1 e tente contar o número de divisores de qualquer outro inteiro.

Exercício 28.
Levando em conta que os livros-texto do Ensino Fundamental apresentam a definição de número primo quando o universo numérico do aluno é apenas $\mathbb{N}$, reflita e responda: existe alguma deficiência numa definição diferente da que foi aqui apresentada?

Exercício 29.
i) Escreva a forma de dois ímpares consecutivos e prove a afirmação por absurdo. *ii)* Basta que não sejam múltiplos de 3 (prove isto!). *iii)* Não. Encontre um contraexemplo.

Exercício 30.
Prove por indução que, para todo n natural não nulo, $10^n - 4$ é múltiplo de 6.

Exercício 31.
O mdc é igual a 1. Sim (Sugere-se que, mais do que um exemplo, Você encontre uma condição genérica que nos garanta isto).

Exercício 32.
i) Use a definição de mdc, suas propriedades e a transitividade da divisibilidade. *ii)* Leve em conta a transitividade da divisibilidade.

Exercício 34.
$1 = 89 \times 389 + (-191) \times 167\,.$

Exercício 35.
Faça uso da combinação linear que expressa o mdc entre os números dados.

Exercício 36.
Prove que $\operatorname{mdc}(ac, bc) = |c| \operatorname{mdc}(a, b)$. Aqui pode ser útil o Exercício 35.

Exercício 38.
Use indução sobre o número de fatores.

Exercícios 39 *e* 40.
Basta apresentar um contraexemplo.

Exercício 41.
Compare essa afirmação com o Teorema 2.55.

Exercício 42.
Use a definição de mdc e as propriedades da divisibilidade. Dica: prove por contraposição, e considere um divisor primo do mdc $(a+b, ab)$.
Para o outro caso (mdc $(a-b, ab) = 1$), raciocine de forma análoga.

Exercício 45.
Use o Teorema Fundamental da Artimética.

Exercício 46.
i) 1 , *ii)* qualquer conjunto de números primos positivos.

Exercício 47.
A (a fatoração de a) $\times$ (a fatoração de b) é sem dúvida *uma* fatoração para ab. Como ela é só formada por fatores primos, pela unicidade de fatoração em primos, basta agrupá-los e reordená-los para obtermos **a** fatoração de ab.

Exercício 48.
A fatoração apresentada é uma possível fatoração para o número 78 em fatores primos; portanto, está correta (veja quadro após o Teorema 2.59).

Exercícios 50, 51, 52, 53.
Leve em conta o Corolário 2.61.

Exercício 54.
i) Divida em casos os múltiplos de 4: ± 4, ± 8 e os diferentes destes; *ii)* parta do estudo da soma $4k = 2k + 2k$; *iii)* Leve em conta a discussão feita no Exemplo 1.27.

Capítulo 3.

Exercício 55.
Lembre que fração irredutivel é uma fração a/b com mdc $(a, b) = 1$.

Exercício 56.
i) Deveria existir um inteiro a, tal que $24a = 560 \times 13$.

Exercício 58.
Nos itens *(i)* e *(ii)*, a maioria dos alunos responde simplesmente $2n/3n$ e $14n/49n$, com $n \in \mathbb{N}^*$ ou $n \in \mathbb{Z}^*$, o que está correto. No entanto, no ítem *(ii)* também está correto $2n/7n$, com $n \in \mathbb{N}^*$. Daí, quem em *(ii)* respondeu $2n/7n$, com $n \in \mathbb{N}^*$, a resposta para *(iv)* é *sim*; para quem respondeu $14n/49n$, com $n \in \mathbb{N}^*$, a resposta para *(iv)* é *não*, pois em sua lista não aparece a fração ordinária $2/7$.
Para *(v)*, deve ser demonstrado que na/nb, com $n \in \mathbb{N}^*$, expressa *todas* as representações do racional a/b se, e só se, mdc $(a, b) = 1$.

Exercício 59.
A resolução está correta. O aluno simplesmente não fez uso do menor denominador possível.

Exercícios 60, 61, 62, 63 *e* 64.
Faça uso do Corolário 2.61.

Exercício 65.
O inteiro bd deve ser um divisor de ac.

Exercício 66.
Faça uso do Corolário 2.61.

Exercício 67.
Verdadeiro. Faça uso do Corolário 2.61.

Exercício 68.
Faça uso do Corolário 2.61.

Exercício 69.
O inteiro bc deve ser um divisor de ad.

Exercício 70.
O numerador de tal fração deve ser um divisor do inteiro dado.

Exercício 72.
Para provar, por exemplo, que o simétrico é único, suponha que r' e r'' são simétricos do racional r, e deduza que $r' = r''$.

Exercício 74.
(ii) Quando um denominador comum é muito fácil de ser encontrado, o critério mencionado não precisa ser aplicado.

Exercício 75 e 76.
Escreva os racionais na forma de fração, aplique o critério estabelecido na última Definição e faça uso da Proposição 2.5.

Exercício 77.
Utilize duas vezes a proposição.

Exercício 78.
Utilize o Exercício 77 com escolhas convenientes para r, s, r', s'.

Exercício 79.
Para *(i)*: $n = 6$; para *(ii)*, representando os racionais envolvidos por frações de mesmo denominador, vê-se que n deve ser o inteiro tal que $(n-1)b < 2a < nb$, ou seja: o (único) inteiro que satisfaz $\frac{2a}{b} < n \leqslant \frac{2a}{b} + 1$.

Exercício 80.
Para *(i)* $m = 19$; *(ii)* $m = 191$; *(iii)* $m = 1914$; *(iv)* $m = 19142$; *(v)* m deve ser tal que $\frac{134}{7} \times 10^n - 1 \leqslant m \leqslant \frac{134}{7} \times 10^n$. Um tal inteiro sempre existe porque os racionais $\frac{134}{7} \times 10^n - 1$ e $\frac{134}{7} \times 10^n$ diferem em uma unidade. Em cada item o valor de m é único.

Exercício 81.
Para *(i)* $m = 1$; *(ii)* $m = 18$; *(iii)* $m = 187$; *(iv)* $m = 1874$ ou 1875; *(v)* a partir de $n = 3$, $m = 1875 \times 10^{n-3}$ ou $m = 1875 \times 10^{n-3} - 1$, não sendo, portanto, o valor de m único.

Exercício 83.
Repita aqui a justificativa dada após o Teorema 3.37.

Exercício 84.
Para *(i)*: não, pois entre $2/4$ e $3/4$ não existe nenhum elemento desse conjunto. *(ii)* Sim, e para provar isso basta utilizar o Exercício 83. *(iii)* Sim.

Exercício 85.
Utilize o Exercício 83.

Exercício 87.
Para *(ii)*, por exemplo, comece em 2 e siga somando $1/2^n$ a 1, em cada etapa. Ou seja, considere a sequência $x_0 = 2$, $x_n = 1 + \frac{1}{2^n}$ (para $n \geqslant 1$).

Exercício 88.
Adapte a ideia apresentada em *(ii)* do *Exercício* 87 para o caso de sequência crescente.

Exercício 89.
Encontre um contraexemplo para tal propriedade.

Capítulo 4.

Exercício 90.
V.

Exercício 91.
Raciocine por absurdo.

Exercício 92.
2/6 e 12/7 não são representáveis por fração decimal.

Exercício 93.
Suponha $a/b = m/10^n$, com $m \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então, reescreva a igualdade na forma $a \times 10^n = b \times m$ e use o Teorema Fundamental da Aritmética.

Exercício 94.
(i) Existem infinitas frações decimais que representam 3/50. A fração ordinária $3 \times 2^6 \times 5^5/50 \times 2^6 \times 5^5 = 3 \times 2^6 \times 5^5/10^7$ é uma delas. *(ii)* Idem *(i):* $3 \times 2^2 \times 5^5/10^5$ é uma delas.

Exercício 95.
(i) Represente os dois racionais por frações de mesmo denominador. A seguir, considere para denominador uma potência de dez que seja maior do que este denominador comum, ficando assim encontrado um valor para n. Agora, basta encontrar m.

Exercício 96.
Utilize indução sobre n.

Exercício 97.
Faça uso do Exercício 96, e prove por indução sobre m.

Exercício 98.
(i) Faça uso das igualdades expressas no Teorema 2.45.

Exercício 99.
(i) Faça uso do Exercício 98.

Exercício 102.
Sim, pois determinar a parte inteira de um racional nada mais é do que fazer a divisão euclidiana do numerador pelo denominador.

Exercício 103.
Basta aplicar a Definição 4.25.

Exercício 104.
Recomenda-se aqui que Você tente imitar a prova do Teorema 4.28, até o ponto em que não possa mais seguir as mesmas ideias. Aí Você encontrará a resposta para essa questão.

Exercício 106.
Se o resto da divisão de 10^7 por 17 fosse 1, já teríamos na primeira linha a determinação do período. Como este resto é igual a 5, foi necessário escrever a segunda

linha. Se o resto da divisão de 5×10^7 por 17 fosse 1 ou 5, já teríamos com a primeira e a segunda linhas a determinação do período. Note que, com a terceira linha, realmente repetiu-se um resto, de modo que com essas três linhas, de fato, conseguimos extrair o período da expansão decimal de $1/17$.

Exercício 108.
(i) Aplique a Proposição 4.30 para chegar na resposta $41\,152/333\,333$. *(ii)* Aplique a Proposição 4.7 para chegar na resposta $1\,707\,817/333\,333$.

Exercício 109.
(i) Substitua 999 por $1000 - 1$. *(ii)* Aplique o Exercício 96.

Exercício 112.
(i) $1\,010\,287/8\,333\,325$; *(ii)* $42\,676\,912/8\,333\,325$.

Exercício 113.
(i) $5/900,\ 48/99\,000,\ 12/99\,900$.

Exercício 115.
Sim, vale sempre: aplique o Teorema 4.33 nos dois casos e mostre que as geratrizes obtidas são iguais. (Note que no enunciado do Teorema 4.33 não foi afirmado que $\overline{c_1 \ldots c_p}$ denota o período; portanto, podemos de fato aplicá-lo nos dois casos.)

Exercício 116.
A regra de recuperação da geratriz é, afinal, uma só.
a dada pelo Teorema 4.33.

Exercício 117.
Muitos livros não chamam a atenção para o fato de que período só formado por 9's nunca ocorre. Daí gera-se um erro quando se questiona "Que fração dá origem à representação decimal $0,999\ldots$?", por exemplo.

Exercício 118.
(ii) Aplique aqui também o Teorema Fundamental de Aritmética.

Exercício 119.
Mostre que a "dízima candidata" a resto é, de fato, a expansão decimal do resto entre 1 e a fração geratriz de r.

Capítulo 6.

Exercício 123.
Utilize a Proposição 6.1.

Exercício 124.
Utilize as Proposições 6.1 e 6.2.

Exercício 125.
(iii) Utilize indução. Aqui, Você vai precisar refletir sobre como se faz indução apenas para n par.

Exercício 126.
Não! Construa um contraexemplo.

Exercício 127.
São eles os pontos da forma $P\,(m/1000)$, com $m \in \mathbb{N}$.

Exercício 128.
(i) Sim: $P(s) = P\left(\frac{10s}{10}\right)$; *(ii)* Sim: $P(\frac{s}{10}) = P\left(\frac{10s}{100}\right)$;

(iii) Sim: $P(\frac{s}{10^n}) = P\left(\frac{10s}{10^{n+1}}\right)$; *(iv)* Existem nove, uma vez que $P(\frac{m}{10^n}) = P\left(\frac{10m}{10^{n+1}}\right)$

e $P(\frac{m+1}{10^n}) = P\left(\frac{10(m+1)}{10^{n+1}}\right) = P\left(\frac{10m+10}{10^{n+1}}\right)$;

Exercício 129.
Verdadeiro: $P\left(\frac{m}{10^n}\right) = P\left(\frac{10^s m}{10^{n+s}}\right)$.

Exercício 130.
$P\left(\frac{10m+9}{10^{n+1}}\right) P\left(\frac{m+1}{10^n}\right)$.

Exercício 131.
$P\left(\frac{m}{10^n}\right) P\left(\frac{10m+1}{10^{n+1}}\right)$.

Exercício 132.
Prove que cada nova rede de graduação inclui vários novos pontos entre os pontos dados. Deduza daí que existem, na verdade, infinitos pontos graduados entre dois quaisquer pontos graduados distintos.

Exercício 133.
$|OP(\frac{m}{10^n})| = \frac{m}{10^n}$. Argumente pensando em como chegamos ao ponto $P(\frac{m}{10^n})$.

Exercício 134.
Verdadeiro. $P(m)$ e $P(m+1)$ são pontos consecutivos da rede de graduação unitária; portanto, são extremos de um segmento de medida $|OU| = 1$.

Exercício 135.
Falso. $P(\frac{m}{10})$ e $P(\frac{m+1}{10})$ são pontos consecutivos da rede de graduação decimal; portanto, são extremos de um segmento de medida $|\frac{1}{10}OU| = \frac{1}{10}$.

Exercício 136.
Considere $P(\frac{m}{10^n})$ e $P(\frac{r}{10^s})$ como pontos de uma mesma rede de graduação, e encontre-a!

Exercício 137.
(i) Por exemplo, construa inicialmente o segmento $2OU$ e depois, usando a técnica do Capítulo 5, divida $2OU$ em três partes iguais e considere o segmento de extremo O; *(ii)* Comece calculando $|OP|$.

Exercício 138.
(i) $|OP| = \frac{11}{35} = |11(\frac{1}{35}OU)|$, de modo que basta dividir OU em 35 partes iguais e emendar 11 delas; *(ii)* Se P fosse um ponto graduado a medida de OP seria expressa por uma fração decimal. Prove que, no entanto, o racional $11/35$ não pode ser expresso por uma fração decimal.

Exercício 139.
(i) O método da medição aproximada com a régua escolar de 30 cm é capaz de medir qualquer segmento de reta de comprimento menor ou igual a 30 cm, desde que seja a cota de erro exigida não seja mmenor do que 1 mm.

Exercício 140.
Faça uso do método da medição aproximada, recorrendo à rede de graduação $1/10^4$.

Exercício 141.
Faça uso do método da medição aproximada, recorrendo à rede de graduação $1/10^2$.

Exercício 142.
Faça uso do método da medição aproximada, recorrendo à rede de graduação $1/10^3$.

Exercício 143.
(i) O argumento resume-se a provar que se OP é congruente a essa diagonal, então P não é um ponto graduado; *(ii)* e *(iii)*: raciocine geometricamente.

Exercício 145.
$5,43000\ldots$ e $5,42999\ldots$.

Exercício 146.
(i) $3,95000\ldots$ e $3,94999\ldots$;*(ii)* $3,59000\ldots$ e $3,58999\ldots$.

Exercício 147.
$3,599000\ldots$ e $3,599999\ldots$.

Exercício 148.
(i) Com erro menor do que 1: qualquer racional entre 13 e 14; com erro menor do

que $1/10$: qualquer racional entre 13 e $13,1 = 131/10$. *(ii)* e *(iii)*: como $1/25 = 4/100 > 1/100$, basta encontrar um racional que aproxime a medida com erro menor do que $1/100$, para termos um exemplo de racional que aproxime a medida com erro menor do que $1/25$.

Exercício 149.
Raciocine por absurdo ou utilize o Teorema 6.28.

Exercício 150.
Sendo a lista periódica, temos que a medida de OP é o número racional $32\,213/9\,990$, ou seja, $|OP| = 32\,213/9\,990$, ou ainda, $9\,990\,|OP| = 32\,213\,OU$.

Exercício 151.
$|OQ| = 161/80$.

Exercício 155.
Imite o exemplo anterior.

Exercício 156.
Dica: releia o Exemplo 6.35.

Capítulo 7.

Exercício 158.
i) e *ii)* Construa um exemplo.

Exercício 159.
Não! É possível construir números irracionais que não acmulem 3 dígitos repetidos.

Exercício 160.
i) e *ii)* Simplesmente porque não satisfazem o primeiro requisito da definição. Por exemplo, $0,999\ldots = 1,000\ldots$.

Exercício 161.
i) Os números dados diferem no décimo dígito. Como $0 < 1$, temos que o primeiro número é o maior; *ii)* o segundo.

Exercício 162.
O menor ab possível é $ab = 49$.

Exercício 163.
$9/4 \leqslant 22/9 \leqslant 2,\overline{54} \leqslant 2,55$.

Exercício 164.
Como $-10 = -10,000\ldots$, temos que -10 é o maior.

Exercício 166.
Considere os casos x e y positivos, x e y negativos e x e y de sinais contrários.

Exercício 167.
Você pode utilizar o Exercício 157.

Exercício 168.
Basta usar a Definição 7.34.

Exercícios 169 e 170:
Use o Teorema Fundamental da Geometria Analítica.

Exercício 171.
Note que na definição de intervalo fechado cabem intervalos do tipo $[a,a]$, os quais denotam o conjunto unitário $\{a\}$.

Exercício 172.
Lembre que um $\mathbb{Q}$-intervalo é formado exclusivamente por números racionais.

Exercício 174.
i) Verdadeiro; *ii)* Falso.

Exercício 175.
Note que um erro menor do que $1/10^5$ para a soma pode ser obtido quando conseguirmos um erro menor do que $2/10^6$. Isto nos sugere utilizar aproximações para x e y com erro menor do que $1/10^6$. Assim, a resposta é qualquer número do intervalo $[16,62775\ ;\ 16,62777]$.

Exercício 176.
Mostre que o processo anteriormente citado vai, de fato, produzir uma lista periódica; portanto, a soma é um número racional. Recupere o racional a partir dessa lista e mostre que ele é igual a $\left(\frac{3215-32}{9900}\right) + \left(2 + \frac{134120-134}{999000}\right)$.

Exercício 177.
Temos $l+m, a_1a_2a_3 \leqslant l+x \leqslant l+m, a_1a_2a_3 + \frac{2}{10^3}$, ou ainda, $l+m+\frac{a_1a_2a_3}{10^3} \leqslant l+x \leqslant l+m+\frac{a_1a_2a_3}{10^3}+\frac{2}{10^3}$, de modo que, pondo $t = m+l$, podemos já afirmar que $x+y = t, a_1a_2\ldots$. (Se quisermos determinar o próximo dígito, então devemos fazer uso de melhores aproximações para x.)

Exercício 179.
(i) Faça uso da Definição 7.37; *(ii)* Qualquer número do intervalo $[-16,6279, -16,6277]$.

Exercício 182.
No item *(i)* é possível fazer um raciocínio genérico (como fizemos no Exemplo 7.46) e concluir que os resultados são efetivamente iguais.

Exercício 183.
A prova para o caso geral é por indução sobre n. Para resolver a multiplicação por 10, use o Teorema 7.54.

Exercício 186.
Encontre um contraexemplo.

Exercício 187.
Geralmente, quando queremos mostrar unicidade, supomos x e y com a tal propriedade (que, no caso é "ser raiz quadrada aritmética de $2a^2$") e deduzimos, a partir dela, que $x = y$. Para a segunda parte, faça uso da unicidade.

Exercício 190.
Para *i)* utilize duas vezes a propriedade *(i)* enunciada no Corolário 7.70, escolhendo, cada vez, um c conveniente.

Exercício 191.
Para *i)* utilize duas vezes a propriedade *(ii)* enunciada no Corolário 7.70, escolhendo, cada vez, um c conveniente.

Exercício 192.
Uma maneira é simplificar para o caso em que os reais são 0 e $m, a_1a_2a_3 \ldots$, e resolver o exercício apenas para este caso. Pense nisso!

Exercício 193.
i) É aqui que é preciso utilizar a propriedade arquimediana. *ii)* Pensar geometricamente aqui ajuda! Esse $1/n$ está relacionado com o item anterior.

Exercício 194.
Basta observar que o termo geral da sequência é $2+1/10^n$, e que $1/10^n$ tende a zero quando $n \to \infty$.

Exercício 196.
A n-ésima soma parcial é $s_n = n$, e ela tende a infinito quando $n \to \infty$.

Exercício 197.
Notar que $t_n = bs_n$, onde $s_n = a_1 + a_2 + \cdots + a_n$ e $t_n = b(a_1 + \cdots + a_n)$, e usar o Exercício 195 .

Exercício 198.
Sendo $t_n = s_n - \alpha$:

$$s_n \to \alpha \overset{\text{def}}{\iff} (\forall\varepsilon > 0)\,(\exists n_0)\,(n > n_0 \Longrightarrow |s_n - \alpha| < \varepsilon)$$
$$\iff (\forall\varepsilon)\,(\exists n_0)\,(n > n_0 \Longrightarrow |t_n| < \varepsilon) \iff t_n \to 0\,.$$

Exercício 199.
Se $r = 1$, então a soma da PG é uma soma de unidades; logo, obviamente, diverge.

Exercício 200.
Usando a soma dos n-termos de uma PG tem-se:

$$\frac{1}{10} + \cdots + \frac{1}{10^n} - \frac{1}{9} = \frac{\frac{1}{10}(\frac{1}{10^n} - 1)}{\frac{1}{10} - 1} - \frac{1}{9} = -\frac{1}{9 \cdot 10^n}\,.$$

Exercício 202.
Suponha $x = M, a_1 \ldots$. Se $x > 0$, então

$$[-x]_n = -M, a_1 \ldots a_n - \frac{1}{10^n} = -\,[x]_n - \frac{1}{10^n}\,;$$

se $x < 0$, então

$$[-x]_n = -M, a_1 \ldots a_n = -\left(M, a_1 \ldots a_n - \frac{1}{10^n}\right) - \frac{1}{10^n} = -\,[x]_n - \frac{1}{10^n}\,.$$

Exercício 205.
Dica: sendo I_m e J_k sequências de intervalos encaixantes e evanescentes em torno de α, dado k existem n_1 e n_2 tais que $I_n \subset J_k$ (para todo $n > n_1$) e $J_n \subset I_k$ (para todo $n > n_2$).

Exercício 207.
Suponha que $x(n)$ converge a α de acordo com a definição dada na Seção 7.11. Seja I_m uma sequência de intervalos encaixantes e evanescentes contendo α. Dado $\varepsilon > 0$, existe m tal que $I_m \subset (\alpha - \varepsilon, \alpha + \varepsilon)$ bem como existe n_0 tal que $x(n) \in I_m$ (para todo $n > n_0$). Logo, $x(n) \in (\alpha - \varepsilon, \alpha + \varepsilon)$ (para todo $n > n_0$). Reciprocamente, supondo que $x(n)$ converge a α de acordo com definição dada na Seção 7.10, basta tomar $I_n = (\alpha - 1/n, \alpha + 1/n)$.

Exercício 208.
Da definição de convergência de séries, definindo $s_n = M + a_1/10 + \cdots + a_n/10^n$, teremos $x = \lim s_n$.

Exercício 209.
Basta notar que se $x < 0$, então $-x > 0$. Logo, y é tal que $x(-y) = (-x)y = 1$.

Exercício 210.

i). $x+y=x+z \Rightarrow (-x)+(x+y)=(-x)+(x+z) \Rightarrow (-x+x)+y=(-x+x)+z$
$\Rightarrow 0+y=0+z \Rightarrow y=z.$

ii). Sendo w o inverso multiplicativo de x, temos:

$$xy=xz \Rightarrow w(xy)=w(xz) \Rightarrow (wx)y=(wx)z \Rightarrow y=z\,.$$

Capítulo 8.

Exercício 211.
Não, da mesma forma que "probabilidade zero" não é sinônimo de "impossível".

Exercício 212.
(i) Utilize indução sobre n. *(ii)* Tente intuir exemplos. *(iii)* $n+1$ é um quadrado perfeito; *(iv) a)* Infinitas; *b)* Nenhuma; *c)* Infinitas.

Exercício 213.

x	y	$x+y$	$x\times y$
$\in\mathbb{Q}$	$\in\mathbb{Q}$	$\in\mathbb{Q}$	$\in\mathbb{Q}$
$\in\mathbb{Q}$	$\notin\mathbb{Q}$	$\notin\mathbb{Q}$	$\notin\mathbb{Q}$, se $x\in\mathbb{Q}^*$
$\notin\mathbb{Q}$	$\in\mathbb{Q}$	$\notin\mathbb{Q}$	$\notin\mathbb{Q}$, se $x\in\mathbb{Q}^*$
$\notin\mathbb{Q}$	$\notin\mathbb{Q}$	varia	varia

A subtração e a divisão podem ser encaradas como especiais adição e multiplicação, respectivamente; portanto, suas propriedades são as mesmas da adição e multiplicação, respectivamente.

Exercício 214.
$x=2\sqrt{2}$ e $y=3\sqrt{2}$.

Exercício 215.
$x=2\sqrt{2}$ e $y=\sqrt{3}$.

Exercício 216.
(i) Por exemplo: $a=2\sqrt{2},\ b=-2\sqrt{2}$; *(ii)* Some nos dois lados o simétrico de a.

Exercício 217.
Utilize a definição de comensurabilidade.

Exercício 218.
Basta trabalhar aproximações de $\sqrt{2}$ e de $\sqrt{3}$, com erro menor do que $1/10^3$.

Exercício 219.
(i) e (ii) É irracional. Prove por absurdo (desnecessário usar expansão decimal).

Exercício 222.
a) Por exemplo, o inverso de $a+b\sqrt{2}$ é $\frac{a-b\sqrt{2}}{a^2+b^2}$;
b) Cada elemento $a+b\sqrt{2}$ é a soma de a com o produto de $\sqrt{2}$ por b; para mostrar a recíproca, mostre que adição/subtração/multiplicação/divisão de um elemento da forma (um racional) + (um produto de um racional por potência de $\sqrt{2}$) por outro elemento desta forma (não nulo, se a operação for de divisão) dá como resultado sempre um número da forma $a+b\sqrt{2}$, com $a,b\in\mathbb{Q}$;
c) Veja item *(a)*; *d)* Prove por absurdo.

Exercício 223.
Não: racionalizando por etapas vamos chegar a $\frac{1}{2}+\frac{\sqrt{2}}{2}-\frac{\sqrt{6}}{4}$, que não pertence a $[\mathbb{Q},\sqrt{2},\sqrt{3}]$; portanto, este conjunto não é um corpo.

Exercício 224.
(i) Inicialmente observe que, qualquer que seja o real x, temos $x^4+x^2+1>0$ e também $x^{100!^{100!^{100!}}}>0$. Daí, conclua que toda raiz da equação dada é positiva.
(ii) É aqui que usamos a observação feita: comece fazendo $x=1$ e $x=2$.
(iii) Faça $x=1,1$.

Exercício 225.
Utilize para u potências de dez.

Exercício 226.
(i) Utilize indução sobre n.

Exercício 227.
(a) Falso. *(b)* Falso. *(c)* Falso. *(d)* Verdadeira. *(e)* Falso.

Exercício 228.
A única resposta correta é a segunda.

Exercício 229.
Uma possível resposta é

$$a_n=\begin{cases} 1, \text{ se } n=\frac{k^2+k}{2}, \text{ para algum } k\in\mathbb{N}^*\,; \\ 0, \text{ caso contrário.}\end{cases}$$

Exercício 230.
Não, pois a frequência do dígito 5 seria zero.

Exercício 231.
Por exemplo, $0,010010001000001\ldots$, mas também $1,12341123411123411111234\ldots$.

Exercício 232.
Verdadeiro, e um tal número nunca será normal. Exemplo: $6,22234334333433334\ldots$.

Exercício 233.
Verdadeiro, porque o bloco 88, por exemplo, nunca vai aparecer em sua expansão decimal.

Exercício 234:
i) $0,\overline{1234567890}$;
ii) $0,\overline{12}$;
iii) Não, por exemplo: $0,1234567890112233445566778899001112223333\ldots$.

Exercício 235.
(i) Falso. Já se sabe que π não é um racional; *(ii)* Verdadeiro.

Exercício 236.
(a) Imite o raciocínio utilizado no Exercício 255; *(b)* Falso.

Exercício 237.
Basta substituir x por α na equação dada.

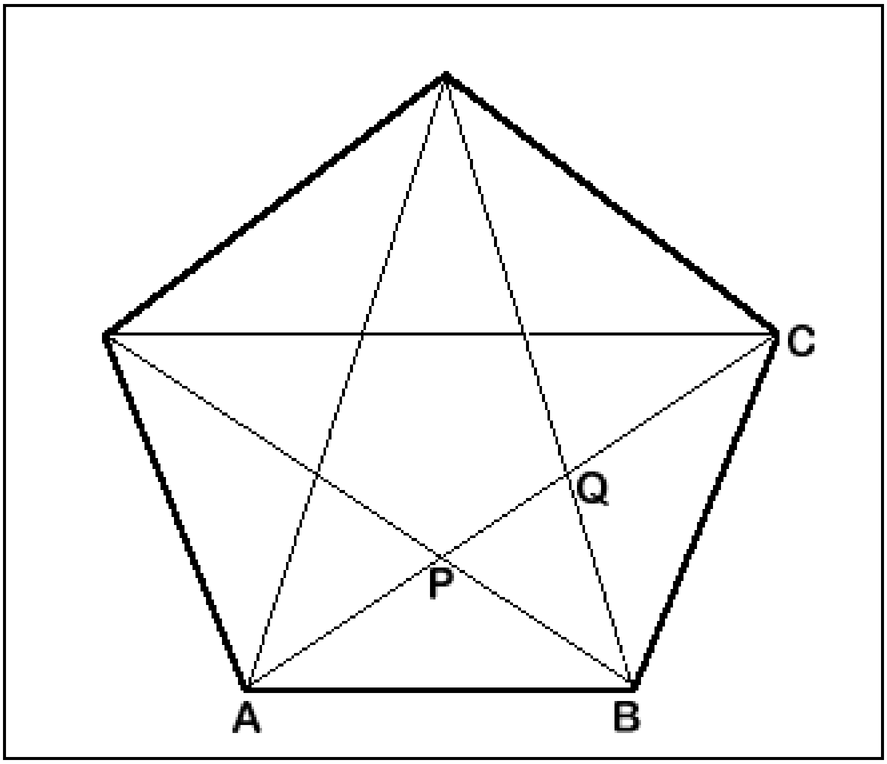
Exercício 238.
Basta isolar x na equação dada e provar que tais valores de x são, de fato, irracionais.

Exercício 239.
Para mostrar a unicidade basta resolver a equação.

Exercício 240.
Fazendo $y = l - x$, da proporção recaia numa equação do segundo grau em x.

Exercício 241.
Utilize indução.

Exercício 242.
Prove que (veja figura a seguir) os triângulos APB e ABC são semelhantes. Utilize o exercício 240 e o fato que o triângulo ABQ é isósceles.



Exercício 243.
Inicialmente, observe que, para termos raízes racionais, é preciso que $b^2 - 4c$ seja um quadrado perfeito. Daí considere os casos em que b é par e em que b é ímpar.

Exercício 244.
a) Não: basta tomar $\sqrt{2}$ e $-\sqrt{2}$; *b)* Sim: se $ar^2+br+c=0$, então $c\,(\frac{1}{r})^2+b\,\frac{1}{r}+a=0$.

Exercício 246.
(i) Faça $x=1$ e $x=2$; *(ii)* Denote por a a raiz real determinada em *(i),* e calcule $q(X)$. A seguir, mostre que $q(X)$ não tem raízes reais.

Exercício 247.
(a) Prove por absurdo, escrevendo a raiz como uma fração já na forma irredutível; *(b)* equação de grau um com coeficientes inteiros sempre tem uma só raiz, e ela é racional.

Exercício 249.
Pove por absurdo que $\sqrt[3]{2}$ não é uma irracionalidade quadrática.

Exercício 250.
Verdadeiro. Note que $ax^2 + bx + c = x^2(a + b\,\frac{1}{x} + c\,\frac{1}{x^2})$.

Exercício 251.
Verdadeiro. Generalize a ideia do Exercício 250.

Exercício 252.
Faça $x = \sqrt{2} + \sqrt{3}$ e trabalhe com a igualdade $x - \sqrt{2} = \sqrt{3}$.

Exercício 253.
Faça $x = a + b\sqrt{2}$ e trabalhe com a igualdade $\sqrt{2} = \frac{x-a}{b}$.

Exercício 255.
Elimine o denominador comum dos coeficientes do polinômio com coeficientes racionais.

Exercício 256.
Coloque em evidência r^n na expressão de grau n em r que é nula.

Exercício 257.
Faça uso de parcelas da forma $\pm(-1)^j$.

Exercício 258.
Substitua r por α^p na expressão em r que é nula, onde $\alpha = \sqrt[p]{r}$.

Exercício 259.
i) V; *ii)* F. Ache um contraexemplo!

Exercício 260.
(i) Prove por absurdo; *(ii)* Utilize *(i)*.

Exercício 261.
(i) $\sqrt{\sqrt{2}}$ é um real algébrico; *(ii)* Prove por absurdo.

Capítulo 9.

Exercício 263.
Ampliação da propriedade $\sqrt{ab} = \sqrt{a}\,\sqrt{b}$, para reais positivos a e b; ampliação da propriedade $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, para reais a e b, e a hipótese $(\sqrt{-1})^2 = -1$; ampliação da propriedade $\sqrt[3]{a^3} = a$, para todo real a.

Exercício 264.
(a) i) Sim; *ii)* Sim; *iii)* Não; *(b) i)* Chamando de x_0 a raiz real obtida em *(a)*, temos que as demais raízes são também reais, pois $-3a^2 + 12 > 0$, e são dadas por

$\frac{-a\pm\sqrt{-3a^2+12}}{2}$; *(b) ii)* Não existem outras raízes reais.

Exercício 265.
Escrevendo $X^3 - 15X - 4 = (X-4)\cdot q(X)$, obtemos $q(X) = X^2 + 4X + 1$. Então, basta usar Bhaskara, para encontrar as raízes de $q(x) = 0$, que serão também raízes de $x^3 - 15x - 4 = 0$ (por quê?).

Exercício 266.
É importante que o leitor tenha se dado conta que quando definimos a adição de complexos (que aqui vamos representar diferenciadamente por $+_{\mathbb{C}}$), fizemos uso da adição de reais (que aqui vamos representar por $+_{\mathbb{R}}$). Confira:

$$(a+bi) +_{\mathbb{C}} (c+di) = (a +_{\mathbb{R}} c) + (b +_{\mathbb{R}} d)i.$$

Agora, se r e s são números reais, $(r+0i) +_{\mathbb{C}} (s+0i) = r +_{\mathbb{R}} s$.

Exercício 267.
Faça $ii = (0+1i)(0+1i)$.

Exercício 268.
Basta identificar o número real 0 com o complexo $0+0i$, como no exercício 266, e realizar a multiplicação de complexos.

Exercício 269.
Suponha $(a+bi)(c+di) = 0$ e que $a+bi \neq 0$ (ou seja, $a^2+b^2 \neq 0$). Então, mostre que necessariamente tem-se $c = d = 0$.

Exercício 270.
A resolução deste exercício é a mesma em qualquer corpo.

Exercício 271.
Escreva, $i^{4n+k} = \left(i^4\right)^n \cdot i^k$, para cada $k \in \{0,1,2,3\}$.

Exercício 272.
Comece isolando $(1+i)^n$ e considere os diferentes restos da divisão de n por 4. Note que $(1+i)^2 = 2i$. A resposta é: nenhum valor de n satisfaz a igualdade.

Exercício 273.
Utilize o Exercício 271.

Exercício 274.
Utilize a Proposição 9.12.

Exercício 275.
i) Imite o argumento de Bombelli quando teve a “ideia louca” de operar com as

expressões da forma $a + b\sqrt{-1}$ como se fossem números reais; *ii)* Raciocine por absurdo; *iii)* $(c + d\delta)^{-1} = \frac{1}{c} - \frac{d}{c^2}\delta$.

Exercício 276.
Sim.

Exercício 277.
Escreva $a^2+b^2 = (a+bi)(c+di)$, o mesmo para c^2+d^2 ; a seguir, use a comutatividade.

Exercício 278.
Utilize indução sobre n.

Exercício 279
Considerando todas as possibilidades de restos na divisão de a e b por 4, supondo que $a^2 + b^2 = 4n + 3$, chegue num absurdo.

Exercício 280.
Para *2)*:

$$\frac{(a,b)}{(c,d)} = \left(\frac{ac+bd}{c^2+d^2}, \frac{-ad+bc}{c^2+d^2}\right).$$

Exercício 281.
Denote por $|r|_{\mathbb{R}}$ o módulo do número real r , e por $|r|_{\mathbb{C}}$ o módulo do número complexo $r = r + 0i$. Agora, mostre que $|r|_{\mathbb{R}} = |r + 0i|_{\mathbb{C}}$.

Exercício 282.
Basta usar a definição de módulo.

Exercício 283.
Basta imitar as outras demonstrações feitas na prova do teorema.

Exercício 284.
Os vetores soma e diferença são precisamente as duas diagonais do paralelogramo formado pelos vetores que representam z e w.

Exercício 285.
i) Essa é a interpretação geométrica do Exercício 284 ;*ii)* Utilize o Teorema de Pythagoras numa representação geométrica da diferença.

Exercício 286.
O lugar geométrico é o círculo de centro em (0,1) e raio 2.

Exercício 287.
$A \cap B$ é a interseção do disco de centro (1,0) e raio 3 com o disco de centro em (0,2)

e raio 2.

Exercício 289.
Este exercício serve como motivação para o Exercício 290.

Exercício 290.
São triângulos retângulos, isósceles; portanto, semelhantes.

Exercício 291.
Suponha $z = a + bi$ e $w = c + di$, e calcule os comprimentos de todos os lados.

Exercício 292.
Os quatro elementos do conjunto $\{i^n z \mid n \in \mathbb{N}\}$ são os pontos do círculo centrado na origem e de raio $|z|$ que estão na intersecção deste com a reta passando por z e a origem, e com a perpendicular a esta última.

Exercício 293.
Trabalhando com a igualdade $(1/w)w = 1$, imite a interpretação geométrica do produto.

Exercício 294.
Utilize o Exercício 291.

Exercício 295.
Utilize duas vezes a definição de conjugado.

Exercício 296.
Utilize as definições de conjugado e de adição de complexos.

Exercício 297.
Obtenha *(iv)* a partir da igualdade $z = w.(z/w)$ e de *(iii)* já demonstrada.

Exercício 298.
Utilize indução sobre n e, para a base de indução, use *(iii)* da última Proposição 9.38.

Exercício 299.
Este fato *nada* tem a ver com o corolário anterior, pois o polinômio em questão não se encaixa nas hipóteses do mesmo.

Exercício 300.
Utilize o Corolário 9.39.

Exercício 301.
Utilize as definições de conjugado e de multiplicação de complexos.

Exercício 304.
Dividir por um número complexo não real é muito mais complicado do que dividir por um número real.

Exercício 305.
Determine geometricamente o conjugado $\overline{w}$. Daí, basta dividir esse complexo por $|w|$, o que geometricamente também é fácil de fazer.

Exercício 306.
Aplique a ideia do Exercício 305.

Exercício 307.
Repare como aqui a prova ficou mais rápida e simples.

Exercício 308.
O conjunto é formado por todos os números $a+bi$, para os quais $(a+5)^2+b^2>16$ (ou seja, pelos números cuja representação no plano cartesiano se encontram fora do círculo de centro em $(-5,0)$ e raio 4).

Exercício 309.
Escreva $z = a+bi$, $w = c+di$, e mostre que $|z-w| = |1-\overline{z}w|$ se, e só se, $(a-c)^2+(b-d)^2 = (1-ac-bd)^2+(bc-ad)^2$. Daí, considere os casos $|z|=1$ e $|w|=1$.

Exercício 310.
a) Lembre que $z+\overline{z} = 2\operatorname{Re}(z)$ e $z-\overline{z} = 2\operatorname{Im}(z)$.

Exercício 311.
Os valores são $\pm\left(\frac{\sqrt{2}}{2}\sqrt{1+\sqrt{5}}+\frac{\sqrt{2}}{2}i\sqrt{-1+\sqrt{5}}\right)$.

Exercício 312.
i) Aqui é importante prestar atenção no "exatamente".

Exercício 313.
Dado $w>0$, se $z=a+bi\in\mathcal{P}$ verificar $z^2=w$, então $w=a^2-b^2$ e $(2ab=0$, com $a>0$ e $b\in\mathbb{R})$, ou $w=a^2-b^2$ e $(2ab=0$, com $a=0$ e $b>0)$. Resta mostrar que apenas a primeira alternativa serve.

Exercício 317.
O erro foi causado pela ambiguidade da expressão $\sqrt{-1}$.

Exercício 319.
$z=i$ é a única solução.

Exercício 320**:** *ii)* Utilize *(i)* para concluir que z_1 e z_2 são raízes de uma equação polinomial com coeficientes reais. Daí, utilize o Corolário 9.40.

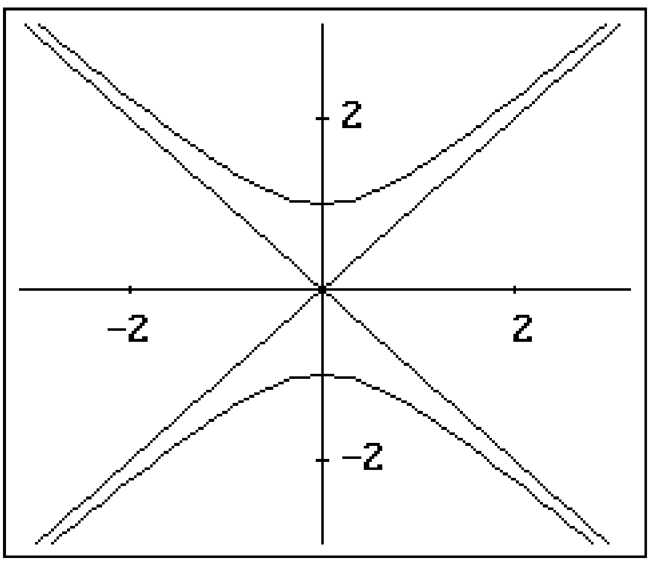
Capítulo 10.

Exercício 325.
Uma maneira é examinar os valores do quociente $p(x)/q(x)$ à medida que x vai crescendo ao infinito. Use o computador ou uma máquina de calcular. Outra maneira de se convencer é vendo que

$$p(x) = x^2\Big(1 + \frac{1000}{x} + \frac{500}{x^2}\Big)\,,$$

e, portanto, $p(x) \cong x^2$ quando x for muito grande; com efeito, para tais valores de x, temos $\frac{1000}{x} \cong 0$ e $\frac{500}{x^2} \cong 0$, comparados com 1.

Exercício 326.
i) $u(x, y) = x^2 - y^2 + 1,\ v(x, y) = 2xy;$
ii) A curva $v(x, y) = 0$ é a união das reta $x = 0$ e $y = 0$, enquanto que a curva $u(x, y) = 0$ está esboçada na figura, com assíntotas $y = \pm x$.



Exercício 328.
Utilize as Definições 10.4 e 10.15.

Exercício 330.
Prove por absurdo, utilizando indução sobre o grau de $p(X)$.

Exercício 331.
A ideia aqui é que qualquer uma das propriedades sobre os polinômios vai requerer que sejam válidas as mesmas propriedades sobre os coeficientes. Como tais coeficientes estão num corpo, tais propriedades sobre os coeficientes são, de fato, válidas.

Exercício 333.
Utiliza indução sobre n.

Exercício 334.
Pelo teorema, a única equação polinomial que tem mais raízes do que o seu grau é a proveniente do polinômio nulo.

Exercício 335.
Simplificar, aqui, significa "dividir por"; mas não podemos dividir por zero, de modo que o erro está precisamente em dizer que vale $b = d + ex$ (para todos os valores de x), e fazer novamente $x = 0$, único valor que x ficou proibido de assumir.

Exercício 336.
A expressão dada é igual a 1.

Exercício 338.
A multiplicidade é 4:

$$x^7 - 11x^6 + 49x^5 - 115x^4 + 160x^3 - 152x^2 + 112x - 48 = (x-2)^4(x^3 - 3x^2 + x - 3)\,,$$

e o polinômio $q(X) = X^3 - 3X^2 + X - 3$ não tem 2 como zero.

Exercício 340.
Inicie observando que, quando calculamos $p(a)$ para qualquer número a, estamos somando uma PG. Isto nos permite concluir que $p(X)$ tem $(X^2 + 1)(X + 1)$ para fatoração real.

Exercício 342.
Supondo que a, b e $a + b$ sejam as raízes da equação dada, desenvolva a expressão $(x - a)(x - b)(x - a - b)$.

Exercício 343.
Prove por contraposição.

Exercício 344.
Desenvolva a expressão $(x-r_1)(x-r_2)(x-r_3)(x-r_4)$ e convença-se que $0 = r_1+r_2+r_3+r_4$, $\alpha = r_1r_2+r_1r_3+r_1r_4+r_2r_3+r_2r_4+r_3r_4$, $\beta = r_2r_3r_4+r_1r_3r_4+r_1r_2r_4+r_1r_2r_3$ e $\gamma = r_1r_2r_3r_4$. Daí, obtenha $u = -\beta/\gamma$ e $v = (\beta^2 - \alpha\gamma)/\gamma^2$.

Exercício 345.
Das equações dadas, obtenha todos os coeficientes do polinômio de grau três que tem x, y e z como raízes; então, resolva a correspondente equação $x^3 - x^2 + x - 1 = 0$, obtendo as soluções 1, i e $-i$.

Capítulo 11.

Exercício 348.
Por absurdo, suponha que a é inversível e divisor de zero, simultaneamente; então, existem b e c, tais que $ab = 1 = ba$, $ac = 0$ e $c \neq 0$. Agora, usando associatividade, calcule bac de duas maneiras distintas.

Exercício 349.
Mostre que o inverso de $a+bi+cj+dk$ é o quatérnio $(a-bi-cj-dk)/(a^2+b^2+c^2+d^2)$. Então, use o Exercício 348.

Exercício 351.

campo numérico	tem inverso multiplicativo? 1/I	1/(1+I)
complexos ($I^2 = -1$)	sim	sim
duais ($I^2 = 0$)	não	sim
hiperbólicos ($I^2 = 1$)	sim	não

Exercício 353.
Ou $z = 0$, ou $z' = 0$, ou z tem a forma $z = \alpha i$, e $z' = \beta i$, para quaisquer $\alpha, \beta \in \mathbb{R}$.

Exercício 362.
Desenvolva a expressão $-1 = (a + bi)^2$ em cada caso.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] **Para números reais:**

[Ba] BAILEY, D. e CRANDALL, R., "On the random character of fundamental constant expansions", *Experimental Math.*, vol 10, pp. 175-190 (2001).

[Car] CARAÇA, B. J., *Conceitos fundamentais da Matemática,* Gradiva Publicações, Coleção Ciências Exatas, Lisboa (1998).

[Ch] CHAMPERNOWNE, D. G., "The construction of decimals normal in the scale of ten", *J. London Math. Soc.* 8, pp. 254-260 (1933).

[D] DEDEKIND, R., *Essays on the Theory of Numbers,* Dover Publications, New York (1963).

[H-W] HARDY,G. H. e WRIGHT, E. M., *An Introduction to Number Theory,* 5th. edition, Oxford Univ. Press, London (1979).

[He] HEATH, Sir T., *The Thirteen Books of Euclid's Elements,* 2nd edition, Dover Publications, New York (1956).

[L] LIMA, E.L. e outros, *A Matemática do Ensino Médio,* Coleção Professor de Matemática, SBM, Rio de Janeiro (2001).

[Li] le LIONNAIS, F., *Les Nombres Remarquables,* Hermann, Paris (1983).

[Me] MENGUE, J., "A normalidade da Constante de Champernowne", in *Anais das Jornadas de Iniciação Científica do IMPA*, pp. 18-42, IMPA, Rio de Janeiro (2004).

[R] REY PASTOR, J., *Elementos de Analisis Algebraico,* Industria Gráfica, Madrid (1958).

[W] WEYL, H., *The Continuum,* Dover, New York (1994).

[2] **Para números complexos:**

[A] ARGAND, R., *Essai sur une maniére de representer les quantités imaginaires dans les constructions géometriques,* Albert Blanchard, Paris (1971). (Reimpressão do original da primeira edição de 1806.)

[B-M] BOTT, R. e MILNOR, J., "On the parallelizability of the spheres", *Bull. Amer. Math. Soc.* 64, pp. 87-89 (1958).

[B] BOYÉ, A. et al., *Images, Imaginaires, Imaginations. Une perspective historique pour l'introduction des nombres complexes,* Ellipses, Paris (1998).

[Caj] CAJORI, F., "History of the exponencial and logarithmic concepts", *Amer. Math. Monthly*, vol 20, pp. 39-42 (1913).

[Cr] CROWE, M. J., *A History of Vector Analysis*, Dover, Notre Dame (1967).

[K] KERVAIRE, M., "Non-parallelizability of the sphere", *Proc. Nat. Acad. Sci. USA* 44, pp. 280-283 (1958).

[Mo] MOUREY, C. V., *La vraie theorie des quantités negatives et des quantités pretendument imaginaires,* Original de 1828/1861(2ed.) reeditado pelo IREM de Dijon, 1992.

[N] NAHIN, P. J., *An Imaginary Tale: The History of* $\sqrt{-1}$*,* Princeton Univ. Press, Princeton (1998).

[Ne] NEVANLINA, R. e PAATERO, V., *Introduction to Complex Analysis*, Addison-Wesley, Reading (1969).

[S-C] STUDY, E. e CARTAN, E., "Nombres Complexes", in *Encyclopédie des Sciences Mathématiques*, t. I, vol I., Paris-Leipzig (1908).

ÍNDICE REMISSIVO

Impressão e acabamento:
XXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXX

Editora da UFRGS • Ramiro Barcelos, 2500 – Porto Alegre, RS – 90035-003 – Fone/fax (51) 3308-5645 – editora@ufrgs.br – www.editora.ufrgs.br • Direção: Sara Viola Rodrigues • Editoração: Luciane Delani (Coordenadora), Carla M. Luzzatto, Fernanda Kautzmann, Michele Bandeira e Rosangela de Mello; suporte editorial: Alexandre Giaparelli Colombo, Jeferson Mello Rocha, Lucas Frota Strey e Renata Baum (bolsistas) • Administração: Najára Machado (coordenadora), Aline Vasconcelos da Silveira, Angela Bittencourt, Jaqueline Trombin, Laerte Balbinot Dias, Maria da Glória Almeida dos Santos e Valéria da Silva Gomes; suporte administrativo: Getúlio Ferreira de Almeida e Janer Bittencourt • Apoio: Laércio Fontoura.

OS AUTORES:

Todos são professores do Instituto de Matemática da UFRGS, onde trabalham há muitos anos. Com formação bastante variada, eles têm em comum o interesse em melhorar a formação matemática dos alunos de cursos de licenciatura em Matemática. Com esse objetivo em mente, eles vêm se reunindo semanalmente há vários anos, bem como lecionando várias disciplinas relevantes na UFRGS. Esse livro resume parte desse trabalho.

Os autores trabalham acreditando que, por mais elementar e antigo que seja um conteúdo matemático, sempre é possível desenvolver novas idéias, novas abordagens e descobrir novos resultados.

UFRGS
EDITORA

ISBN 85-7025-880-1
9788570258809