UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

A impossibilidade das construções clássicas com régua e compasso, com aplicações no ensino básico

Alan Gabriel Cassaro

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP
SÃO CARLOS

Alan Gabriel Cassaro

A impossibilidade das construções clássicas com régua e compasso, com aplicações no ensino básico

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Ires Dias

USP – São Carlos
Agosto de 2023

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

Cassaro, Alan Gabriel
C343i A impossibilidade das construções clássicas com régua e compasso, com aplicações no ensino básico / Alan Gabriel Cassaro; orientadora Ires Dias. -- São Carlos, 2023.
159 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2023.

1. Construções geométricas. 2. Régua e compasso. 3. Duplicação do cubo. 4. Trissecção do ângulo. 5. Construção de polígonos regulares. I. Dias, Ires, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Alan Gabriel Cassaro

The impossibility of classical straightedge-and-compass constructions, with applications in basic education

Dissertation submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP – in accordance with the requirements of the Professional Master's Program in Mathematics in National Network, for the degree of Master in Science. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Profa. Dra. Ires Dias

USP – São Carlos
August 2023

Este trabalho é dedicado a todos que, como eu,
amam a matemática e se emocionam no começo, no meio e no fim
da demonstração de um teorema.

AGRADECIMENTOS

Em determinado momento, após finalizar os estudos do último capítulo das soluções dos problemas de construção com régua e compasso, durante a minha frenética digitação em LaTeX, correndo contra o tempo, me lembrei de um certo Paulo e então várias lembranças começaram a me ocorrer de diversas pessoas que fizeram e fazem parte da minha história com a matemática. Quando eu percebi, havia parado de digitar e começado a escrever o rascunho destes agradecimentos, sem planejamento algum. Tão logo, lágrimas começaram a escorrer e em segundos eu já chorava e soluçava, como há muito tempo não acontecia. Eu sou uma pessoa extremamente abençoada por ter tido a sorte de cruzar com muitas pessoas incríveis que me ajudaram a trilhar o caminho até aqui e sou eternamente grato a cada uma delas.

Agradeço a toda a minha família, que sempre me apoiou em todas as minhas escolhas e sempre me acolheu em todos os momentos difíceis. E também incluo aqui meu agradecimento especial à Ana Catarina, que considero parte da família e para a qual não existem palavras suficientes que traduzam de forma justa tudo o que sinto. Também incluo aqui a Fer, o Thiago e a tia Ruth, sem os quais não teria vencido muitos desafios até aqui.

Quero agradecer a todos os professores que fizeram e fazem parte da minha jornada, desde o ensino fundamental, passando pelo ensino médio, até a graduação e o mestrado. Em particular, quero citar alguns nomes que tiveram uma influência maior. A ordem a seguir não representa nenhum tipo de gradação, até mesmo porque não existe medida que dê conta do enorme papel de cada um deles em minha vida. Porém, sei que todos irão compreender que um deles precisa começar a lista.

Ao professor Paulo Dattori, que foi meu professor no primeiro Programa de Iniciação Científica Jr. da OBMEP e também foi meu professor na graduação, eu agradeço por seus brilhantes ensinamentos, suas aulas inspiradoras e pelos seus pacientes e-mails quando eu estava na escola, que alimentaram minha paixão pela demonstração de teoremas. Eu sei que não fui um ótimo aluno, mas o professor Paulo foi minha inspiração para seguir uma carreira na matemática, e continuo querendo ser cada vez mais como ele. Quero incluir aqui meus agradecimentos à professora Michela Tuchapesk, que contribuiu para as aulas do PIC e também foi minha professora no mestrado. Juntamente com esse agradecimento ao professor Paulo e à professora Michela, preciso agradecer imensamente à OBMEP e a todos que a criaram e a promovem, direta e indiretamente. A OBMEP e o PIC, através do professor Paulo, fizeram com que eu descobrisse o meu amor pela matemática. Dentre várias coisas incríveis que o professor Paulo me ensinou no PIC, foi determinante na minha trajetória o fato de que 1+1 pode ser zero.

À professora e orientadora Ires Dias, com quem tive o primeiro contato em uma reunião do primeiro PICME no ICMC com os medalhistas da OBMEP e professores que apresentaram ali ideias de projeto de Iniciação Científica, e que foi minha professora na graduação e também no mestrado, eu agradeço por todos os seus ensinamentos, orientações e paciência ao longo de todos esses anos. A professora Ires foi como uma mãe durante todos esses anos em que eu fui aluno do PROFMAT, auxiliando em diversos aspectos, muito além do papel de orientadora. Durante o primeiro ano do mestrado, eu fui monitor da professora Ires na disciplina de *Elementos de Matemática* e, a partir do segundo ano do mestrado, eu tive a oportunidade de ser professor do PIC da OBMEP, no polo de Sertãozinho. Agradeço imensamente à professora Ires Dias e ao professor Tiago Henrique Picon por essa oportunidade de retornar ao PIC, mas dessa vez como professor. Ambas as bolsas (da monitoria e do PIC) foram fundamentais para o desenvolvimento deste trabalho, visto que eu não tive bolsa do PROFMAT. Além disso, a professora Ires foi um constante pilar de sustentação para que eu terminasse de escrever esta dissertação quando, em alguns momentos, eu pensei em desistir. Enfim, não há espaço suficiente para descrever todo o auxílio da professora Ires. Tudo o que posso dizer é que este trabalho não existiria sem ela. Muito obrigado, professora Ires.

Ao professor Daniel Levcovitz, que foi meu orientador de iniciação científica durante vários anos e também foi meu professor na graduação, não tenho palavras para agradecer. Foi tanta paciência e tanto aprendizado ao longo de tanto tempo que eu não conseguiria descrever aqui a minha gratidão. O professor Daniel foi minha fonte de inspiração constante durante a graduação e sempre me deu liberdade e apoio para eu escolher tópicos de estudo que me cativaram e fizeram com que eu me apaixonasse ainda mais pela beleza da matemática. Dentre várias coisas incríveis que estudei sob sua orientação, também foi determinante na minha trajetória o fato de que $1+2+2^2+2^3+...$ pode ser convergente.

À professora Miriam Utsumi, que foi minha orientadora no PIBID e também foi minha professora na graduação, também não tenho palavras para agradecer. Além da sabedoria infinita e de todos os ensinamentos matemáticos e pedagógicos, a professora Miriam me ajudou a superar momentos difíceis e, portanto, também foi como uma mãe durante a graduação.

Ao professor Eduardo Tengan, com quem também tive o primeiro contato na já mencionada reunião do primeiro PICME, e que quase foi meu orientador e foi meu professor na graduação, agradeço por suas incríveis e divertidas aulas de álgebra. Foi uma sorte imensa ter tido Álgebra 1 e Álgebra 2 com o professor Tengan, que é uma pessoa sem igual, como sabem todos que o conhecem. O professor Tengan aumentou ainda mais minha paixão por álgebra e suas aulas, sua simplicidade de escrita, seus exemplos intuitivos e seus trocadilhos inesquecíveis são uma constante inspiração para as minhas aulas e foram uma inspiração na escrita deste trabalho.

Ao professor Sérgio Luís Zani, que também estava na já mencionada reunião do primeiro PICME, e foi meu professor na graduação e também no mestrado, agradeço por seus ensina-

mentos e por toda a sua ajuda durante todos esses anos, em particular agradeço pelos inúmeros e-mails sempre prontamente respondidos.

Ao professor Hermano Ribeiro, que foi meu professor no mestrado, agradeço por suas aulas inigualáveis e únicas! Suas aulas foram contagiantes! O professor Hermano gerou lembranças que não se apagam, tais como "DYKA" e "The Boys", e constituem uma inspiração constante nas minhas aulas. O professor Hermano me fez descobrir uma paixão por *matemática discreta* que eu desconhecia, apresentando diversos tópicos fascinantes durante as suas aulas.

À professora Erica Filletti e ao professor Alexandre Cassola, que foram meus professores no mestrado, agradeço por seus ensinamentos e por toda a dedicação e empenho nas aulas ministradas no PROFMAT.

À professora Katia Gonçalves de Azevedo, que é minha coordenadora do Programa de Iniciação Científica Jr. da OBMEP, agradeço pela paciência de sempre e pela compreensão durante o período de conclusão desta dissertação, que foi permeado por uma rotina exaustiva de muito trabalho, incluindo o PIC e os dois cargos de professor que atualmente exerço.

Por fim, quero agradecer a todos os meus amigos, em especial ao Davi, e também quero agradecer a todas as prefeituras nas quais trabalhei ou trabalho como professor de matemática, incluindo todas as pessoas, escolas e alunos que contribuíram para o meu crescimento como pessoa e como professor.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

“Os encantos cativantes desta ciência sublime só são revelados àqueles que têm a coragem de mergulhar profundamente nela.”

(Carl Friedrich Gauss)

RESUMO

CASSARO, A. G. **A impossibilidade das construções clássicas com régua e compasso, com aplicações no ensino básico**. 2023. 159 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2023.

O grande objetivo deste trabalho é fornecer um material completo e autocontido sobre a impossibilidade das construções clássicas com régua e compasso, que possibilite o estudo por qualquer pessoa que se interesse pelo assunto. Para isso, o trabalho é dividido em duas partes. Na primeira parte, são apresentadas as soluções dos problemas de construção com régua e compasso da duplicação do cubo e da trissecção do ângulo, de forma mais simplificada que a usual, em uma tentativa de tornar a teoria mais acessível a um professor do ensino básico. De modo análogo, na segunda parte, o problema de construção de polígonos regulares com régua e compasso é resolvido e então é explicado porque não se pode empregar as mesmas ferramentas construídas nas soluções dos três problemas mencionados para resolver o problema da quadratura do círculo. Por fim, após essas duas partes, são apresentadas algumas ideias para aplicações desses problemas e de suas soluções no ensino básico.

Palavras-chave: Construções geométricas, Régua e compasso, Duplicação do cubo, Trissecção do ângulo, Construção de polígonos regulares.

ABSTRACT

CASSARO, A. G. **The impossibility of classical straightedge-and-compass constructions, with applications in basic education**. 2023. 159 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2023.

The main goal of this work is to provide a complete and self-contained material on the impossibility of classical straightedge-and-compass constructions that enables anyone interested in the subject to study it. To achieve this, the work is divided into two parts. In the first part, solutions to the straightedge-and-compass construction problems of doubling the cube and angle trisection are presented in a more simplified manner than usual, in an attempt to make the theory more accessible to a primary school teacher. Similarly, in the second part, the construction problem of regular polygons with ruler and compass is solved, and then it is explained why the same tools used in the solutions to the three aforementioned problems cannot be employed to solve the problem of squaring the circle. Finally, after these two parts, some ideas for applications of these problems and their solutions in basic education are presented.

Keywords: Geometric constructions, Straightedge and compass, Doubling the cube, Angle trisection, Constructing regular polygons.

LISTA DE ILUSTRAÇÕES

LISTA DE SÍMBOLOS

$\overline{AB}$ — Segmento de reta de extremidades A e B

AB — Medida do segmento de reta de extremidades A e B

$\overrightarrow{AB}$ — Semirreta de origem A e que passa por B

$\overleftrightarrow{AB}$ — Reta que passa pelos pontos A e B

$\widehat{AOB}$ — Ângulo formado pelas semirretas $\overrightarrow{OA}$ e $\overrightarrow{OB}$

$\mathbb{N}$ — $\{1,2,3,4,5,...\}$

$\mathbb{N} \cup \{0\}$ — $\{0,1,2,3,4,5,...\}$

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

De tempos em tempos, matemáticos em universidades ao redor do mundo recebem cartas de entusiastas dizendo que resolveram o problema da trissecção do ângulo. Ainda chegam cartas de matemáticos amadores onde mostram como dividir um ângulo de 60° em três partes iguais usando apenas régua e compasso, embora tenha sido demonstrado há quase duzentos anos que tal construção é impossível. Esse fenômeno em torno da trissecção do ângulo provavelmente existe porque é muito fácil enunciar este problema, mas um tanto difícil compreender sua solução. Isso faz com que qualquer pessoa consiga compreender qual é a questão, mesmo que não seja capaz de entender que o problema está resolvido nem tampouco o que diz a sua solução.

Assim como a trissecção do ângulo, é bem simples enunciar todos os problemas que serão estudados neste trabalho. *Usando apenas uma régua sem marcações e um compasso*, busca-se:

1. Construir um cubo com o dobro do volume de um cubo dado *(duplicação do cubo)*;
2. Dividir um ângulo dado em três ângulos congruentes *(trissecção do ângulo)*;
3. Construir um quadrado com a mesma área de um círculo dado *(quadratura do círculo)*;
4. Construir um polígono regular com um dado número de lados.

E do mesmo modo que a trissecção do ângulo, todos esses problemas têm soluções extremamente avançadas. Os três primeiros são comumente conhecidos como *os três problemas clássicos* da geometria grega. Embora a origem dos quatro problemas seja incerta e envolta em lendas e mitos, eles foram estudados pelos gregos antigos, o que contribuiu para a sua fama nos séculos que se seguiram, mesmo que nenhum matemático da Grécia Antiga tenha conseguido resolvê-los usando apenas régua e compasso. Apesar de comum na Grécia Antiga, a restrição ao uso desses instrumentos não era uma regra de toda a matemática grega.

1.1 Por que usar somente régua e compasso?

Há um mito bem difundido de que a restrição ao uso de régua e compasso estaria relacionada à filosofia de Platão, segundo a qual a régua e o compasso constituiriam instrumentos ideais, que forneceriam construções com alto grau de perfeição, em oposição a ferramentas de verdade, que realizariam construções mecânicas e imperfeitas. Alguém poderia apontar que a régua e o compasso também são ferramentas reais, porém usar uma régua sem marcações equivale a traçar *retas* e usar um compasso equivale a traçar *círculos*, figuras geométricas consideradas superiores na filosofia platônica. Contudo, não há nas obras de Platão recomendações explícitas impondo o uso de retas e círculos como modelo para a geometria grega nem tampouco proibindo a utilização de outras ferramentas nas construções geométricas (ROQUE, 2012, p. 160, 161).

Não conseguindo realizar as construções clássicas com apenas régua e compasso, alguns dos gregos antigos abordaram esses problemas com outros instrumentos, tais como as *cônicas*, a *quadratriz*, a *neusis* e a *espiral de Arquimedes*, e vários outros.[1] Então, se a restrição ao uso da régua e do compasso não era uma lei, como se explica o uso exclusivo desses instrumentos no enunciado dos problemas escrito acima? Embora não se tenha uma resposta precisa para essa pergunta, uma coisa é certa: essa prática não está ligada a Platão, como se acreditou no passado e ainda aparece em alguns livros de matemática. Tatiana Roque desfaz esse mito em seu livro *História da matemática* (ROQUE, 2012). Outra coisa que se sabe com certeza é que a restrição ao uso de régua e compasso permeia *Os Elementos*, de Euclides. Nessa obra não se fala literalmente em "régua e compasso" e sim em retas e círculos: todas as construções são feitas por meio dessas figuras geométricas, definidas abstratamente, embora em nenhum momento essa prática seja colocada como uma regra de modo explícito no livro. Roque (2012, p. 160, 161) escreve:

> Euclides não afirma explicitamente, em lugar nenhum de sua obra [*Os Elementos*], que as construções tenham de ser efetuadas com retas e círculos. Simplesmente elas são, de fato, realizadas desse modo. (...) Referimo-nos especificamente aos *Elementos*, pois a restrição à régua e ao compasso não parece ser importante nem mesmo em outros escritos de Euclides.

Então surge um novo questionamento: Qual foi o motivo do uso exclusivo de régua e compasso nos *Elementos* de Euclides? Há algumas hipóteses que fazem muito sentido e ajudam a entender até mesmo os prováveis propósitos da obra de Euclides. Uma delas é a simplicidade das construções feitas com esses instrumentos, tal como Roque (2012, p. 161) explica:

> As construções feitas desse modo são mais simples e não exigem nenhuma teoria adicional (como seria o caso das construções por meio de cônicas). Desse ponto de

[1] O leitor pode encontrar excelentes soluções com esses instrumentos nas referências (KAZARINOFF, 2003) e (ROQUE, 2012).

> vista, a restrição não seria consequência de uma proibição, mas de uma otimização: deve-se usar a régua e o compasso sempre que possível para simplificar a solução dos problemas de construção.

Ou seja, essa primeira hipótese seria uma motivação pedagógica de Euclides, de modo a facilitar a compreensão dos resultados para abranger um público amplo e até mesmo convencer os leitores de que os resultados ali apresentados são verdadeiros.

Uma outra hipótese muito plausível para o uso restrito de régua e compasso nos *Elementos* é a de que Euclides buscava em sua obra ordenar e sistematizar a geometria, de modo a juntar todos os resultados básicos da matemática desenvolvida até ali de modo organizado. Pensando assim, o uso exclusivo de retas e círculos teria uma origem prática: são as construções suficientes para os resultados apresentados na obra. Roque (2012, p. 163) escreve:

> Na época de Euclides, o conjunto dos conhecimentos dos geômetras já estava bastante desenvolvido e era necessário ordená-lo. Essa ordem implicaria uma gradação da matemática, do nível mais elementar em direção ao superior. E Euclides se teria proposto, nos *Elementos*, a expor a matemática elementar da época, aquela que demanda somente o emprego da régua e do compasso.

Essa segunda explicação é muito interessante e tentadora, pois harmoniza com a simplicidade proposta na primeira hipótese e nos remete ao nome da obra: desse ponto de vista, o título *Os Elementos* provavelmente quer dizer literalmente *"o elementar da matemática"*. Por fim, Roque (2012, p. 163) conclui o seguinte sobre as duas hipóteses:

> Quer optemos pela motivação pedagógica ou por essa segunda razão, de cunho epistemológico, parece mais adequado entender a exclusividade da régua e do compasso nos *Elementos* como uma restrição pragmática cujo objetivo poderia ser apresentar um uso ótimo dos instrumentos mais simples possíveis. Nesse caso, a mensagem implícita nessa obra seria: eis tudo o que se pode fazer em geometria com o uso somente da régua e do compasso.

1.2 Problemas impossíveis

Apesar de os gregos antigos terem obtido soluções com outros instrumentos para os quatro problemas mencionados anteriormente, ao longo do tempo os matemáticos continuaram tentando resolver esses problemas de construção, pois algumas perguntas permaneciam em aberto: Como realizar tais construções com apenas régua e compasso? Será que é realmente possível? Eventualmente surgiu a desconfiança de que talvez *não* fosse possível realizar essas construções com o uso exclusivo de régua e compasso. Fato é que o interesse dos matemáticos

em desvendar o mistério envolvendo essas construções e o uso de régua e compasso levou a descobertas incríveis. Além disso, a sua solução acabou por mostrar conexões surpreendentes entre diversas áreas da matemática, o que contribuiu para que a fama desses problemas alcançasse patamares tão elevados. A questão teve seu desfecho final somente no século XIX, cerca de dois mil anos depois dos estudos dos gregos antigos. Mas essa demora imensa se justifica: *Todas as construções são impossíveis!*

Então surge a pergunta: "Se as construções são impossíveis, como os problemas foram resolvidos?". Para entender esse aparente paradoxo, é necessário esclarecer o que significa resolver esses problemas e o que significa que as construções são impossíveis. Isso será feito através de uma analogia com um exemplo de construção mais simples.

Esqueça por um momento o uso de régua e compasso e considere o seguinte problema: *Obter um quadrado de lado inteiro cuja área seja igual a um número natural dado*.[2] A restrição aqui não é sobre os instrumentos de construção e sim sobre a medida do lado do quadrado, que deve ser um número inteiro. De início pode parecer que a analogia não se aplica, porém o objetivo final é comparar a solução desse problema com as soluções dos problemas de construção com régua e compasso, e não o seu enunciado.

Em primeiro lugar, é preciso entender o enunciado do problema. Quando se escreve "um número natural dado", o que se quer dizer é que, para todo número natural n, deve-se obter um quadrado de área n, cuja medida do lado seja um número inteiro l; além disso, "obter um quadrado" equivale simplesmente a encontrar o lado deste quadrado. A área de um quadrado é dada pelo quadrado da medida de seu lado. Assim, para se obter um quadrado de área n, deve-se encontrar um número inteiro l que satisfaça a seguinte igualdade:

$$l^2 = n.$$

Como a construção deve ser feita para cada número natural n, pode-se começar a analisar a situação pelo primeiro número natural: $n = 1$. Nesse caso, é fácil ver que $l = 1$, pois $1^2 = 1$. Note que l deve ser positivo, pois se trata da medida de um segmento de reta. Como $l = 1$ é um número inteiro, conclui-se que é possível obter um quadrado de área 1 como solicitado no enunciado. Porém a solução do problema não pode parar por aí! Seria um erro muito grande concluir que a construção sempre é possível, para todo número natural, a partir de apenas um caso em particular. Seguindo na lista dos números naturais, tem-se $n = 2$. Para encontrar o número l nesse caso, é necessário resolver a equação a seguir:

$$l^2 = 2,$$

cuja única raiz positiva é $\sqrt{2}$. Ou seja, se um quadrado tem área igual a 2, então obrigatoriamente a medida de seu lado é igual a $\sqrt{2}$, que claramente não é um número inteiro (pode-se argumentar

[2] Uma interessante versão alternativa deste problema seria a seguinte: *Obter um quadrado de lado racional cuja área seja igual a um número dado*. Essa versão é explorada no capítulo de aplicações no ensino.

que $1^2 = 1$ e $2^2 = 4$ e, por isso, $\sqrt{2}$ deve ser um número maior do que 1 e menor do que 2).[3] Logo, não existe um quadrado de lado inteiro cuja área seja igual a 2. Portanto, é impossível obter um quadrado de área 2 com a condição exigida. A investigação termina nesse momento, pois não há mais nada a se fazer. Alguém poderia dizer: "Ainda há outros números a testar. Por exemplo, é possível obter um quadrado de área 4 exatamente como solicitado." Porém, como explicado anteriormente, o problema consiste em obter um quadrado *para cada número natural dado*. Como é impossível obter um quadrado no caso em que o número dado é 2, então é claro que não se pode obter em todos os casos. É fácil perceber que há outros infinitos casos em que não é possível (e também infinitos casos em que é possível), mas isso não importa, pois a impossibilidade de apenas um mostra que não se pode atingir o objetivo para todos. Portanto, o problema está resolvido e a sua solução é a seguinte:

> É impossível obter um quadrado de lado inteiro cuja área seja igual a n, para todo número natural n. Para provar isso, basta exibir um número natural n para o qual é impossível obter um quadrado de lado inteiro l e área n. Tomando $n = 2$, o lado do quadrado deveria medir $\sqrt{2}$, que é um número maior do que 1, pois $1^2 = 1$, e menor do que 2, pois $2^2 = 4$, o que mostra que $\sqrt{2}$ não é um número inteiro. Portanto, é impossível obter um quadrado como solicitado nesse caso, como se queria demonstrar.

Uma observação importante é a seguinte: Se por acaso fosse possível obter um quadrado de lado inteiro e área n para todo natural n, então a demonstração teria que ser feita para *todo* número natural (o que poderia ser feito, por exemplo, através de um procedimento genérico que servisse para qualquer natural dado). Mas o ponto é que ocorre justamente o contrário: não é possível obter um quadrado para todo número natural e por isso é suficiente exibir *apenas um* número natural que não dá certo, para garantir uma demonstração válida.

De modo análogo, quando se escreve "dividir um ângulo dado" no enunciado do problema da *trissecção do ângulo*, o que se quer dizer é que se busca dividir *todos* os ângulos em três partes iguais usando somente régua e compasso. Assim como no caso do problema do quadrado de lado inteiro, alguém poderia exibir um procedimento particular com régua e compasso para trissectar, por exemplo, um ângulo de 180°. Isso de fato é possível, mas não mostra que é possível trissectar todos os ângulos. Para provar que qualquer ângulo pode ser dividido em três partes iguais, seria necessário exibir um procedimento geral com régua e compasso para trissectar um ângulo de medida qualquer, o que é impossível, pois o ângulo de 60° não pode ser trissectado usando apenas régua e compasso, como será mostrado mais adiante. Equivalentemente ao problema do quadrado de lado inteiro, ao se provar que um ângulo de 60° não pode ser dividido em três partes

[3] No momento deste argumento fica claro porque se optou pela versão com "lado inteiro" e não "lado racional": para se evitar a justificativa mais forte de que $\sqrt{2}$ não é racional. Ou seja, buscou-se um exemplo que facilitasse a compreensão tanto do aluno como do professor.

iguais, o problema da trissecção fica resolvido e sua solução mostra que é impossível dividir todos os ângulos em três partes iguais usando somente régua e compasso. Como no problema do quadrado, existem outros infinitos ângulos que não podem ser divididos (e também infinitos ângulos que podem ser divididos), mas isso não importa, pois a impossibilidade de apenas um mostra que não se pode trissectar todos os ângulos com o uso exclusivo de régua e compasso.

A moral da história é que o problema do quadrado de lado inteiro proposto acima está resolvido e sua solução mostra que é impossível atingir o objetivo desejado. Uma conclusão análoga se aplica à duplicação do cubo, à trissecção do ângulo, à quadratura do círculo e à construção de polígonos regulares: *Os problemas estão resolvidos e suas soluções mostram que é impossível realizar tais construções utilizando somente a régua e o compasso*. Com uma pequena alteração, seria sempre possível obter o quadrado com a área desejada: basta permitir que o lado do quadrado tenha como medida qualquer número real. De maneira análoga, basta permitir o uso de outros instrumentos além da régua e do compasso para que se possa trissectar qualquer ângulo, inclusive o ângulo de 60°. Com o uso de outros instrumentos, todas as quatro construções geométricas citadas neste trabalho podem ser realizadas, como os gregos antigos fizeram.

Entretanto, somente com o passar do tempo e com o desenvolvimento de novas ferramentas matemáticas é que os problemas de construção puderam ser completamente resolvidos. Mais de 2000 anos depois dos estudos dos gregos antigos, em 1837, Pierre Louis Wantzel provou que, usando apenas régua e compasso, é impossível duplicar um cubo de volume igual a 1, trissectar um ângulo de 60° e construir um n-ágono regular quando n é divisível por um primo que não é da forma $2^k + 1$ ou quando n é divisível pelo quadrado de qualquer primo maior do que 2. E, em 1882, Ferdinand von Lindemann provou que a quadratura do círculo é impossível através do uso restrito de régua e compasso (KAZARINOFF, 2003). Ao longo deste trabalho, a maioria dessas demonstrações serão apresentadas em detalhes, mas com esperança a analogia inicial do quadrado de lado inteiro ilustrará desde já e de modo claro o aparente paradoxo das soluções dos quatro problemas de construção. Ao passo que o problema mais simples do quadrado exigiu apenas operações básicas, os quatro problemas de construção com régua e compasso exigirão um pouco mais de matemática. Neste trabalho, busca-se construir toda a teoria necessária para as suas soluções de modo rigoroso, mas acessível. No decorrer dos próximos capítulos, serão provados todos os resultados necessários para apresentar as soluções dos problemas de construção com régua e compasso, porém alguns resultados elementares de geometria e de divisibilidade serão assumidos sem demonstração, pois esse não é o foco do trabalho.

1.3 Problemas não resolvidos

Além de as soluções dos quatro problemas conterem um pouco de matemática avançada, se tratam de provas indiretas, no sentido que não apresentam quase nenhuma construção geomé-

trica concretamente. Pelo contrário, são provas abstratas que nem mesmo usam ferramentas da geometria e sim resultados da álgebra. Talvez também por isso alguns matemáticos amadores não aceitem a solução e insistam em perder tempo procurando uma construção geométrica com régua e compasso para trissectar o ângulo de 60°, que seria tão concreta e direta para todos se não fosse inexistente. Seja qual for o motivo, o fato é que compreender a solução do problema da trissecção do ângulo é muito mais difícil do que entender o seu simples enunciado, e a existência de pessoas que ainda tentam trissectar o ângulo de 60° e qualquer outro ângulo é uma consequência disso.

Outro fato que talvez possa confundir matemáticos amadores é que também há problemas não resolvidos em matemática. Um exemplo famoso é a *Conjectura de Goldbach*, que afirma que todo número par maior do que 2 é a soma de dois números primos. Ainda não há uma demonstração de que essa afirmação é verdadeira. Então, neste caso há ainda perguntas sem respostas: Será que existe algum número par que não pode ser escrito como a soma de dois números primos assim como existem ângulos que não podem ser trissectados usando somente régua e compasso? Ou será que realmente vale para todo número par maior do que 2? Será que é mesmo possível responder essas perguntas? Há indícios de que provavelmente não seja o mesmo caso da trissecção do ângulo, onde falha em algum caso, porém o fato é que o problema continua em aberto. Então é importante que se entenda a diferença: enquanto a Conjectura de Goldbach é um problema que não foi resolvido até o momento da escrita deste trabalho, a trissecção do ângulo é um problema que já foi resolvido e que diz que é impossível trissectar todo ângulo com apenas régua e compasso. Essa diferença entre *problemas não resolvidos* e *problemas resolvidos na negativa* (cujas soluções mostram que não é possível fazer o que se pretendia) é um ponto chave do qual os "trissectores de ângulo" provavelmente não têm conhecimento.

Deste modo, percebe-se que de fato há uma dificuldade em compreender por completo os problemas clássicos de construção geométrica, pois é contra-intuitivo que não seja possível de jeito algum criar construções com régua e compasso para dividir todo ângulo em três partes iguais ou construir um cubo com o dobro do volume de um dado cubo, e menos intuitivo ainda é o fato de que podemos fazer demonstrações algébricas de que tais construções não existem. Alguém poderia pensar que certamente é possível e, se ninguém conseguiu fazer, é porque simplesmente se tratam de construções muito difíceis. Sem conhecimento e explanação, pode parecer inesperado e frustrante que problemas tão fáceis de enunciar tenham soluções tão difíceis, mas após um pouco de estudo se vê que na realidade é surpreendente e belo. Com isso em mente, um dos objetivos deste trabalho é tentar simplificar e esclarecer as soluções, com foco no professor de matemática e no processo de ensino-aprendizagem. Ao se dar conta dessa beleza contra-intuitiva e das surpreendentes conexões entre áreas aparentemente distantes da matemática, talvez os professores e alunos se interessem mais por esses problemas. Como Kazarinoff (2003) escreve em seu livro:

"O capítulo final da história desses antigos problemas de construção ainda está sendo escrito. É a disseminação de suas soluções e da aritmética requintada que eles envolvem."

Espera-se que, através deste trabalho, seja possível escrever uma pequena seção neste capítulo final da história dos problemas de construção, em particular uma seção voltada para o ensino básico de matemática. Assim, ao se cumprir o objetivo de apresentar as soluções completas e simplificadas ao professor do ensino básico, se está concretizando o grande propósito deste trabalho, que é a disseminação das soluções dos problemas clássicos de construção com régua e compasso e da álgebra tão elegante que faz parte das mesmas. Afinal, cada uma dessas soluções é o resultado de um grande esforço intelectual: todas são baseadas em séculos de trabalho e no desenvolvimento de nova matemática. Embora enunciadas na negativa ("não é possível realizar tais construções"), essas soluções são realizações positivas e grandes contribuições para o conhecimento humano.[4]

[4] As últimas frases deste parágrafo foram inspiradas e adaptadas de uma fala de Oskar Morgenstern presente no livro *Famous problems of geometry and how to solve them*, de Benjamin Bold (BOLD, 1982).

CAPÍTULO

2

CONSTRUÇÃO COM RÉGUA E COMPASSO

Para iniciar um estudo rigoroso das construções geométricas, é necessário esclarecer o que significa *construção com régua e compasso* no contexto original da geometria euclidiana plana e então traduzir esse significado para o contexto da álgebra abstrata. Assim, na primeira seção deste capítulo serão estabelecidas as definições e regras básicas das construções a serem estudadas neste trabalho, enquanto que nas demais seções será feita a transição para o contexto da geometria analítica, seguida da interpretação algébrica dos conceitos e regras iniciais.

2.1 Pontos construtíveis

De modo informal e intuitivo, pode-se pensar que fazer uma *construção geométrica com régua e compasso* consiste em executar uma sequência de construções que utilize, a cada nova etapa, apenas pontos, segmentos e curvas previamente obtidos nas etapas anteriores usando-se somente régua e compasso. Pensando especificamente nos pontos que podem ser obtidos com esses instrumentos, é natural pensar que, para gerar novos pontos com régua e compasso, é necessário que se utilize pontos previamente obtidos deste modo. Percebe-se assim que a obtenção de pontos com régua e compasso é um processo *recursivo*: pontos anteriormente obtidos com esses instrumentos podem gerar novos pontos que, por sua vez, podem gerar novos pontos, e assim sucessivamente. Pensando de trás para frente, o único modo de se obter novos pontos com régua e compasso é usando pontos antes construídos que, por sua vez, precisam ter sido construídos a partir de pontos preexistentes, e assim por diante até... Até quando? Qual é o início dessa *recorrência*? Ela parece não ter um início. De fato, sem assumir nenhum ponto "construído a priori", não existe maneira de iniciar uma construção com régua e compasso, pois não há um modo de iniciar uma construção a partir do plano em branco, sem ter *pontos iniciais dados* a partir dos quais se possa traçar uma reta com a régua ou uma circunferência com o compasso. Então poderia se imaginar que *um ponto inicial* resolveria o problema, porém tampouco é possível traçar uma reta ou uma circunferência com esses instrumentos a partir de

apenas um ponto. Diante disso, percebe-se que é preciso estabelecer *dois pontos iniciais* a partir dos quais se poderá construir efetivamente novos pontos com régua e compasso. Os "pontos que podem ser construídos com régua e compasso" serão chamados logo menos de "pontos construtíveis", mas o fato é que os dois pontos iniciais dados sem construção devem entrar de modo axiomático na definição de "pontos construtíveis", pois sem eles não há como iniciar nenhuma construção.

Assim, através desse raciocínio intuitivo, é necessário que se entenda que o processo de qualquer construção com régua e compasso que se faça é um processo recursivo, que tem início nos dois pontos iniciais dados e, a partir de operações permitidas por esses instrumentos, gera novos pontos que, por sua vez, geram novos pontos, e assim por diante. Tendo em mente este espírito é que se inicia a formalização da teoria no próximo parágrafo. Antes porém, deve-se observar que a parte teórica desenvolvida neste trabalho seguiu a linha principal do que é feito em Kazarinoff (2003), porém a sequência e a forma de apresentar foram, em sua maior parte, alteradas e suplementadas com novas definições e proposições; além disso, buscou-se detalhar e explicar todas as afirmações e demonstrações feitas, procurando sempre se introduzir cada nova ideia com exemplos, de modo a ilustrar a teoria e tentar fornecer um raciocínio lógico e intuitivo.

Para iniciar a formalização no contexto da geometria euclidiana plana, parte-se de apenas dois pontos distintos no plano euclidiano, denominados de O e A, que estão, por definição, a uma unidade de distância um do outro. Como os pontos O e A são fornecidos sem construção, mas são necessários para se iniciar qualquer construção geométrica com régua e compasso, será dito que eles são *pontos contrutíveis*.

Nesse plano, somente é permitido o uso de:

- uma *régua sem marcações*, com a qual se pode apenas traçar retas;
- um *compasso*, com o qual se pode apenas traçar circunferências.

É importante frisar que a "régua" referida aqui não é uma régua usual no sentido que as pessoas estão acostumadas, e sim uma régua sem quaisquer marcações de medidas que não permite, portanto, qualquer comparação de distâncias.

Uma vez estabelecidos os *pontos construtíveis iniciais* e os *instrumentos admitidos*, pode-se descrever as *operações de construção* permitidas para se realizar uma construção com régua e compasso:

1. Com a *régua* pode-se traçar uma reta passando por dois pontos construtíveis;
2. Com o *compasso* pode-se traçar uma circunferência tendo como centro um ponto construtível e como raio a distância entre dois pontos construtíveis.

Além disso, ao se realizar qualquer construção geométrica com régua e compasso, as operações acima podem ser executadas apenas um número finito de vezes.

Observação 1 (Tranferência de distâncias)**.** Com o compasso que se conhece hoje em dia, é possível *transferir distâncias*, ou seja, pode-se posicionar as pontas do compasso em dois pontos distintos do plano, obtendo assim a distância entre esses pontos, e então levantar o compasso do papel e posicionar sua ponta seca em qualquer outro ponto do plano para traçar uma circunferência que tenha como raio aquela distância obtida, pois o compasso moderno é ajustável e mantém a abertura ao ser retirado da superfície onde suas pontas estão apoiadas. Por outro lado, essa transferência de distância não podia ser feita com o compasso dos gregos antigos, porque o mesmo se fechava ao ser alçado da superfície onde se fazia a construção e assim só era possível traçar uma circunferência posicionando a ponta seca do compasso em um ponto C do plano e a outra ponta em um ponto distinto P (o centro e o raio da circunferência assim traçada eram, respectivamente, o ponto C e a distância CP). Deste modo, a segunda operação tal como foi enunciada só pode ser executada com o compasso moderno. Caso contrário, se estivesse disponível apenas o compasso dos gregos antigos, tal operação deveria ser assim enunciada: *Com o compasso pode-se traçar uma circunferência que tenha como centro um ponto construtível e que passe por outro ponto construtível (diferente de seu centro).* Felizmente, pode-se provar[1] que tudo o que é feito com a régua e o compasso moderno poderia ser feito com a régua e o compasso dos gregos antigos, o que é muito útil, pois as construções geométricas com régua e compasso podem ser muito encurtadas ao se fazer uso da *transferência de distâncias* (KAZARINOFF, 2003).

Deve-se observar também que os únicos *pontos construtíveis* definidos até o momento são os pontos iniciais O e A. Deste modo, enquanto não for feita uma definição mais ampla de pontos construtíveis, as operações acima estarão usando apenas os dois pontos iniciais, assim como as definições que serão apresentadas a seguir, que basicamente estabelecem como *construtíveis* todos aqueles objetos que podem ser obtidos a partir das operações permitidas.

Definição 1 (Segmento construtível)**.** Um *segmento construtível* é um segmento de reta cujas extremidades são pontos construtíveis.

Definição 2 (Reta construtível)**.** Uma *reta construtível* é uma reta que contém pelo menos dois pontos construtíveis.

Definição 3 (Semirreta construtível)**.** Uma *semirreta construtível* é uma semirreta cuja origem é um ponto construtível e que contém no mínimo outro ponto construtível (distinto de sua origem).

Definição 4 (Ângulo construtível)**.** Um *ângulo construtível* é um ângulo formado por duas semirretas construtíveis de mesma origem.

[1] O leitor pode encontrar uma demonstração na referência (KAZARINOFF, 2003).

Definição 5 (Circunferência construtível)**.** Uma *circunferência construtível* é uma circunferência cujo centro é um ponto construtível e cujo raio é a distância entre dois pontos construtíveis.

A princípio, a definição a seguir poderá parecer confusa. Por isso é indispensável lembrar que os únicos pontos construtíveis existentes até o momento são os pontos O e A, e que, portanto, as definições acima usaram somente esses dois pontos iniciais até aqui, como já foi observado antes de elas serem enunciadas, mas que vale reforçar porque é uma passagem delicada. Ainda não foi apresentada outra definição de pontos construtíveis além dos pontos iniciais, porém finalmente há condições para isso, desde que se lembre também que o processo de obtenção de pontos construídos com régua e compasso (i.e., pontos construtíveis) é um processo *recursivo*, ou seja, *cada novo ponto construtível é obtido a partir de pontos construtíveis preexistentes*, como explicado no início desta seção.

Definição 6 (Ponto construtível)**.** Um *ponto construtível* é:

(i) O, A; ou

(ii) um ponto de interseção entre duas retas construtíveis concorrentes; ou

(iii) um ponto de interseção entre uma reta e uma circunferência construtíveis; ou

(iv) um ponto de interseção entre duas circunferências construtíveis distintas.

Os pontos iniciais O e A já haviam sido definidos como pontos construtíveis no texto, o que foi essencial, porém eles foram inclusos nessa definição para unificar e centralizar todas as definições de *ponto construtível*.

A confusão inicial vem do fato que "pontos construtíveis" foram usados para se definir retas e circunferências construtíveis e essas por sua vez foram utilizadas para se definir "pontos construtíveis". Sem a devida explicação, tem-se a sensação de que algo está errado! Porém, com o devido conhecimento, tudo faz sentido. Na realidade, *pontos construtíveis preexistentes* (que no início eram apenas O e A) foram usados para gerar retas e circunferências construtíveis e essas por sua vez geraram *novos pontos construtíveis*, os quais foram então usados para gerar novas retas e circunferências, e assim sucessivamente.

Por fim, é possível resumir uma *construção com régua e compasso* de modo formal. Inicia-se com apenas dois pontos construtíveis, O e A. A partir deles, pode-se realizar operações de construção e assim se obter novos pontos com régua e compasso. Esses novos pontos são então chamados de pontos construtíveis, pois foram obtidos a partir de pontos construtíveis preexistentes e de operações permitidas. Com isso, o conjunto de pontos contrutíveis é ampliado. A partir deste conjunto ampliado de pontos, pode-se executar mais operações de construção e assim se obter novos pontos, e de maneira análoga estes pontos são chamados de pontos

construtíveis. Deste modo, o conjunto de pontos construtíveis é mais uma vez ampliado. Esse processo pode ser repetido tantas vezes quanto se queira, gerando assim uma infinidade de pontos construtíveis.

Observação 2. Uma consequência importante da definição 6 é que, a partir dos pontos construtíveis iniciais O e A, é possível obter pontos construtíveis indefinidamente efetuando-se as operações de construção permitidas um número finito de vezes.

Daqui em diante, a característica de algum objeto "poder ser ou não construído com régua e compasso" se traduz como "ser ou não construtível".

2.2 Sistema de coordenadas cartesiano

Uma vez esclarecido o que exatamente significa *construção com régua e compasso* no contexto original da geometria euclidiana plana, se faz necessária a transição para o terreno da geometria analítica, que permitirá transformar problemas clássicos de construção em problemas algébricos. Para isso, é inserido um sistema de coordenadas cartesiano no plano euclidiano de modo que o ponto construtível O fique identificado com a origem $(0,0)$ e o ponto construtível A fique identificado com o ponto $(1,0)$.

É natural que o próximo passo seja tentar identificar as coordenadas de outros pontos construtíveis nesse sistema cartesiano. Após uma investigação inicial, não é tão difícil perceber que todos os pontos de coordenadas racionais são construtíveis, porém é um pouco trabalhoso demonstrar este fato de modo rigoroso, e este é o objetivo desta seção. Por isso, essa demonstração será feita passo a passo, tentando sempre que possível ilustrar cada etapa com exemplos, com o intuito de tornar o processo mais intuitivo.

No que segue, o símbolo $\overline{AB}$ é usado para denotar o segmento de reta de extremidades A e B, enquanto que AB denota a *medida* do segmento $\overline{AB}$; o símbolo $\overrightarrow{AB}$ é usado para denotar a semirreta de origem A que passa por B, e $\overleftrightarrow{AB}$ denota a reta que passa pelos pontos A e B. Por outro lado, o símbolo $\widehat{AOB}$ será usado para denotar tanto o ângulo formado pelas semirretas $\overrightarrow{OA}$ e $\overrightarrow{OB}$ como a medida desse ângulo. Além disso, nesta seção serão usados os clássicos *casos de congruência de triângulos* da geometria euclidiana plana.

Inicialmente serão feitas as seguintes construções com régua e compasso: a construção da mediatriz de um segmento de reta; a construção de uma reta paralela a outra reta; e a construção dos eixos x e y do plano cartesiano. Essas construções iniciais serão úteis em vários momentos e, além disso, constituem ótimos exemplos para serem feitos com os alunos em uma primeira aula sobre construções geométricas com régua e compasso. É importante que o professor saiba distinguir a linguagem formal aqui utilizada da linguagem prática a ser usada em sala de aula. Por exemplo, a primeira afirmação do lema abaixo pode ser colocada em termos mais simples do seguinte modo: *A mediatriz de um segmento pode ser construída com régua e compasso*.

Lema 1. Valem as seguintes afirmações:

(i) a mediatriz de um segmento construtível é uma reta construtível;

(ii) a reta paralela a uma reta construtível r e que passa por um ponto construtível P, tal que $P \notin r$, é uma reta construtível;

(iii) os eixos x e y são retas construtíveis.

Demonstração. A demonstração será feita item por item.

(i) A mediatriz de um segmento de reta é a reta perpendicular ao segmento que passa pelo ponto médio do mesmo.

Seja então $\overline{CD}$ um segmento de reta construtível arbitrário. A construção da mediatriz de $\overline{CD}$ apresentada a seguir está ilustrada na figura 1.

Pela definição 1, tem-se que as extremidades C e D do segmento de reta $\overline{CD}$ são pontos construtíveis. Então trace a circunferência construtível $\mathscr{C}$ de centro C e raio CD e a circunferência construtível $\mathscr{D}$ de centro D e raio CD. Chame as interseções entre $\mathscr{C}$ e $\mathscr{D}$ de P e Q, que são portanto pontos construtíveis. Por fim, trace a reta r que passa por P e Q. Pela definição 2, r é uma reta construtível, pois contém pelo menos dois pontos construtíveis. Será provado que r é a mediatriz de $\overline{CD}$.

Chame de M o ponto de interseção entre $\overline{CD}$ e r. O objetivo é provar que M é o ponto médio de $\overline{CD}$ e que $\widehat{CMP} = 90°$. Note que CP e CQ são raios da circunferência $\mathscr{C}$ e, portanto, $CP = CQ = CD$; analogamente, DP e DQ são raios da circunferência $\mathscr{D}$ e, portanto, $DP = DQ = CD$. Logo, $CP = DP$ e $CQ = DQ$, e assim, pelo *caso LLL* de congruência de triângulos, $\triangle PCQ$ e $\triangle PDQ$ são triângulos congruentes, pois possuem três pares de lados congruentes. Segue que os ângulos $\widehat{CPM}$ e $\widehat{DPM}$ são congruentes, e assim, pelo *caso LAL* de congruência de triângulos, $\triangle CPM$ e $\triangle DPM$ são triângulos congruentes, pois possuem dois pares de lados congruentes e os ângulos entre esses lados também sâo congruentes. Portanto, $CM = DM$ e $\widehat{CMP} = \widehat{DMP}$. De $CM = DM$, tem-se que M é o ponto médio de $\overline{CD}$; e de $\widehat{CMP} = \widehat{DMP}$, segue que $\widehat{CMP} = 90°$, pois $\widehat{CMP} + \widehat{DMP} = 180°$. Portanto, r é a mediatriz do segmento $\overline{CD}$ e, assim sendo, conclui-se que a mediatriz de $\overline{CD}$ é uma reta construtível.

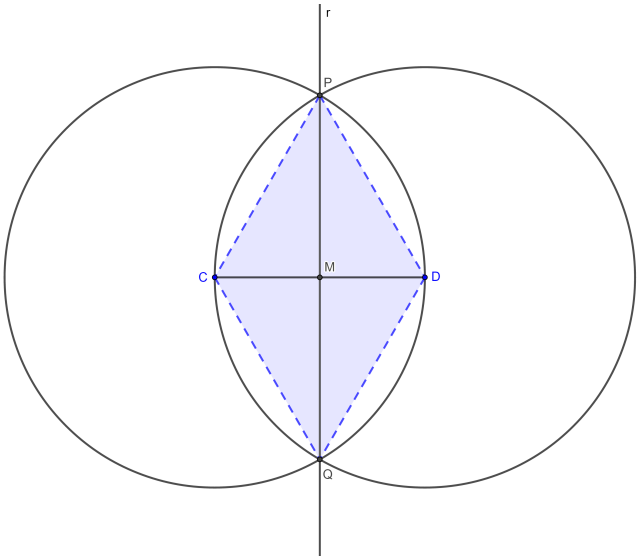


Figura 1 – Construção da mediatriz.

(ii) Sejam r uma reta construtível e P um ponto construtível quaisquer, tais que $P \notin r$. O objetivo é construir com régua e compasso a reta paralela à r que passa por P. Essa construção é apresentada a seguir e ilustrada na figura 2.

Pela definição 2, r contém pelo menos dois pontos construtíveis, pois é uma reta construtível. Sejam então $C, D \in r$ dois pontos construtíveis. Trace a reta construtível s que passa pelos pontos construtíveis C e P, e a circunferência construtível $\mathscr{C}$ de centro P e raio PC; a reta s e a circunferência $\mathscr{C}$ se intersectam em dois pontos, sendo que um deles é o ponto C e o outro será denotado por P', que é portanto um ponto construtível. O objetivo agora é construir um triângulo com lado $\overline{P'P}$ que seja congruente ao triângulo $\triangle PCD$ de modo que o lado $\overline{P'P}$ do novo triângulo seja correspondente ao lado $\overline{PC}$ do $\triangle PCD$. Para isso, basta traçar a circunferência construtível $\mathscr{D}$ de centro P e raio CD e a circunferência construtível $\mathscr{E}$ de centro P' e raio PD; chame de D' o ponto de interseção entre $\mathscr{D}$ e $\mathscr{E}$ que está no semiplano α gerado por s tal que $D \in \alpha$. Por fim, trace a reta r' que passa por P e D'. Por ser uma interseção de duas circunferências construtíveis, o ponto D' é construtível; por sua vez, a reta r' é construtível, pois contém pelo menos dois pontos construtíveis. Será provado que a reta r' é paralela à reta r. Para isso, observe que:

- $PC = P'P$ (raio da circunferência $\mathscr{C}$);
- $CD = PD'$ (raio da circunferência $\mathscr{D}$);
- $PD = P'D'$ (raio da circunferência $\mathscr{E}$).

Logo, pelo *caso LLL* de congruência de triângulos, $\triangle PCD$ e $\triangle P'PD'$ são triângulos congruentes. Segue que os ângulos $\widehat{PCD}$ e $\widehat{P'PD'}$ são congruentes. Ou seja, são congruentes os ângulos que a reta transversal s forma com as retas r e r'. Portanto, as retas r e r' são paralelas e, assim sendo, conclui-se que é construtível a reta que é paralela a uma reta construtível e que passa por um ponto fora dela.

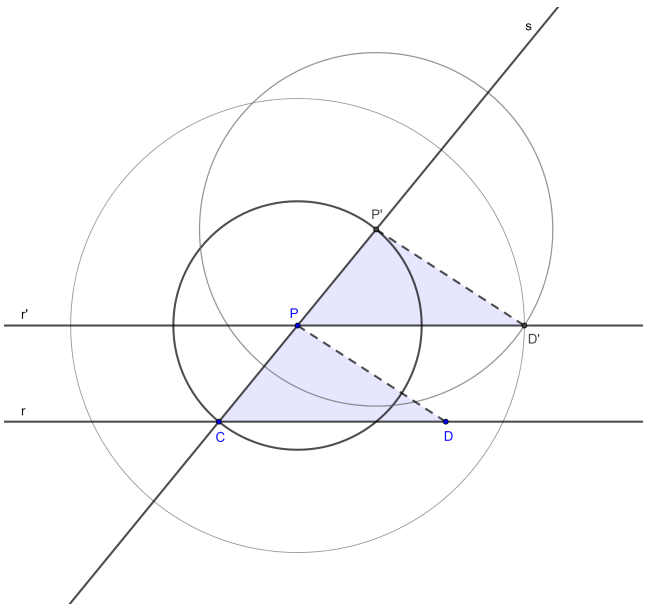


Figura 2 – Construção da reta paralela.

(iii) Note que o eixo x contém os pontos construtíveis $O = (0,0)$ e $A = (1,0)$. Portanto, pela definição 2, o eixo x é uma reta construtível. Agora trace a circunferência construtível $\mathscr{C}$ de centro $(0,0)$ e raio $OA = 1$. As interseções entre a circunferência $\mathscr{C}$ e o eixo x são os pontos $A = (1,0)$ e $A' \doteq (-1,0)$. Logo, como a circunferência $\mathscr{C}$ e o eixo x são construtíveis, o ponto A' é construtível. Segue então que o segmento de reta $\overline{A'A}$ é construtível, pois suas extremidades são pontos construtíveis. Por outro lado, o eixo y é a mediatriz do segmento $\overline{A'A}$ e, portanto, pelo item (i) acima, o eixo y é uma reta construtível. □

Com os resultados acima, alguns pontos construtíveis podem ser facilmente identificados. Por exemplo, traçando a circunferência $\mathscr{C}_1$ de centro $(1,0)$ e raio $OA = 1$, obtém-se um novo ponto construtível, de coordenadas $(2,0)$, que é uma das interseções entre $\mathscr{C}_1$ e o eixo x. Note que o eixo x é uma reta construtível, pelo lema 1, e que a circunferência $\mathscr{C}_1$ é construtível, pois seu centro é um ponto construtível e seu raio é a distância entre dois pontos construtíveis. Logo, como a circunferência $\mathscr{C}_1$ e o eixo x são construtíveis, segue que o ponto $(2,0)$ é de fato construtível. A partir disso, traçando a circunferência $\mathscr{C}_2$ de centro $(2,0)$ e raio 1, obtém-se de modo análogo o ponto construtível $(3,0)$. Repetindo os mesmos passos, conclui-se que são construtíveis os pontos $(4,0), (5,0), (6,0)$ e assim por diante. Essas construções são ilustradas na figura 3.

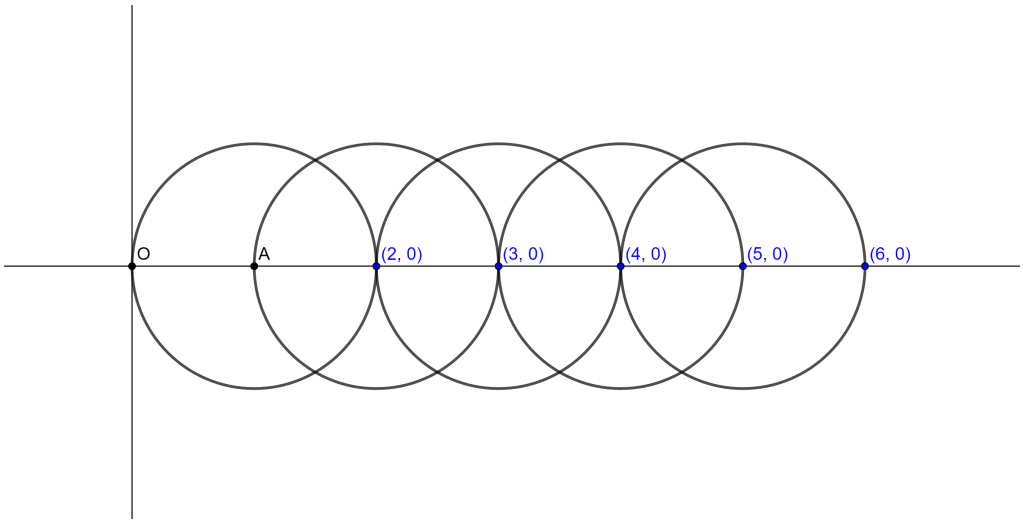


Figura 3 – Pontos construtíveis da forma $(n,0)$, $n \in \mathbb{N}$.

As conclusões acima são formalizadas na proposição a seguir.

Proposição 1. Se $n \in \mathbb{N}$, então o ponto $(n,0)$ é construtível.

Demonstração. Considere o conjunto

$$X = \{n \in \mathbb{N} \mid (n,0) \text{ é construtível}\} \subseteq \mathbb{N}.$$

Esse subconjunto dos naturais tem as seguintes propriedades:

(i) $1 \in X$, pois $(1,0)$ é construtível por definição.

(ii) Se $n \in X$, então $n+1 \in X$. De fato, suponha que $n \in X$, i.e., $(n,0)$ é construtível. Trace a circunferência $\mathscr{C}_n$ de centro $(n,0)$ e raio $OA = 1$. Essa circunferência é construtível, pois seu centro é um ponto construtível e seu raio é a distância entre dois pontos construtíveis. Note que $(n+1,0)$ é um ponto de interseção entre a circunferência construtível $\mathscr{C}_n$ e o eixo x. Logo, $(n+1,0)$ é construtível, ou seja, $n+1 \in X$.

Pelo *Princípio da Indução Finita*, segue de (i) e (ii) que $X = \mathbb{N}$. Portanto, $(n,0)$ é construtível, para todo $n \in \mathbb{N}$. □

Uma consequência imediata da proposição 1 é que toda circunferência de centro em um ponto construtível e raio $n \in \mathbb{N}$ é construtível, pois seu raio é a distância entre os pontos construtíveis $(0,0)$ e $(n,0)$. Com isso, fica fácil estender o resultado acima para todo $n \in \mathbb{Z}$ e para os pontos análogos do eixo y.

Proposição 2. Se $n \in \mathbb{Z}$, então os pontos $(n,0)$ e $(0,n)$ são construtíveis.

Demonstração. Seja n um número inteiro qualquer. Se $n = 0$, o ponto $(0,0)$ é construtível, por definição. Suponha então que $n \neq 0$ e trace a circunferência construtível $\mathscr{C}$ de centro $(0,0)$ e raio $|n| \in \mathbb{N}$. A circunferência $\mathscr{C}$ intersecta o eixo x nos pontos $(|n|,0)$ e $(-|n|,0)$, e intersecta o eixo y nos pontos $(0,|n|)$ e $(0,-|n|)$. Como $n = |n|$ ou $n = -|n|$, segue que $(n,0)$ é uma das interseções entre $\mathscr{C}$ e o eixo x, e $(0,n)$ é uma das interseções entre $\mathscr{C}$ e o eixo y. Portanto, $(n,0)$ e $(0,n)$ são pontos construtíveis. □

A construção chave da demonstração da proposição 2 está ilustrada na figura 4.

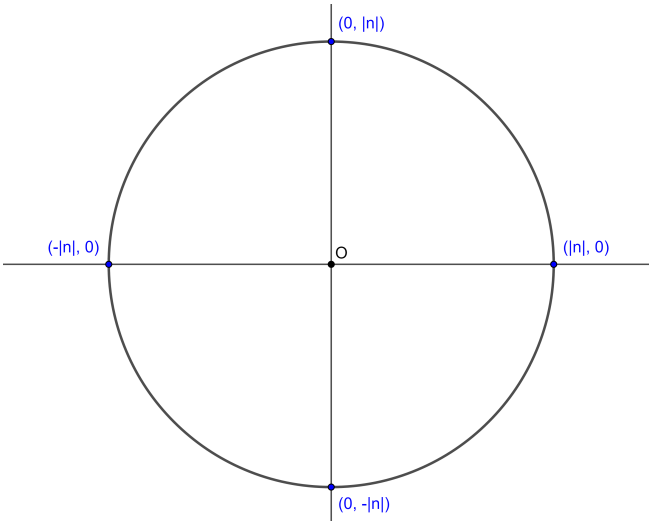


Figura 4 – Pontos construtíveis das formas $(n,0)$ e $(0,n)$, $n \in \mathbb{Z}$.

Tendo a proposição 2 em mãos, basta um pequeno passo para mostrar que todos os pontos de coordenadas inteiras são construtíveis.

Proposição 3. Se $m,n \in \mathbb{Z}$, então o ponto (m,n) é construtível.

Demonstração. Sejam m e n números inteiros quaisquer. Se $m = 0$ ou $n = 0$, então o ponto (m,n) é construtível, pela proposição 2. Suponha então que $m \neq 0$ e $n \neq 0$. Pela proposição 2, $(m,0)$ e $(0,n)$ são pontos construtíveis. Então trace a reta r paralela ao eixo y que passa pelo ponto $(m,0)$ e trace a reta s paralela ao eixo x que passa pelo ponto $(0,n)$. Pelo lema 1, as retas r e s são construtíveis. Além disso, r e s se intersectam no ponto (m,n). Portanto, pela definição 6, o ponto (m,n) é construtível. □

Assim, são construtíveis todos os pontos cujas coordenadas são números inteiros. Naturalmente, o próximo passo é estender o resultado para os números racionais. Isso será feito através dos próximos dois resultados.

Lema 2. Se $r \in \mathbb{Q}$, então o ponto $(r,1)$ é construtível.

Demonstração. Seja r um número racional qualquer. Se $r = 0$, o ponto $(0,1)$ é construtível, pela proposição 3. Suponha então que $r \neq 0$. Logo, existem $m,n \in \mathbb{Z}$, $m,n \neq 0$, tais que $r = \frac{m}{n}$. Trace a reta s que passa pelos pontos construtíveis $(0,0)$ e (m,n) e a reta t que passa pelos pontos construtíveis $(0,1)$ e $(m,1)$. Note que s e t são retas construtíveis, pois ambas contêm no mínimo dois pontos construtíveis. Claramente, uma equação de t é $y = 1$; e como $(0,0)$ e (m,n) são pontos de s, sendo (x,y) um outro ponto qualquer de s, tem-se:

$$\frac{y-0}{x-0} = \frac{n-0}{m-0} \Rightarrow my = nx \Rightarrow nx - my = 0.$$

Logo, $nx - my = 0$ é uma equação de s. Assim, para encontrar o ponto de interseção entre s e t, basta resolver o sistema a seguir.

$$\begin{cases} nx - my = 0 \\ y = 1 \end{cases}$$

Substituindo $y = 1$ na primeira equação, obtém-se $nx - m = 0$. Logo, $x = \frac{m}{n}$ e, assim, $\left(\frac{m}{n}, 1\right)$ é o ponto de interseção das retas s e t. Portanto, como as retas s e t são construtíveis, segue que o ponto $(r,1)$ é construtível. □

Com o resultado acima, é possível finalmente se concretizar o objetivo desta seção, que é mostrar que todos os pontos de coordenadas racionais são construtíveis.

Teorema 1. Se $r,s \in \mathbb{Q}$, então o ponto (r,s) é construtível.

Demonstração. Sejam r e s números racionais quaisquer. Pelo lema 2, os pontos $(r,1)$ e $(s,1)$ são construtíveis. Se $s = 0$, basta traçar a reta construtível paralela ao eixo y que passa $(r,1)$; a

reta traçada intersecta o eixo x no ponto $(r,0)$, que é, portanto, um ponto construtível. Suponha então que $s \neq 0$. Traçando a reta construtível t paralela ao eixo y que passa por $(s,1)$ e tomando a interseção entre t e o eixo x, obtém-se o ponto construtível $S \doteq (s,0)$. Trace então a circunferência construtível $\mathscr{C}$ de centro $(0,0)$ e raio $OS = |s|$. Deste modo, o ponto $(0,s)$ é uma das interseções entre $\mathscr{C}$ e o eixo y e, portanto, $(0,s)$ é um ponto construtível. Essas construções estão ilustradas na figura 5.

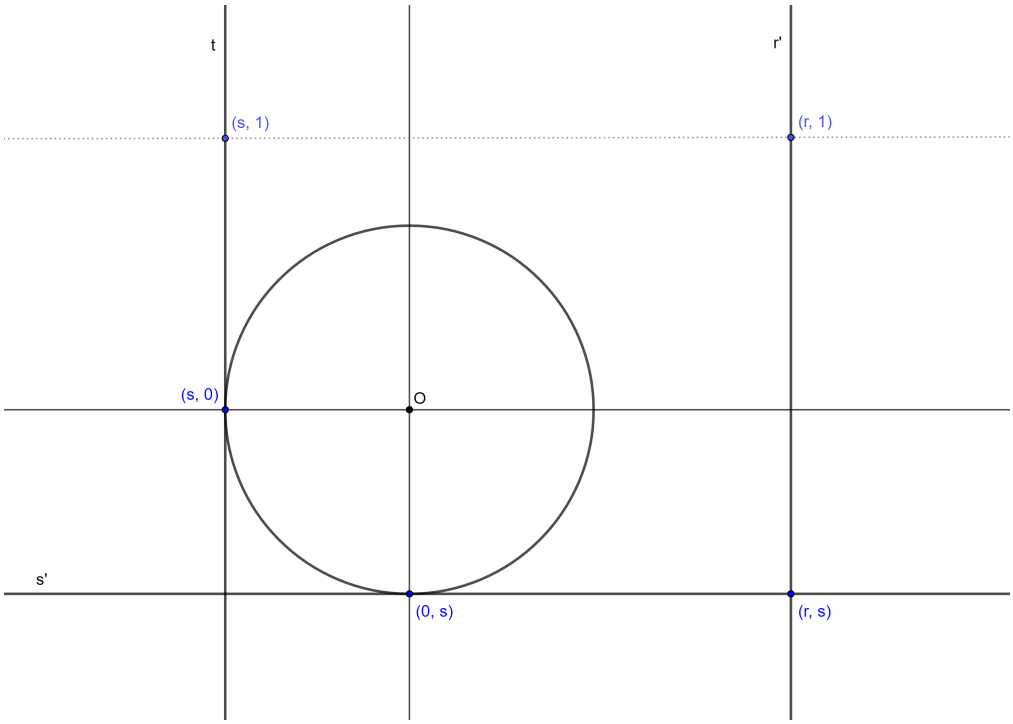


Figura 5 – Pontos construtíveis da forma (r,s), $r,s \in \mathbb{Q}$.

Agora basta traçar a reta s' paralela ao eixo x que passa por $(0,s)$ e a reta r' paralela ao eixo y que passa por $(r,1)$. Pelo lema 1, as retas r' e s' são construtíveis. O ponto (r,s) é a interseção das retas construtíveis r' e s' e, portanto, é um ponto construtível. □

É importante observar que a recíproca do teorema 1 não é verdadeira: há pontos construtíveis cujas coordenadas não são números racionais. Para obter um contra-exemplo clássico e simples, trace a circunferência construtível $\mathscr{C}$ cujo centro é o ponto construtível $(0,0)$ e cujo raio é a distância entre os pontos construtíveis $(0,0)$ e $(1,1)$. Pelo *Teorema de Pitágoras*, é fácil ver que o raio de $\mathscr{C}$ é $\sqrt{2}$; logo, o ponto $(\sqrt{2},0)$ é uma das interseções entre $\mathscr{C}$ e o eixo x e, portanto, $(\sqrt{2},0)$ é um ponto construtível que não tem coordenadas racionais.

A introdução de um sistema de coordenadas cartesiano no plano euclidiano foi o primeiro passo para se interpretar algebricamente as construções com régua e compasso. E a identificação das coordenadas de alguns pontos construtíveis foi um primeiro passeio para se ganhar famili-

aridade neste novo território, porém com um objetivo específico, que ficará claro na próxima seção.

2.3 Números construtíveis

Uma vez no terreno da geometria analítica, o próximo passo é interpretar as *operações permitidas* algebricamente. Sabe-se já que só é possível gerar novos pontos construtíveis a partir de interseções de retas e circunferências construtíveis. Então surge a pergunta: Como caracterizar algebricamente as retas e circunferências construtíveis? Naturalmente, isso será feito através das equações das retas e circunferências no plano. E será necessário um novo conceito, que é definido a seguir e é a chave da solução dos problemas clássicos de construção, como será visto adiante.

Definição 7 (Número construtível)**.** Um número real será dito *construtível* se for coordenada de algum ponto construtível.

Assim, a busca por coordenadas de *pontos construtíveis* se torna agora uma busca por *números construtíveis*, ou seja, neste momento migra-se do plano da geometria para as estruturas da álgebra. Deste modo, surge uma importante pergunta: *Quais números são construtíveis?* Essa pergunta não será facilmente respondida, porém através de ferramentas algébricas da *teoria de corpos*, será possível respondê-la por completo. Por enquanto, pode-se apenas dar uma resposta parcial através dos resultados obtidos na seção anterior.

Teorema 2. Todos os números racionais são construtíveis.

Demonstração. Seja r um número racional qualquer. Pelo lema 2, o ponto $(r,1)$ é construtível. Portanto, pela definição 7, r é um número construtível. □

Além disso, a partir do estudo realizado até o momento, pode-se obter outro resultado imediato sobre os números construtíveis, que será útil em diversas situações e é apresentado a seguir.

Proposição 4. A distância entre dois pontos construtíveis quaisquer é um número construtível.

Demonstração. Sejam P e Q pontos construtíveis quaisquer. Se $P = Q$, então $PQ = 0$ é um número construtível pelo teorema 2. Se $P \neq Q$, trace a circunferência construtível $\mathscr{C}$ de centro $(0,0)$ e raio PQ. O ponto $(PQ,0)$ é uma das interseções entre $\mathscr{C}$ e o eixo x e, portanto, é um ponto construtível. Segue da definição 7 que PQ é um número construtível. □

Através da proposição anterior, conclui-se facilmente, por exemplo, que $\sqrt{2}$ é um número construtível, pois é a distância entre os pontos construtíveis $(0,0)$ e $(1,1)$ (basta usar o *Teorema de Pitágoras* para calcular a distância).

O estudo dos números construtíveis fornecerá informações essenciais sobre as construções com régua e compasso. Acontece que o conjunto dos números construtíveis tem algumas propriedades muito úteis com relação à adição e à multiplicação usuais de números reais. E isso

será a chave para a aplicação das ferramentas algébricas na resolução dos problemas clássicos de construção. Tais propriedades são apresentadas nos lemas 3 e 4 a seguir.

Lema 3. Seja $a \in \mathbb{R}$ um número construtível qualquer. Então:

(i) os pontos $(|a|,0)$, $(-|a|,0)$, $(0,|a|)$ e $(0,-|a|)$ são construtíveis;

(ii) $|a|$ é um número construtível;

(iii) $-a$ é um número construtível.

Demonstração. Seja $a \in \mathbb{R}$ um número construtível qualquer.

(i) Pela definição 7, a é uma coordenada de algum ponto construtível; então suponha sem perda de generalidade que exista um ponto construtível P tal que a é a abscissa de P, i.e., $P = (a,b)$, para algum $b \in \mathbb{R}$ (se a for a ordenada de algum ponto construtível, o raciocínio é análogo). Trace a reta construtível r paralela ao eixo y que passa pelo ponto P. A interseção entre r e o eixo x é o ponto $Q \doteq (a,0)$, que é portanto construtível. Agora basta traçar a circunferência construtível $\mathscr{C}$ de centro $(0,0)$ e raio $OQ = |a|$. A circunferência $\mathscr{C}$ intersecta o eixo x nos pontos $(|a|,0)$ e $(-|a|,0)$, e intersecta o eixo y nos pontos $(0,|a|)$ e $(0,-|a|)$. Como a circunferência $\mathscr{C}$, o eixo x e o eixo y são construtíveis, segue que as quatro interseções mencionadas são pontos construtíveis.

(ii) Do item (i) acima e da definição 7, é imediato que $|a|$ é um número construtível, pois é uma coordenada do ponto construtível $(|a|,0)$.

(iii) Do item (i), é imediato que $|a|$ e $-|a|$ são números construtíveis, pois são coordenadas de pontos construtíveis. Além disso, como

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

segue que $-a = -|a|$ ou $-a = |a|$. Portanto, $-a$ é um número construtível. □

A proposição a seguir fornece uma *equivalência entre pontos construtíveis* e *números construtíveis*. Sendo assim, tem uma importância teórica grande, que vai muito além da sua aplicação nas demonstrações dos próximos resultados.

Proposição 5. Sejam $a,b \in \mathbb{R}$. Então: a e b são números construtíveis se, e somente se, (a,b) é um ponto construtível.

Demonstração. Sejam a e b números reais quaisquer.

($\Leftarrow$) Suponha que (a,b) é um ponto construtível. Então, pela definição 7, a e b são números construtíveis.

($\Rightarrow$) Reciprocamente, suponha que a e b são números construtíveis. Como $a = |a|$ ou $a = -|a|$, segue do lema 3 que $P \doteq (a,0)$ é um ponto construtível. Analogamente, como $b = |b|$ ou $b = -|b|$, segue que $Q \doteq (0,b)$ é um ponto construtível.

Se $a = 0$ ou $b = 0$, então o ponto (a,b) é igual a Q ou P, respectivamente, e portanto é construtível. Suponha então que $a \neq 0$ e $b \neq 0$. Trace a reta r paralela ao eixo y que passa pelo ponto P e a reta s paralela ao eixo x que passa pelo ponto Q; pela proposição 1, as retas r e s são construtíveis. A interseção de r e s é o ponto (a,b), que é portanto construtível. □

Um fato muito importante é que são números construtíveis a soma, a diferença, o produto e o quociente de números construtíveis. Esse resultado é formalizado através do lema a seguir.

Lema 4. Sejam $a,b \in \mathbb{R}$ números construtíveis quaisquer. Então:

(i) $a+b$ é um número construtível;

(ii) $a-b$ é um número construtível;

(iii) ab é um número construtível;

(iv) $\frac{a}{b}$ é um número construtível, se $b \neq 0$.

Demonstração. Sejam $a,b \in \mathbb{R}$ números construtíveis quaisquer. Pela proposição 5, $P \doteq (a,0)$ e $Q \doteq (b,0)$ são pontos construtíveis.

(i) Se $b = 0$, então $a+b = a$ é construtível. Suponha então que $b \neq 0$. Trace a circunferência construtível $\mathscr{C}$ de centro P e raio $OQ = |b|$. As interseções entre $\mathscr{C}$ e o eixo x são os pontos construtíveis $R \doteq (a+|b|,0)$ e $S \doteq (a-|b|,0)$. Como $b = |b|$ ou $b = -|b|$, segue que $(a+b,0)$ é igual a R ou S e, portanto, é um ponto construtível. Logo, pela definição 7, $a+b$ é um número construtível.

(ii) Como b é construtível, segue do lema 3 que $-b$ é construtível. Logo, como $a-b = a+(-b)$, segue do item (i) acima que $a-b$ é um número construtível.

(iii) Se $a = 0$ ou $b = 0$, então $ab = 0$ é construtível, pelo teorema 2. Suponha então que $a \neq 0$ e $b \neq 0$. A construção descrita a seguir está ilustrada na figura 6.

Trace a circunferência construtível $\mathscr{C}$ de centro $(0,0)$ e raio $OP = |a|$. Trace a reta construtível r que passa pelos pontos construtíveis $(0,0)$ e $(1,1)$. Chame de B o ponto de interseção entre $\mathscr{C}$ e r que está no primeiro quadrante do plano cartesiano. Note que OB é o raio da circunferência $\mathscr{C}$ e, portanto, $OB = |a|$. Além disso, sendo $A = (1,0)$ e $C \doteq (|b|,0)$, trace

a reta construtível s paralela à reta construtível $\overleftrightarrow{AB}$ que passa pelo ponto C, e chame de D a interseção entre r e s. Pelo *Teorema de Tales*, segue que:

$$\frac{OB}{OA} = \frac{OD}{OC} \Rightarrow \frac{|a|}{1} = \frac{OD}{|b|} \Rightarrow OD = |a||b| = |ab|.$$

Como O e D são pontos construtíveis, segue da proposição 4 que $OD = |ab|$ é um número construtível. Pelo lema 3, $-|ab|$ também é um número construtível. Além disso, sabe-se que $ab = |ab|$ ou $ab = -|ab|$. Portanto, ab é um número construtível.

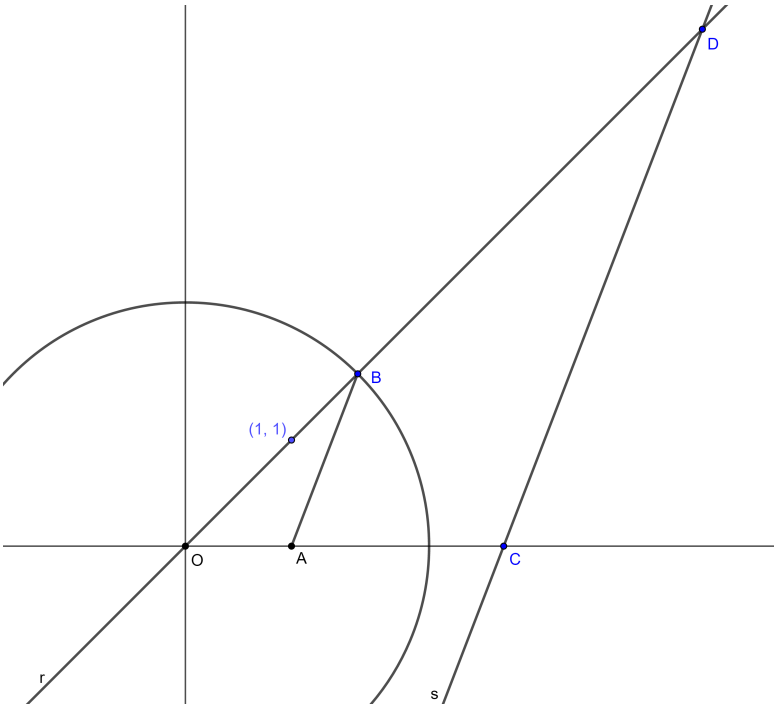


Figura 6 – Construção do número ab.

(iv) Suponha que $b \neq 0$. A construção descrita a seguir está ilustrada na figura 7.

Trace a circunferência construtível $\mathscr{D}$ de centro $(0,0)$ e raio 1. Trace a reta construtível r que passa pelos pontos construtíveis $(0,0)$ e $(1,1)$. Chame de E o ponto de interseção entre $\mathscr{D}$ e r que está no primeiro quadrante do plano cartesiano. Note que OE é o raio da circunferência $\mathscr{D}$ e, portanto, $OE = 1$. Além disso, sendo $A = (1,0)$ e $C = (|b|,0)$, trace a reta construtível t paralela à reta construtível $\overleftrightarrow{EC}$ que passa pelo ponto A, e chame de F o ponto de interseção entre r e t. Pelo *Teorema de Tales*, segue que:

$$\frac{OF}{OA} = \frac{OE}{OC} \Rightarrow \frac{OF}{1} = \frac{1}{|b|} \Rightarrow OF = \frac{1}{|b|}.$$

Como O e F são pontos construtíveis, segue da proposição 4 que $OF = \frac{1}{|b|}$ é um número construtível. Pelo lema 3, $-\frac{1}{|b|}$ também é um número construtível. Além disso, sabe-se que $\frac{1}{b} = \frac{1}{|b|}$ ou $\frac{1}{b} = -\frac{1}{|b|}$. Logo, $\frac{1}{b}$ é um número construtível. Portanto, pelo item (iii) acima, segue que $a \cdot \frac{1}{b} = \frac{a}{b}$ é um número construtível.

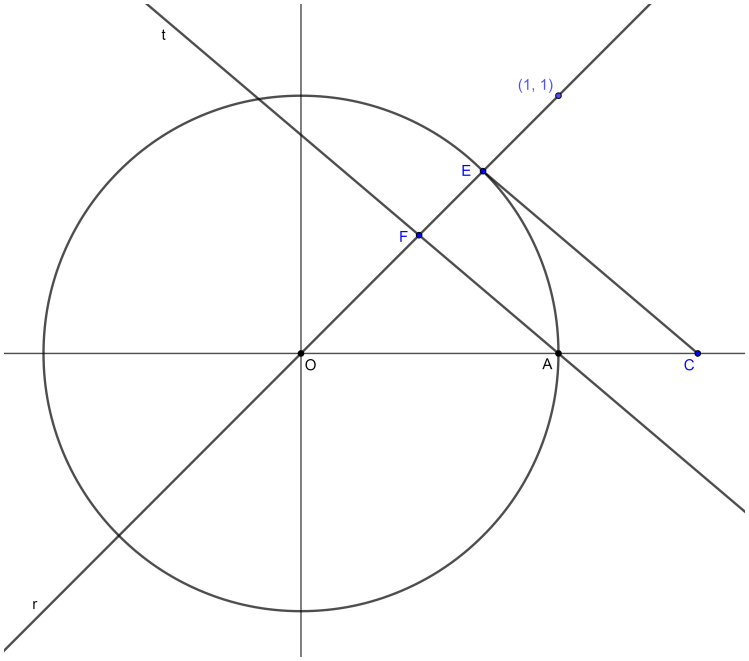


Figura 7 – Construção do número $\frac{1}{b}$.

Assim sendo, conclui-se que as quatro operações básicas entre números construtíveis resultam em números construtíveis, como se queria demonstrar. □

No próximo capítulo será visto que essas propriedades dos números construtíveis terão um papel fundamental, pois caracterizarão o conjunto dos números construtíveis como uma importante estrutura algébrica, que será o coração de todas as aplicações de ferramentas algébricas para a resolução dos problemas clássicos de construção. Por enquanto, tem-se o necessário para se caracterizar algebricamente as retas e circunferências construtíveis, que é o objetivo da próxima e última seção deste capítulo.

2.4 Retas e circunferências construtíveis

A caracterização algébrica das retas construtíveis é fornecida pelo teorema a seguir.

Teorema 3. Para cada reta construtível r não paralela ao eixo y, existe um único par de números construtíveis a e b tais que

$$y = ax + b \tag{2.1}$$

é uma equação de r; e para cada reta construtível r paralela ao eixo y, e também para o próprio eixo y, existe um único número construtível c tal que

$$x = c \tag{2.2}$$

é uma equação de r.

Reciprocamente, dados números construtíveis a, b e c, a equação 2.1 é uma equação de uma única reta construtível não paralela ao eixo y e a equação 2.2 é uma equação de uma única reta construtível paralela ao eixo y ou do próprio eixo y.

Demonstração. Seja r uma reta construtível qualquer.

Suponha que r não é paralela ao eixo y. Da geometria analítica, sabe-se que existem únicos $a, b \in \mathbb{R}$ tais que $y = ax + b$ é uma equação da reta r. Basta então provar que a e b são números construtíveis. A reta r contém pelo menos dois pontos construtíveis, pois é uma reta construtível. Sejam então dois pontos construtíveis distintos $(x_1, y_1), (x_2, y_2) \in r$. Substituindo essas coordenadas na equação da reta, obtém-se o sistema abaixo:

$$\begin{cases} ax_1 + b = y_1 \\ ax_2 + b = y_2 \end{cases}.$$

Subtraindo a primeira equação da segunda, membro a membro, e isolando-se a incógnita a, conclui-se que

$$a = \frac{y_2 - y_1}{x_2 - x_1}.$$

Note que $x_2 - x_1 \neq 0$, pois a reta r não é paralela ao eixo y. Como (x_1, y_1) e (x_2, y_2) são pontos construtíveis, segue da definição 7 que x_1, x_2, y_1 e y_2 são números construtíveis. Portanto, pelo lema 4, a é um número construtível. Como $b = y_1 - ax_1$, segue de modo análogo que b também é um número construtível.

Suponha agora que r é paralela ao eixo y ou é o próprio eixo y. De modo análogo, sabe-se que existe um único $c \in \mathbb{R}$ tal que $x = c$ é uma equação de r. Basta então provar que c é um número construtível. Como a reta r e o eixo x são construtíveis, segue que o ponto de interseção $(c, 0)$ entre elas é um ponto construtível. Portanto, c é um número construtível.

Reciprocamente, sejam $a, b, c \in \mathbb{R}$ números construtíveis quaisquer.

Da geometria analítica, sabe-se que $y = ax + b$ é uma equação de uma única reta r no plano, tal que r não é paralela ao eixo y. Basta então provar que r é uma reta construtível. Para isso, é suficiente mostrar que r contém pelo menos dois pontos construtíveis. Note que $P \doteq (0,b)$ e $Q \doteq (1,a+b)$ são pontos de r. Como a e b são números construtíveis, segue do lema 4 que $a+b$ é um número construtível; portanto, como 0, 1, b e $a+b$ são números construtíveis, segue da proposição 5 que os pontos P e Q são construtíveis.

De modo análogo, também sabe-se que $x = c$ é uma equação de uma única reta r no plano, que é paralela ao eixo y ou é o próprio eixo y. Basta então provar que r é uma reta construtível. Se r é o eixo y, então r é construtível pela proposição 1. Suponha então que r não é o eixo y. Note que $(c,0)$ é um ponto construtível, pela proposição 5, pois c é um número construtível por hipótese. Assim sendo, r é uma reta paralela ao eixo y que passa pelo ponto construtível $(c,0)$. Portanto, pela proposição 1, r é uma reta construtível. □

De modo análogo, a caracterização das circunferências construtíveis é fornecida pelo teorema a seguir.

Teorema 4. Para cada circunferência construtível $\mathscr{C}$, existe uma única equação da forma

$$(x-a)^2 + (y-b)^2 = r^2, \tag{2.3}$$

onde a, b e r são números construtíveis, e $r > 0$.

Reciprocamente, dados números construtíveis a, b e r, com $r > 0$, a equação 2.3 é uma equação de uma única circunferência construtível.

Demonstração. Seja $\mathscr{C}$ uma circunferência construtível qualquer.

Pela definição 5, o centro de $\mathscr{C}$ é um ponto construtível e seu raio é a distância entre dois pontos construtíveis. Chame o centro de $\mathscr{C}$ de (a,b) e seu raio de r, e note que $r > 0$, pois é a distância entre dois pontos. Da geometria analítica, sabe-se que, sendo (x,y) um ponto qualquer de $\mathscr{C}$,

$$(x-a)^2 + (y-b)^2 = r^2 \tag{2.4}$$

é uma equação de $\mathscr{C}$. Como (a,b) é um ponto construtível, segue que a e b são números construtíveis. Além disso, r é um número construtível, pela proposição 4, pois é a distância entre dois pontos construtíveis. A unicidade da equação 2.4 decorre imediatamente da unicidade do centro e do raio da circunferência $\mathscr{C}$.

Reciprocamente, sejam $a,b,r \in \mathbb{R}$ números construtíveis quaisquer tais que $r > 0$.

Da geometria analítica, sabe-se que $(x-a)^2 + (y-b)^2 = r^2$ é uma equação de uma única circunferência de centro (a,b) e raio r. Chame esta circunferência de $\mathscr{C}$.

Como 0, a, b e r são números construtíveis, segue da proposição 5 que (a,b) e $(r,0)$ são pontos construtíveis. Logo, r é a distância entre os pontos construtíveis $(0,0)$ e $(r,0)$. Assim sendo, o centro da circunferência $\mathscr{C}$ é um ponto construtível e o raio de $\mathscr{C}$ é a distância entre dois pontos construtíveis. Portanto, $\mathscr{C}$ é uma circunferência construtível. □

Observação 3. O teorema 3 garante a existência de uma relação entre o conjunto de todas as retas construtíveis e o conjunto de equações lineares da forma

$$Ax + By + C = 0,$$

onde A, B e C são números construtíveis.

Analogamente, o teorema 4 garante a existência de uma relação entre o conjunto de todas as circunferências construtíveis e o conjunto de equações quadráticas da forma

$$(x-a)^2 + (y-b)^2 = r^2,$$

onde a, b e r são números construtíveis, e $r > 0$.

Essas relações constituem um ponto chave para a resolução dos problemas clássicos de construção, pois traduzem o que pode ser feito geometricamente com régua e compasso para a linguagem algébrica.

Pela definição 6, cada *novo ponto construtível* só pode ser obtido a partir de *pontos construtíveis preexistentes* como resultado exclusivo de:

(i) uma interseção entre duas retas construtíveis distintas ou;

(ii) uma interseção entre uma reta construtível e uma circunferência construtível ou;

(iii) uma interseção entre duas circunferências construtíveis distintas.

Portanto, aplicando a caracterização algébrica de retas e circunferências construtíveis feita nesta seção, conclui-se que cada novo ponto construtível corresponde a uma solução de um dos sistemas a seguir.

(i) Um sistema de duas equações lineares da forma

$$\begin{cases} A_1x + B_1y + C_1 = 0 \\ A_2x + B_2y + C_2 = 0 \end{cases},$$

onde A_i, B_i e C_i são números construtíveis, para $i \in \{1,2\}$.

(ii) Um sistema de uma equação linear e uma equação quadrática da forma

$$\begin{cases} Ax+By+C=0 \\ (x-a)^2+(y-b)^2=r^2 \end{cases},$$

onde A, B, C, a, b e r são números construtíveis, e $r>0$.

(iii) Um sistema de duas equações quadráticas da forma

$$\begin{cases} (x-a_1)^2+(y-b_1)^2=r_1^2 \\ (x-a_2)^2+(y-b_2)^2=r_2^2 \end{cases},$$

onde a_i, b_i e r_i são números construtíveis, e $r_i>0$, para $i\in\{1,2\}$.

Ao se resolver os sistemas de equações acima, chega-se em determinadas equações polinomiais, que devem ser resolvidas algebricamente. Deste modo, percebe-se que *obter pontos construtíveis é equivalente a resolver certas equações polinomiais*. Consequentemente, como a proposição 5 fornece uma equivalência entre pontos construtíveis e números construtíveis, deduz-se que *obter números construtíveis também é equivalente a resolver certas equações polinomias*. Essas conclusões são ilustradas no exemplo a seguir.

Exemplo 1. Pelo teorema 2, todos os números racionais são construtíveis. Portanto, o sistema a seguir é um caso particular do sistema apresentado no item (ii) acima.

$$\begin{cases} y=3x+1 \\ (x-2)^2+y^2=9 \end{cases} \tag{2.5}$$

Para resolver o sistema 2.5, pode-se substituir $y=3x+1$ na segunda equação do sistema, o que resulta na equação polinomial

$$(x-2)^2+(3x+1)^2=9,$$

que pode ser reescrita, após expansão dos quadrados e simplificações, como

$$5x^2+x-2=0. \tag{2.6}$$

Assim, é possível ver mais concretamente que encontrar os pontos de interseção da reta e da circunferência construtíveis do sistema 2.5 é equivalente a obter as soluções da equação polinomial 2.6.

Aplicando-se a *fórmula de Bháskara*, é fácil ver que as soluções da equação 2.6 são:

$$x_1=\frac{-1+\sqrt{41}}{10} \text{ e } x_2=\frac{-1-\sqrt{41}}{10}.$$

Como $y = 3x + 1$, os novos pontos construtíveis obtidos a partir do sistema 2.5 são:

$$\left(\frac{-1+\sqrt{41}}{10}, \frac{7+3\sqrt{41}}{10}\right) \text{ e } \left(\frac{-1-\sqrt{41}}{10}, \frac{7-3\sqrt{41}}{10}\right).$$

Consequentemente, as duas abscissas e as duas ordenadas dos pontos acima constituem os novos números construtíveis obtidos a partir do sistema 2.5.

A equivalência entre novos pontos construtíveis e soluções de equações polinomias é de extrema importância, pois significa que cada problema de construção com régua e compasso pode ser transformado em um problema de equações polinomiais, que é um assunto central da álgebra abstrata, a qual possui um ramo muito rico que resolve por completo a questão da resolubilidade de equações por meio de radicais, que é a *Teoria de Galois*. Alguns problemas clássicos de construção podem ser resolvidos com ferramentas básicas da *Teoria de Corpos*, enquanto que outros problemas de construção exigirão ferramentas mais sofisticadas da *Teoria de Galois*. Sabendo disso, não é de se espantar que os gregos antigos não tenham conseguido resolver esses problemas de construção usando somente régua e compasso! Foram necessários séculos de desenvolvimento da matemática para que instrumentos adequados fossem descobertos e assim as soluções pudessem ser finalmente concluídas. No próximo capítulo, serão apresentadas algumas dessas poderosas ferramentas.

CAPÍTULO

3

CARACTERIZAÇÃO DOS NÚMEROS CONSTRUTÍVEIS

Quando foi feita a definição de número construtível no capítulo anterior, surgiu uma pergunta muito importante: *Quais números são construtíveis?* Essa questão foi parcialmente respondida. Basicamente, sabe-se que são construtíveis todos os números racionais e também a soma, a diferença, o produto e o quociente de números construtíveis. Porém, o conceito de número construtível ainda parece uma ideia muito abstrata. Restam perguntas em aberto. *Quais são todos os números construtíveis? Como saber se um dado número real é ou não um número construtível? Como pode-se representar um número construtível qualquer?* Esses questionamentos indicam a necessidade de uma caracterização mais concreta do conjunto dos números construtíveis.

No final do capítulo anterior, foi visto como se obtém algebricamente os pontos construtíveis e, por consequência, os números construtíveis. Essa interpretação algébrica será a chave para se construir uma *caracterização dos números construtíveis*, que é o objetivo deste capítulo, e constituirá o resutado mais importante deste trabalho. Para iniciar essa construção são necessários alguns conceitos de álgebra abstrata, que serão introduzidos na primeira seção deste capítulo.

3.1 Corpo dos números construtíveis

No lema 4 foi mostrado que são números construtíveis a soma, a diferença, o produto e o quociente de números construtíveis. Após um pouco de reflexão, pode-se perceber que o mesmo vale para o conjunto dos números racionais: a soma de dois números racionais é um número racional, assim como a diferença, o produto e o quociente de racionais. Esse fato pode ser generalizado através de uma estrutura algébrica, e o objetivo dessa generalização é facilitar o estudo da estrutura formada pelos números construtíveis. De forma generalizada, fica mais fácil fazer manipulações com números construtíveis e também pode-se deduzir propriedades desses

números através de resultados já conhecidos sobre essa estrutura algébrica.

Na escola, os alunos estão acostumados a trabalhar com as operações de adição, subtração, multiplicação e divisão no conjunto dos números reais. Um conjunto que tem essas quatro operações e as propriedades das mesmas como em $\mathbb{R}$ é chamado de *corpo*. Ou seja, pode-se pensar em um *corpo* como uma estrutura parecida com a do conjunto dos números reais com as quatro operações básicas. Esse é um jeito simplificado de pensar que ajuda a entender melhor a definição formal de *corpo* apresentada a seguir, desde que se observe que a *subtração* é na realidade a "adição do oposto" e a *divisão* é no fundo a "multiplicação pelo inverso". Por exemplo,

$$5-2=5+(-2) \quad \text{e} \quad 3\div 4=3\cdot\frac{1}{4}.$$

Ou seja, pode-se pensar que há apenas duas operações básicas entre números reais, a *adição* e a *multiplicação*. Este é o modo como os matemáticos veem as operações básicas com números reais e, apesar de poder parecer um pouco complicado no início, este modo de trabalhar com as operações em $\mathbb{R}$ facilita o estudo da teoria.

Definição 8. Um corpo $(F,+,\cdot)$ é um conjunto não vazio F dotado de duas operações $+$ e $\cdot$, chamadas de *adição* e *multiplicação*, respectivamente, que satisfazem as propriedades a seguir, onde a, b e c são elementos quaisquer de F.

1. $a+b\in F$ (fechamento da adição);
2. $a+(b+c)=(a+b)+c$ (associatividade da adição);
3. Existe um elemento $0\in F$ tal que $a+0=a$ (elemento neutro da adição);
4. Para cada a em F, existe um elemento $-a$ em F tal que $a+(-a)=0$ (elemento inverso da adição);
5. $a+b=b+a$ (comutatividade da adição);
6. $a\cdot b\in F$ (fechamento da multiplicação);
7. $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (associatividade da multiplicação);
8. Existe um elemento $1\in F$ tal que $a\cdot 1=a$ (elemento neutro da multiplicação);
9. Para cada $a\neq 0$ em F, existe um elemento $\dfrac{1}{a}$ em F tal que $a\cdot\dfrac{1}{a}=1$ (elemento inverso da multiplicação);
10. $a\cdot b=b\cdot a$ (comutatividade da multiplicação);
11. $a\cdot(b+c)=a\cdot b+a\cdot c$ (distributividade da multiplicação com relação à adição).

O elemento inverso da multiplicação também é comumente denotado por a^{-1}.

Note também que é usada a notação $(F,+,\cdot)$ para um corpo, porque o mesmo é formado por um conjunto e duas operações, e não apenas um conjunto F. Porém, para facilitar a escrita, é comum se referir ao corpo $(F,+,\cdot)$ simplesmente por F.

Além disso, também por abreviação, muitas vezes se escreve ab ao invés de $a \cdot b$.

Exemplo 2. Naturalmente, o conjunto dos números reais $\mathbb{R}$, juntamente com as operações usuais de adição e multiplicação, é um corpo, que pode ser denotado por $(\mathbb{R},+,\cdot)$ ou simplesmente $\mathbb{R}$. Outro exemplo muito frequente de corpo é $(\mathbb{Q},+,\cdot)$, formado pelo conjunto dos números racionais e pelas operações usuais dos números reais. De fato, é fácil verificar que $\mathbb{Q}$ tem todas as propriedades de corpo. Lembre-se que

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a,b \in \mathbb{Z}, b \neq 0 \right\}.$$

Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais quaisquer, isto é, $a,b,c,d \in \mathbb{Z}$, $b \neq 0$ e $d \neq 0$. Então:

1. Os números $ad+bc$ e bd são inteiros e $bd \neq 0$. Portanto, segue que
$$\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd} \in \mathbb{Q}.$$
2. A associatividade da adição em $\mathbb{Q}$ pode ser deduzida diretamente da associatividade da adição em $\mathbb{R}$, pois todos os números racionais são números reais.
3. Existe um número $0 = \frac{0}{1}$ em $\mathbb{Q}$ tal que
$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}.$$
4. Para cada $\frac{a}{b}$ em $\mathbb{Q}$, existe um elemento $-\frac{a}{b} = \frac{(-a)}{b}$ em $\mathbb{Q}$ tal que
$$\frac{a}{b} + \frac{(-a)}{b} = \frac{a+(-a)}{b} = \frac{0}{b} = 0.$$
5. A comutatividade da adição em $\mathbb{Q}$ pode ser deduzida diretamente da comutatividade da adição em $\mathbb{R}$, pois todos os números racionais são números reais.
6. Os números ac e bd são inteiros e $bd \neq 0$. Portanto, segue que
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}.$$
7. A associatividade da multiplicação em $\mathbb{Q}$ pode ser deduzida diretamente da associatividade da multiplicação em $\mathbb{R}$.

8. Existe um número $1 = \frac{1}{1}$ em $\mathbb{Q}$ tal que
$$\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}.$$

9. Para cada $\frac{a}{b} \neq 0$ em $\mathbb{Q}$, existe um elemento $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ em $\mathbb{Q}$ tal que
$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = 1.$$

10. A comutatividade da multiplicação em $\mathbb{Q}$ pode ser deduzida diretamente da comutatividade da multiplicação em $\mathbb{R}$.

11. A propriedade distributiva em $\mathbb{Q}$ também pode ser deduzida diretamente da propriedade distributiva em $\mathbb{R}$.

Portanto, pelas propriedades acima, segue da definição 8 que $\mathbb{Q}$ é um corpo.

Observa-se que $\mathbb{Q} \subset \mathbb{R}$ e, além disso, $(\mathbb{Q}, +, \cdot)$ é um corpo com as mesmas operações de $(\mathbb{R}, +, \cdot)$. Isso confere uma relação especial entre os dois corpos. Uma vez que $\mathbb{R}$ é um corpo, a adição e a multiplicação em $\mathbb{Q}$ "herdam" a associatividade, a comutatividade e a distributividade das operações em $\mathbb{R}$, como já foi observado acima, porém há ainda outras propriedades que também são herdadas e não precisariam ter sido feitas para mostrar que $\mathbb{Q}$ é um corpo. Por exemplo, na propriedade 8, bastaria provar que $1 \in \mathbb{Q}$, pois o fato de que $r \cdot 1 = r$, para todo racional r, decorre imediatamente do fato de que $r \in \mathbb{R}$ e não exige, portanto, uma nova demonstração. Essa relação especial entre os corpos $\mathbb{Q}$ e $\mathbb{R}$ é formalizada através dos conceitos de *subcorpo* e *extensão de corpo*.

Definição 9. Seja F um corpo. Se $K \subseteq F$ é um corpo com as mesmas operações de adição e multiplicação de F, então se diz que K é um *subcorpo* de F e que F é uma *extensão de corpo* de K.

Assim, pode-se dizer então que $\mathbb{Q}$ é um *subcorpo* de $\mathbb{R}$ ou ainda que $\mathbb{R}$ é uma *extensão de corpo* de $\mathbb{Q}$. Partindo do conhecimento de que $\mathbb{R}$ é corpo, fica mais fácil mostrar que $\mathbb{Q}$ é corpo através da demonstração de que $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$. Na proposição a seguir, é traduzido formalmente o fato de que muitas propriedades são herdadas do "corpo maior" e que é necessário provar um mínimo de condições para garantir que um subconjunto de um dado corpo é um subcorpo.

Proposição 6. Sejam $(F, +, \cdot)$ um corpo e $K \neq \emptyset$ um subconjunto de F. Então K é um subcorpo de F se, e somente se, valem as afirmações a seguir:

(i) se $a, b \in K$, então $a + b \in K$;

(ii) se $a \in K$, então $-a \in K$;

(iii) se $a, b \in K$, então $ab \in K$;

(iv) $1 \in K$;

(v) se $a \in K$ e $a \neq 0$, então $a^{-1} \in K$.

Demonstração. É claro que, se K é um subcorpo de F, então K é um corpo e, portanto, é trivial que valem as condições de (i) a (v), pois são algumas das propriedades de um corpo. O resultado importante é que basta as cinco condições acima para garantir que K é um subcorpo de F. Suponha então que o subconjunto não vazio K de F, juntamente com as operações de adição e multiplicação de F, satisfaçam as condições de (i) a (v) acima. Será mostrado a seguir que valem todas as propriedades da definição 8. Sejam a, b e c elementos quaisquer de K.

1. $a+b \in K$, pela hipótese (i).

2. $a+(b+c) = (a+b)+c$, pois $a, b, c \in F$, que é um corpo.

3. Existe um elemento $0 \in F$ tal que $a+0 = a$, pois F é um corpo e $a \in F$. Pela hipótese (ii), $-a \in K$. Logo, por (i), segue que $0 = a+(-a) \in K$. Portanto, existe um elemento $0 \in K$ tal que $a+0 = a$.

4. Para cada a em K, existe um elemento $-a$ em F tal que $a+(-a) = 0$, pois F é corpo e $a \in F$. Pela hipótese (ii), $-a \in K$. Portanto, para cada a em K, existe um elemento $-a \in K$ tal que $a+(-a) = 0$.

5. $a+b = b+a$, pois $a, b \in F$, que é um corpo.

6. $a \cdot b \in K$, pela hipótese (iii).

7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, pois $a, b, c \in F$, que é um corpo.

8. Existe um elemento $1 \in F$ tal que $a \cdot 1 = a$, pois F é corpo e $a \in F$. Pela hipótese (iv), $1 \in K$. Portanto, existe um elemento $1 \in K$ tal que $a \cdot 1 = a$.

9. Para cada a em K, existe um elemento a^{-1} em F tal que $a \cdot a^{-1} = 1$, pois F é corpo e $a \in F$. Pela hipótese (v), $a^{-1} \in K$. Portanto, para cada a em K, existe um elemento a^{-1} em K tal que $a \cdot a^{-1} = 1$.

10. $a \cdot b = b \cdot a$, pois $a, b \in F$, que é um corpo.

11. $a \cdot (b+c) = a \cdot b + a \cdot c$, pois $a, b, c \in F$, que é um corpo.

Logo, pela definição 8, segue das propriedades acima que K é um corpo com as mesmas operações de F. Portanto, como $K \subseteq F$, segue da definição 9 que K é um subcorpo de F.

□

Com esses conceitos da álgebra abstrata, já é possível iniciar a caracterização dos números construtíveis. É uma consequência imediata dos lemas 3 e 4 que o conjunto de todos os números contrutíveis juntamente com as operações usuais de adição e multiplicação em $\mathbb{R}$ formam um corpo. Essa conclusão é formalizada através do teorema a seguir.

Teorema 5. Seja E o conjunto de todos os números construtíveis. Então E, juntamente com as operações usuais dos números reais, é um subcorpo de $\mathbb{R}$.

Demonstração. Pela definição 7 de número construtível, tem-se que $E \subseteq \mathbb{R}$. Assim, basta provar que valem as condições da proposição 6 para as operações usuais dos reais em E. As propriedades (i), (ii), (iii) e (v) seguem imediatamente dos lemas 3 e 4. E do teorema 2, segue que $1 \in E$, pois 1 é um número racional.

Portanto, pela proposição 6, segue que E é um subcorpo de $\mathbb{R}$. □

Tem-se então que E é um corpo. Mais do que isso: E é uma extensão de corpo de $\mathbb{Q}$, pois, como foi visto no capítulo anterior, todos os números racionais são construtíveis. Essa afirmação é formalizada através do corolário a seguir. Vale ressaltar que, a partir de agora, E é a notação do corpo dos números construtíveis.

Corolário 1. O corpo E dos números construtíveis é uma extensão de corpo de $\mathbb{Q}$.

Demonstração. Pelo teorema 2, todos os números racionais são construtíveis, i.e., $\mathbb{Q} \subseteq E$. Portanto, E é uma extensão de corpo de $\mathbb{Q}$, com as operações usuais de $\mathbb{R}$. □

Talvez seja interessante observar que é conhecido, da teoria de álgebra abstrata, que todo subcorpo de $\mathbb{R}$ contém $\mathbb{Q}$, o que mostra que $\mathbb{Q}$ é o "menor" corpo contido em $\mathbb{R}$. Então, deste resultado de estruturas algébricas seguiria direto que $\mathbb{Q} \subseteq E$. O caminho aqui utilizado para se chegar em $\mathbb{Q} \subseteq E$ foi mais construtivo e não passou pelo resultado mais teórico, dispensando assim a necessidade de abordá-lo e prová-lo detalhadamente.

Entender que E é uma extensão de corpo de $\mathbb{Q}$ é o primeiro passo na direção de uma caracterização de E. Ainda soa como algo muito abstrato falar do corpo E de números construtíveis, porém, apesar de não se ter concretamente os elementos de E, já se sabe como esses elementos se comportam com relação às operações de adição e multiplicação. Na seção seguinte, serão dados novos passos em direção à caracterização de E.

3.2 Extensões quadráticas do corpo de números racionais

No capítulo anterior, foi provado que a distância entre dois pontos construtíveis é um número construtível e, como exemplo dessa propriedade, foi visto que $\sqrt{2}$ é um número construtível, ou seja, $\sqrt{2} \in E$. Como E é uma extensão de corpo de $\mathbb{Q}$, tem-se, por exemplo, que os números $7-5\sqrt{2}$ e $-11+\sqrt{2}$ são números contrutíveis (pois estão no corpo as somas e os produtos de elementos do corpo). Mais geralmente, se a e b são números racionais, então qualquer número da forma $a+b\sqrt{2}$ é um número construtível, pois E é corpo e $a, b, \sqrt{2} \in E$. O conjunto dos números da forma $a+b\sqrt{2}$ é um importante exemplo de subconjunto de E. Como já era de se esperar, juntamente com as operações usuais dos números reais, esse conjunto é um subcorpo de E. E novamente tem-se mais: o corpo dos números da forma $a+b\sqrt{2}$, $a,b \in \mathbb{Q}$, é claramente uma extensão de corpo de $\mathbb{Q}$, pois todo número racional é da forma $a+0\cdot\sqrt{2}$. Essas afirmações serão formalizadas através da proposição a seguir.

Proposição 7. Considere o seguinte conjunto:

$$\mathbb{Q}(\sqrt{2}) \doteq \left\{ a+b\sqrt{2} \;\middle|\; a,b \in \mathbb{Q} \right\}.$$

Então $\mathbb{Q}(\sqrt{2})$, juntamente com as operações usuais de adição e multiplicação em $\mathbb{R}$, é uma extensão de corpo de $\mathbb{Q}$.

Demonstração. É claro que $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$; então primeiramente será provado que $\mathbb{Q}(\sqrt{2})$ é um subcorpo de $\mathbb{R}$ e para isso basta mostrar que valem as condições da proposição 6. Sejam $u, v \in \mathbb{Q}(\sqrt{2})$ elementos arbitrários, i.e., $u = a+b\sqrt{2}$ e $v = c+d\sqrt{2}$, onde $a,b,c,d \in \mathbb{Q}$.

(i) $u+v = (a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$. Como $\mathbb{Q}$ é corpo, tem-se que $a+c, b+d \in \mathbb{Q}$. Portanto, $u+v \in \mathbb{Q}(\sqrt{2})$.

(ii) $-u = -(a+b\sqrt{2}) = (-a)+(-b)\sqrt{2}$. Como $\mathbb{Q}$ é subcorpo de $\mathbb{R}$, tem-se que $-a, -b \in \mathbb{Q}$. Portanto, $-u \in \mathbb{Q}(\sqrt{2})$.

(iii) $uv = (a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$. Como $\mathbb{Q}$ é corpo, tem-se que $ac+2bd, ad+bc \in \mathbb{Q}$. Portanto, $uv \in \mathbb{Q}(\sqrt{2})$.

(iv) Note que $1 = 1+0\cdot\sqrt{2}$. Como $0, 1 \in \mathbb{Q}$, segue que $1 \in \mathbb{Q}(\sqrt{2})$.

(v) Se $u \neq 0$, então a e b não são ambos nulos. Logo, $a-b\sqrt{2} \neq 0$ (se $a = b\sqrt{2}$, então $a = b = 0$, pois $\sqrt{2} \notin \mathbb{Q}$). Assim,

$$u^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2},$$

o que pode ser reescrito como:

$$u^{-1} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}.$$

Portanto, $u^{-1} \in \mathbb{Q}(\sqrt{2})$, pois, como $\mathbb{Q}$ é corpo, tem-se que

$$\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}.$$

Note que $a^2-2b^2 \neq 0$, pois caso contrário, supondo $b \neq 0$, ocorreria:

$$a^2 = 2b^2 \;\Rightarrow\; \frac{a^2}{b^2} = 2 \;\Rightarrow\; \frac{a}{b} = \pm\sqrt{2},$$

o que seria um absurdo, pois $\sqrt{2}$ é irracional. Note que, se fosse $b = 0$ e $a \neq 0$, bastaria fazer um processo análogo e deduzir que

$$\frac{b}{a} = \pm\frac{1}{\sqrt{2}} = \pm\frac{\sqrt{2}}{2},$$

e então a conclusão seria a mesma.

Pela proposição 6, segue das propriedades de (i) a (v) acima que $\mathbb{Q}(\sqrt{2})$ é um subcorpo de $\mathbb{R}$. Além disso, é direto que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, pois $r = r + 0 \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, para todo número racional r. Portanto, $\mathbb{Q}(\sqrt{2})$ é uma extensão de corpo de $\mathbb{Q}$. □

Deste modo, tem-se agora uma extensão de corpo de $\mathbb{Q}$, mais concreta do que E, onde todos os números são construtíveis. É claro que nem todos os números construtíveis estão em $\mathbb{Q}(\sqrt{2})$, porém ter uma extensão assim, onde se sabe como são todos os números, já é um avanço importante.

Uma vez que se sabe que $\sqrt{2}$ é um número construtível, pode-se mostrar facilmente que $\sqrt{3}$ também é um número construtível, pois é a distância entre os pontos construtíveis $(0,0)$ e $(\sqrt{2},1)$ (basta usar o *Teorema de Pitágoras* para calcular a distância). De modo análogo, pode-se mostrar que $\sqrt{4}$ é um número construtível calculando a distância entre $(0,0)$ e $(\sqrt{3},1)$. É claro que no caso de $\sqrt{4} = 2$ não seria necessário este procedimento, porém, incluindo este caso, fica mais fácil visualizar como esse processo pode ser repetido indefinidamente. Assim fica claro que todas as raízes quadradas de números naturais são números construtíveis. E do mesmo modo que foi obtida a extensão de corpo $\mathbb{Q}(\sqrt{2})$, pode-se obter várias outras, como por exemplo $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{5})$, onde todos os números são construtíveis. Extensões desse tipo desempenharão um papel central na caracterização dos números construtíveis.

Mais geralmente, se $x \in \mathbb{Q}$ é tal que $x > 0$ e $\sqrt{x} \notin \mathbb{Q}$, então o conjunto

$$\mathbb{Q}(\sqrt{x}) = \left\{ a + b\sqrt{x} \;\middle|\; a,b \in \mathbb{Q} \right\},$$

juntamente com as operações usuais de $\mathbb{R}$, é uma extensão de corpo de $\mathbb{Q}$. A demonstração desta afirmação é análoga à demonstração feita para $\mathbb{Q}(\sqrt{2})$, bastando trocar 2 por x. Porém, ao invés de se fazer essa demonstração, será provado um resultado mais geral, cuja necessidade ficará clara na próxima seção e cuja prova também é análoga à que foi feita para $\mathbb{Q}(\sqrt{2})$.

Teorema 6. Sejam F um subcorpo de $\mathbb{R}$ arbitrário e $x \in F$ tal que $x > 0$ e $\sqrt{x} \notin F$. Então

$$F(\sqrt{x}) \doteq \left\{ a + b\sqrt{x} \;\middle|\; a, b \in F \right\},$$

juntamente com as operações usuais dos números reais, é uma extensão de corpo de F.

Demonstração. Note que $\sqrt{x} \in \mathbb{R}$, pois $x > 0$. Logo, se $a, b \in F \subseteq \mathbb{R}$, então $a + b\sqrt{x} \in \mathbb{R}$, pois $\mathbb{R}$ é corpo. Assim, fica claro que $F(\sqrt{x}) \subseteq \mathbb{R}$. Então primeiramente será provado que $F(\sqrt{x})$ é um subcorpo de $\mathbb{R}$ e para isso basta mostrar que valem as condições de (i) a (v) da proposição 6. Sejam $u, v \in F(\sqrt{x})$ elementos arbitrários, i.e., $u = a + b\sqrt{x}$ e $v = c + d\sqrt{x}$, onde $a, b, c, d \in F$.

(i) $u + v = (a + b\sqrt{x}) + (c + d\sqrt{x}) = (a + c) + (b + d)\sqrt{x}$. Como F é corpo, tem-se que $a + c, b + d \in F$. Portanto, $u + v \in F(\sqrt{x})$.

(ii) $-u = -(a + b\sqrt{x}) = (-a) + (-b)\sqrt{x}$. Como F é subcorpo de $\mathbb{R}$, tem-se que $-a, -b \in F$. Portanto, $-u \in F(\sqrt{x})$.

(iii) $uv = (a + b\sqrt{x})(c + d\sqrt{x}) = (ac + xbd) + (ad + bc)\sqrt{x}$. Como F é corpo, tem-se que $ac + xbd, ad + bc \in F$. Portanto, $uv \in F(\sqrt{x})$.

(iv) Note que $1 = 1 + 0 \cdot \sqrt{x}$ e que $0, 1 \in F$, pois F é subcorpo de $\mathbb{R}$. Portanto, $1 \in F(\sqrt{x})$.

(v) Se $u \neq 0$, então a e b não são ambos nulos. Logo, $a - b\sqrt{x} \neq 0$ (se $a = b\sqrt{x}$, então $a = b = 0$, pois $\sqrt{x} \notin F$). Assim,

$$u^{-1} = \frac{1}{a + b\sqrt{x}} = \frac{1}{a + b\sqrt{x}} \cdot \frac{a - b\sqrt{x}}{a - b\sqrt{x}} = \frac{a - b\sqrt{x}}{a^2 - xb^2},$$

o que pode ser reescrito como:

$$u^{-1} = \left(\frac{a}{a^2 - xb^2} \right) + \left(\frac{-b}{a^2 - xb^2} \right) \sqrt{x}.$$

Portanto, $u^{-1} \in F(\sqrt{x})$, pois, como F é corpo, tem-se que

$$\frac{a}{a^2 - xb^2}, \frac{-b}{a^2 - xb^2} \in F.$$

Note que $a^2 - xb^2 \neq 0$, pois caso contrário, supondo $b \neq 0$, ocorreria:

$$a^2 = xb^2 \;\Rightarrow\; \frac{a^2}{b^2} = x \;\Rightarrow\; \frac{a}{b} = \pm\sqrt{x},$$

o que seria um absurdo, pois $\frac{a}{b} \in F$ e $\sqrt{x} \notin F$. Note que, se fosse $b = 0$ e $a \neq 0$, bastaria fazer um processo análogo e deduzir que

$$\frac{b}{a} = \pm\frac{1}{\sqrt{x}} = \pm\frac{\sqrt{x}}{x},$$

e então a conclusão seria a mesma.

Pela proposição 6, segue das propriedades de (i) a (v) acima que $F(\sqrt{x})$ é um subcorpo de $\mathbb{R}$. Além disso, é direto que $F \subseteq F(\sqrt{x})$, pois $a = a + 0 \cdot \sqrt{x} \in F(\sqrt{x})$, para todo número $a \in F$. Portanto, $F(\sqrt{x})$ é uma extensão de corpo de F. □

A formalização de que $\mathbb{Q}(\sqrt{x})$ é uma extensão de corpo de $\mathbb{Q}$ segue imediatamente do teorema acima, e é explicitada no corolário a seguir.

Corolário 2. Seja x um número racional tal que $x > 0$ e $\sqrt{x} \notin \mathbb{Q}$. Então $\mathbb{Q}(\sqrt{x})$, juntamente com as operações usuais em $\mathbb{R}$, é uma extensão de corpo de $\mathbb{Q}$.

Demonstração. Como $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$, segue do teorema 6 que $\mathbb{Q}(\sqrt{x})$, juntamente com as operações usuais dos números reais, é uma extensão de corpo de $\mathbb{Q}$. □

Definição 10. Sejam F um subcorpo de $\mathbb{R}$ arbitrário e $x \in F$ tal que $x > 0$ e $\sqrt{x} \notin F$. Então, a extensão $F(\sqrt{x})$ é chamada de *extensão quadrática de* F.

Se x é um número racional tal que $x > 0$ e $\sqrt{x} \notin \mathbb{Q}$, segue da definição acima que a extensão $\mathbb{Q}(\sqrt{x})$ é chamada de *extensão quadrática de* $\mathbb{Q}$.

As extensões quadráticas de $\mathbb{Q}$ são importantes porque, assim como em $\mathbb{Q}(\sqrt{2})$, todos os números em $\mathbb{Q}(\sqrt{x})$ são construtíveis. Para provar isso, basta mostrar que $\sqrt{x}$ é um número construtível. Porém, ao invés de se fazer uma demonstração apenas para $x \in \mathbb{Q}$, será apresentado um resultado mais geral que, tal qual o teorema 6, terá sua necessidade esclarecida na próxima seção.

Lema 5. Seja $a \in \mathbb{R}$ tal que $a > 0$ e a é um número construtível. Então $\sqrt{a}$ é um número construtível.

Demonstração. Seja $a \in \mathbb{R}$ tal que $a > 0$ e a é um número construtível. Pelo teorema 3, $x = 0$ é uma equação de uma reta construtível r. E pelo teorema 4,

$$\left(x - \frac{a-1}{2}\right)^2 + (y-0)^2 = \left(\frac{a+1}{2}\right)^2 \tag{3.1}$$

é uma equação de uma circunferência construtível $\mathscr{C}$, uma vez que 0, $\frac{a-1}{2}$ e $\frac{a+1}{2}$ são números construtíveis, pois E é um corpo e $a \in E$. Logo, as interseções entre r e $\mathscr{C}$ são pontos construtíveis. Para encontrar essas interseções, basta substituir $x = 0$ na equação 3.1, e isolar a incógnita y:

$$y^2 = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 = \frac{a^2+2a+1}{4} - \frac{a^2-2a+1}{4} = \frac{4a}{4} = a.$$

Assim, $y^2 = a$ e, portanto, $y = \sqrt{a}$ ou $y = -\sqrt{a}$. Ou seja, os pontos de interseção entre r e $\mathscr{C}$ são $(0, \sqrt{a})$ e $(0, -\sqrt{a})$, que são por isso pontos construtíveis. Portanto, $\sqrt{a}$ é um número construtível. □

Assim sendo, se $x \in E$, então $\sqrt{x} \in E$. Logo, se $a, b \in \mathbb{Q} \subseteq E$, então $a + b\sqrt{x} \in E$, pois E é um corpo. Portanto, $\mathbb{Q}(\sqrt{x}) \subseteq E$, ou seja, todo número de $\mathbb{Q}(\sqrt{x})$ é um número construtível. Esse é mais um importante passo em direção à caracterização dos números construtíveis, pois deste modo obtém-se infinitas extensões de corpo de $\mathbb{Q}$ onde todos os números são construtíveis. Porém, as extensões quadráticas do corpo de números racionais ainda não cobrem todos os números construtíveis. E é fácil de provar isso usando o resultado apenas provado. De fato, pelo lema 5 acima, tem-se, por exemplo, que os números

$$\sqrt{\sqrt{2}}, \sqrt{4 - 7\sqrt{3}} \text{ e } \sqrt{1 + \sqrt{1 - \sqrt{5}}}$$

são construtíveis. Por outro lado, estes números não são elementos de extensões quadráticas de $\mathbb{Q}$. Esses são apenas alguns exemplos de números que consistem em resultados de expressões numéricas obtidas de números construtíveis através de repetidas adições, subtrações, multiplicações, divisões e extrações de raízes quadradas. Expressões assim, que envolvem radicais com qualquer índice e as quatro operações básicas, são conhecidas como *expressões radicais*; no caso dos números acima, as expressões possuem apenas radicais com índice 2.

A conclusão então é que todas as expressões radicais formadas apenas por raízes quadradas resultam em números construtíveis, e isso por sua vez constitui um subconjunto bem grande de E. Uma pergunta que surge é: *Será que todos os números construtíveis são resultados de expressões radicais formadas apenas por raízes quadradas?* Como já explicado no capítulo 2, a obtenção de pontos construtíveis é um processo recorrente, ou seja, se inicia com apenas dois pontos construtíveis e a partir deles são construídos novos pontos construtíveis, a partir dos quais são construídos mais pontos construtíveis, e assim por diante. Tendo isso em mente, na próxima seção serão feitas sucessivas construções a partir da situação inicial de dois pontos contrutíveis para se analisar os tipos de números construtíveis que podem aparecer. O que se perceberá é que *sim, todos os números construtíveis que vão aparecendo são de fato resultados de expressões radicais formadas apenas por raízes quadradas*.

3.3 Extensões quadráticas iteradas do corpo de números racionais

Vale ressaltar que em todo início de seção ou capítulo está sendo feita uma tentativa de se introduzir o assunto de modo ilustrado, com exemplos e construções, num esforço de construir explicações que podem ser trabalhadas com alunos no ensino básico, e então as ideias são formalizadas através de resultados e demontrações matemáticos feitos com rigor e de modo detalhado, a fim de que o professor do ensino básico possa compreender com clareza. A formalização não é necessária ao professor do ensino básico que queira aplicar o conteúdo em sala, porém a mesma consiste na justificativa teórica que garante que as afirmações exemplificadas são verdadeiras, além se servir, é claro, ao professor que queira se aprofundar no assunto.

Assim sendo, para iniciar esta seção, serão feitas algumas construções com régua e compasso para se analisar concretamente os "primeiros" números construtíveis que podem ser obtidos a partir dos pontos construtíveis iniciais O e A. O objetivo é que se perceba um padrão nos tipos de números que aparecem através de alguns exemplos.

Como definido no primeiro capítulo, há duas *operações de construção*: traçar uma reta que passa por dois pontos construtíveis; e traçar uma circunferência cujo centro é um ponto construtível e cujo raio é igual à distância entre dois pontos construtíveis. Partindo da situação inicial em que se tem apenas os pontos construtíveis $O = (0,0)$ e $A = (1,0)$ no plano, pode-se pensar do seguinte modo:

0. Se nenhuma operação de construção for efetuada, tem-se apenas dois números construtíveis: 0 e 1, que são os números que aparecem como coordenadas dos pontos construtíveis O e A fornecidos sem nenhuma construção.

1. Se apenas uma operação de construção for realizada, nenhum novo número construtível é obtido. De fato, há três operações possíveis a partir dos pontos O e A: traçar uma reta construtível que passa por O e A; traçar uma circunferência construtível de centro O e raio OA; ou traçar uma circunferência construtível de centro A e raio OA. Ao se fazer apenas uma dessas três operações, não se obtém nenhuma interseção e, portanto, não se obtém nenhuma nova coordenada. Assim, os únicos números construtíveis continuam sendo apenas 0 e 1.

2. Se apenas duas operações de construção forem feitas, novos números construtíveis são obtidos e é possível determinar exatamente que números são esses. Para isso, basta analisar as possibilidades de pares de operações.

    - Pode-se traçar a reta construtível r que passa por O e A, e a circunferência construtível $\mathscr{C}_1$ de centro O e raio OA. Encontrar as interseções entre r e $\mathscr{C}_1$ equivale a resolver o

sistema abaixo.

$$\begin{cases} y = 0 \\ x^2 + y^2 = 1 \end{cases}$$

Substituindo $y = 0$ na segunda equação, obtém-se $x^2 = 1$. Logo, $x = 1$ ou $x = -1$. Portanto, as interseções entre r e $\mathscr{C}_1$ são $(1,0)$ e $(-1,0)$. Deste modo, é obtido um novo ponto construtível: $(-1,0)$.

Obs.: Note que traçar primeiro a reta r e depois a circunferência $\mathscr{C}_1$ é a mesma possibilidade que traçar primeiro a circunferência $\mathscr{C}_1$ e depois a reta r. Ou seja, a ordem em que duas operações são efetuadas não altera as interseções obtidas.

- Pode-se traçar a reta construtível r que passa por O e A, e a circunferência construtível $\mathscr{C}_2$ de centro A e raio OA. Encontrar as interseções entre r e $\mathscr{C}_2$ equivale a resolver o sistema abaixo.

$$\begin{cases} y = 0 \\ (x-1)^2 + y^2 = 1 \end{cases}$$

Substituindo $y = 0$ na segunda equação, obtém-se:

$$(x-1)^2 = 1 \;\Rightarrow\; x^2 - 2x + 1 = 1 \;\Rightarrow\; x(x-2) = 0.$$

Logo, $x = 0$ ou $x = 2$. Portanto, as interseções entre r e $\mathscr{C}_2$ são $(0,0)$ e $(2,0)$. Deste modo, é obtido um novo ponto construtível: $(2,0)$.

- Pode-se traçar a circunferência construtível $\mathscr{C}_1$ de centro O e raio OA, e a circunferência construtível $\mathscr{C}_2$ de centro A e raio OA. Encontrar as interseções entre $\mathscr{C}_1$ e $\mathscr{C}_2$ equivale a resolver o sistema a seguir.

$$\begin{cases} x^2 + y^2 = 1 \\ (x-1)^2 + y^2 = 1 \end{cases}$$

Subtraindo a primeira equação da segunda, membro a membro, obtém-se:

$$(x-1)^2 - x^2 = 0 \;\Rightarrow\; x^2 - 2x + 1 - x^2 = 0 \;\Rightarrow\; 2x = 1 \;\Rightarrow\; x = \frac{1}{2}.$$

Substituindo $x = \frac{1}{2}$ na primeira equação do sistema, obtém-se:

$$\left(\frac{1}{2}\right)^2 + y^2 = 1 \;\Rightarrow\; y^2 = 1 - \frac{1}{4} \;\Rightarrow\; y^2 = \frac{3}{4}.$$

Logo, $y = \frac{\sqrt{3}}{2}$ ou $y = -\frac{\sqrt{3}}{2}$. Portanto, as interseções entre $\mathscr{C}_1$ e $\mathscr{C}_2$ são $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ e $\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$, que por isso são pontos construtíveis.

Assim sendo, todos os novos números construtíveis que podem ser obtidos a partir de duas operações de construção são:

$$-1, 2, \frac{1}{2}, \frac{\sqrt{3}}{2}, -\frac{\sqrt{3}}{2}.$$

3. Se três operações de construção forem feitas, vários novos números construtíveis podem ser obtidos e é possível determinar todos eles, pois trata-se de um número finito de operações com um número finito de pontos construtíveis preexistentes. Porém, neste caso já se tem muitas possibilidades e por isso fica inviável listar todos os novos números construtíveis obtidos. O mesmo vale para o caso de quatro operações de construção efetuadas, e também para cinco operações, e assim por diante.

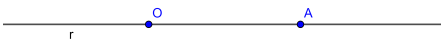
O experimento ainda não está concluído. Por enquanto, dá para notar que todos os números construtíveis que podem ser obtidos através de duas operações ou menos estão contidos em $\mathbb{Q}(\sqrt{3})$, que é uma extensão quadrática de $\mathbb{Q}$. Entretanto, isso ainda não é suficiente para se perceber um padrão. Por outro lado, foi visto que é inviável listar todos os números construtíveis que podem ser obtidos a partir de três ou mais operações de construção.

Uma solução é simplificar o experimento e listar apenas alguns números construtíveis após cada aumento do número de operações. Para isso, será apresentado um exemplo a seguir, no qual uma sequência específica de operações é construída, começando sem nenhuma operação, depois uma, duas, e assim sucessivamente, até seis operações.

Exemplo 3. A construção da sequência de operações será cumulativa, ou seja, cada item acrescenta uma nova operação, sendo que ficam mantidas as operações dos itens anteriores, e isso ficará ainda mais claro com o auxílio de figuras. Vale ressaltar que o objetivo deste exemplo é analisar os números construtíveis obtidos e tentar perceber um padrão que auxilie na compreensão da caracterização desses números. Por isso, após se efetuar cada operação, as interseções serão apresentadas sem a exibição dos cálculos, de modo que o texto não fique muito extenso e não se perca o objetivo no meio de tantos cálculos rotineiros.

0. Sem efetuar nenhuma operação de construção: tem-se apenas os pontos construtíveis iniciais $O = (0,0)$ e $A = (1,0)$. Portanto, os únicos números construtíveis nesta etapa são 0 e 1.

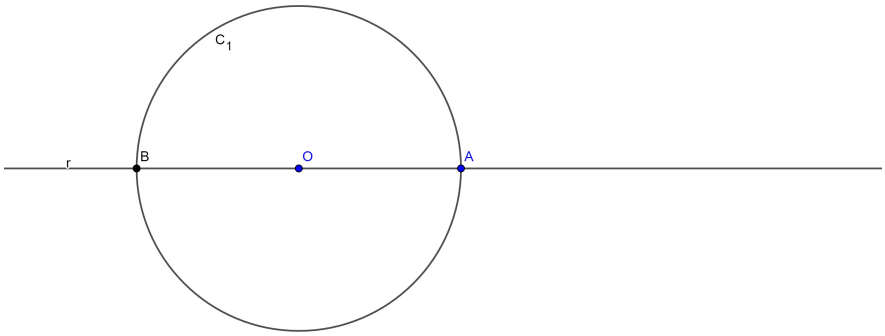
1. Traçar a reta construtível r que passa pelos pontos construtíveis O e A.



Após a primeira operação de construção não há nenhuma interseção e por isso não há nenhum novo ponto construtível. Portanto, nenhum novo número construtível é obtido nesta etapa.

Note que todos os números construtíveis até o final desta etapa são racionais.

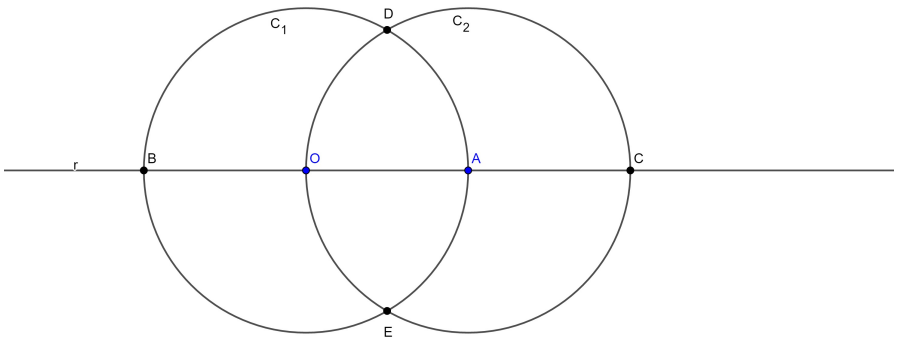
2. Traçar a circunferência construtível $\mathscr{C}_1$ de centro O e raio $OA = 1$.



Após a segunda operação de construção, há interseções entre r e $\mathscr{C}_1$: A e $B \doteq (-1,0)$. Portanto, o único número construtível novo obtido nesta etapa é -1.

Note que todos os números construtíveis obtidos desde a primeira etapa até o final desta etapa são racionais.

3. Traçar a circunferência construtível $\mathscr{C}_2$ de centro A e raio $OA = 1$.



Após a terceira operação de construção, há novos pontos construtíveis.

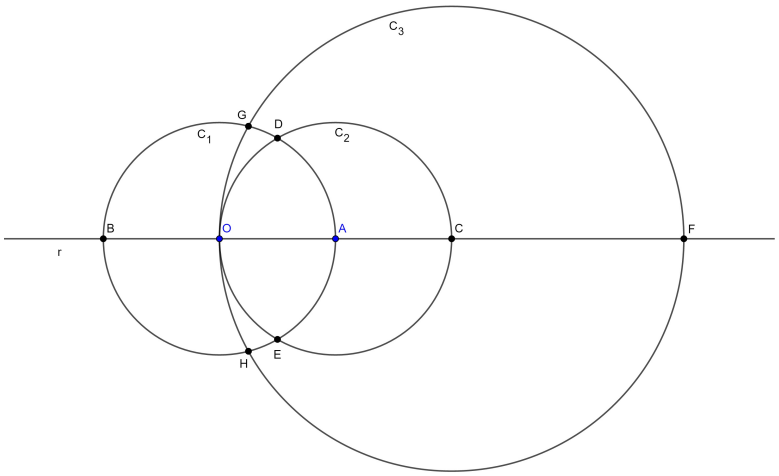
- Interseções entre r e $\mathscr{C}_2$: O e $C \doteq (2,0)$;
- Interseções entre $\mathscr{C}_1$ e $\mathscr{C}_2$: $D \doteq \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ e $E \doteq \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$.

Portanto, os novos números construtíveis obtidos nesta etapa são: 2, $\frac{1}{2}$, $\frac{\sqrt{3}}{2}$ e $-\frac{\sqrt{3}}{2}$.

Note que todos os números construtíveis obtidos desde a primeira etapa até o final desta etapa são da forma

$$a + b\sqrt{3}, \text{ onde } a, b \in \mathbb{Q}.$$

4. Traçar a circunferência construtível $\mathscr{C}_3$ de centro C e raio $OC = 2$.



Após a quarta operação de construção, há novos pontos construtíveis.

- Interseções entre r e $\mathscr{C}_3$: O e $F \doteq (4,0)$;
- Interseções entre $\mathscr{C}_1$ e $\mathscr{C}_3$: $G \doteq \left(\frac{1}{4}, \frac{\sqrt{15}}{4}\right)$ e $H \doteq \left(\frac{1}{4}, -\frac{\sqrt{15}}{4}\right)$.
- Interseção entre $\mathscr{C}_2$ e $\mathscr{C}_3$: O.

Portanto, os novos números construtíveis obtidos nesta etapa são: 4, $\frac{1}{4}$, $\frac{\sqrt{15}}{4}$ e $-\frac{\sqrt{15}}{4}$.

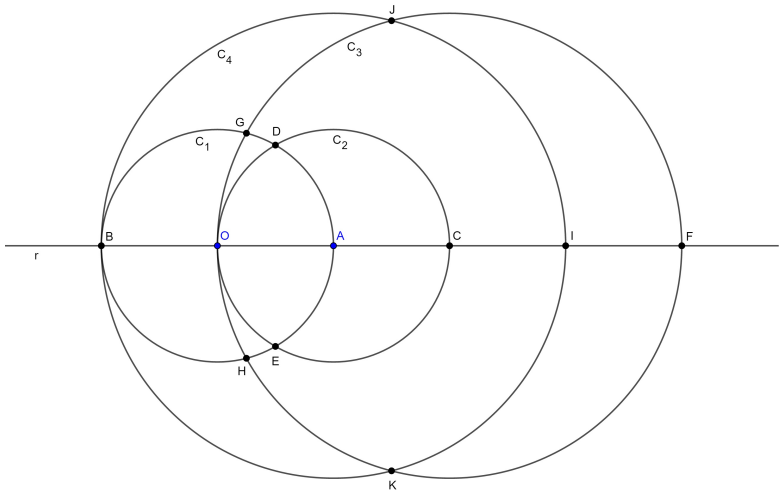
Pode-se reescrever o número $\frac{\sqrt{15}}{4}$ como $\frac{\sqrt{3}}{4} \cdot \sqrt{5}$. Assim sendo, note que todos os números construtíveis obtidos desde a primeira etapa até o final desta etapa são da forma

$$a + b\sqrt{5}, \text{ onde } a, b \in \mathbb{Q}(\sqrt{3}).$$

5. Traçar a circunferência construtível $\mathscr{C}_4$ de centro A e raio $OC = 2$.

Após a quinta operação de construção, há novos pontos construtíveis.

- Interseções entre r e $\mathscr{C}_4$: B e $I \doteq (3,0)$.
- Interseção entre $\mathscr{C}_1$ e $\mathscr{C}_4$: B.
- Interseções entre $\mathscr{C}_3$ e $\mathscr{C}_4$: $J \doteq \left(\frac{3}{2}, \frac{\sqrt{15}}{2}\right)$ e $K \doteq \left(\frac{3}{2}, -\frac{\sqrt{15}}{2}\right)$.



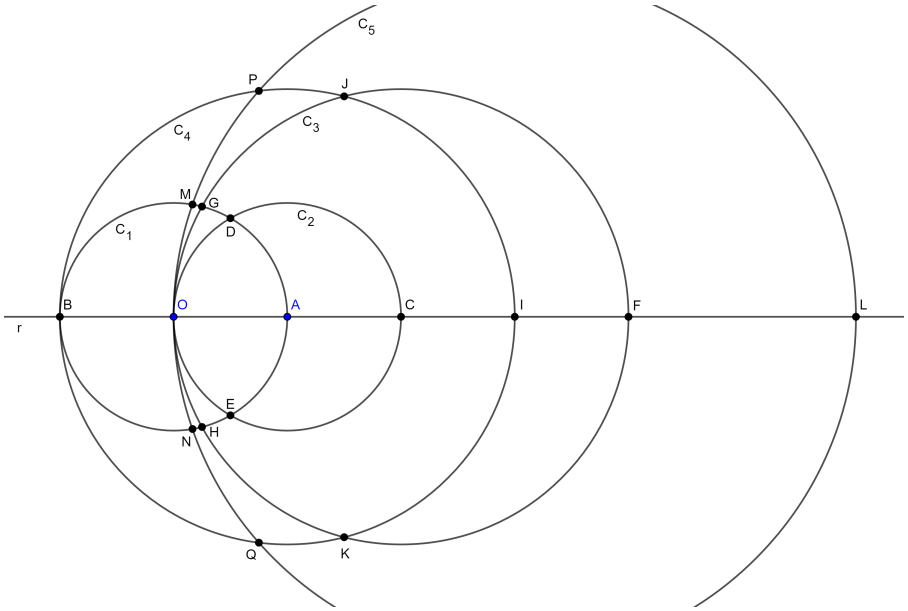
Portanto, os novos números construtíveis obtidos nesta etapa são: 3, $\frac{3}{2}$, $\frac{\sqrt{15}}{2}$ e $-\frac{\sqrt{15}}{2}$.

Uma vez que o número $\frac{\sqrt{15}}{2}$ pode ser reescrito como $\frac{\sqrt{3}}{2}\cdot\sqrt{5}$, todos os números construtíveis obtidos desde a primeira etapa até o final desta etapa são da forma

$$a+b\sqrt{5},\ \text{onde}\ \ a,b\in\mathbb{Q}(\sqrt{3}).$$

Ou seja, observa-se que esta etapa não gerou nenhum "tipo novo de número", num sentido que ficará ainda mais claro com a próxima e última operação de construção deste exemplo.

6. Traçar a circunferência construtível $\mathscr{C}_5$ de centro I e raio $OI=3$.



Após a sexta operação de construção, há novos pontos construtíveis.

- Interseções entre r e $\mathscr{C}_5$: O e $L\doteq(6,0)$.
- Interseções entre $\mathscr{C}_1$ e $\mathscr{C}_5$: $M\doteq\left(\frac{1}{6},\frac{\sqrt{35}}{6}\right)$ e $N\doteq\left(\frac{1}{6},-\frac{\sqrt{35}}{6}\right)$.
- Interseção entre $\mathscr{C}_2$ e $\mathscr{C}_5$: O.
- Interseção entre $\mathscr{C}_3$ e $\mathscr{C}_5$: O.
- Interseções entre $\mathscr{C}_4$ e $\mathscr{C}_5$: $P\doteq\left(\frac{3}{4},\frac{3\sqrt{7}}{4}\right)$ e $Q\doteq\left(\frac{3}{4},-\frac{3\sqrt{7}}{4}\right)$.

Portanto, os novos números construtíveis obtidos nesta etapa são:

$$6,\frac{1}{6},\frac{3}{4},\frac{\sqrt{35}}{6},-\frac{\sqrt{35}}{6},\frac{3\sqrt{7}}{4},-\frac{3\sqrt{7}}{4}.$$

Note que o número $\frac{\sqrt{35}}{6}$ pode ser reescrito como $\frac{\sqrt{5}}{6}\cdot\sqrt{7}$. Assim sendo, todos os números construtíveis obtidos desde a primeira etapa até o final desta etapa são da forma

$$a+b\sqrt{7},$$

onde os números a e b são, por sua vez, da forma $c+d\sqrt{5}$, e $c,d\in\mathbb{Q}(\sqrt{3})$.

Observa-se que, assim como após a terceira e a quarta operações, esta última etapa gerou uma combinação de uma nova raiz quadrada com números da forma de etapas anteriores. E esse é o padrão que se buscava: a cada nova operação de construção, ou se obtém números construtíveis que têm a mesma forma de números construtíveis de operações anteriores ou se obtém números construtíveis que são combinações de uma nova raiz quadrada com números da mesma forma de etapas anteriores.

Observação 4. A sequência escolhida pode não parecer arbitrária: alguém poderia dizer que ela foi escolhida de propósito para fornecer os resultados desejados. De fato, a sequência foi escolhida de modo a facilitar os cálculos e o entendimento do experimento, porém ela pode ser considerada sim como representativa de uma sequência arbitrária de operações, como será provado até o final deste capítulo. Além disso, vale ressaltar que, para se calcular as interseções fornecidas acima, basta escrever o sistema correspondente a cada par de operações e então resolver o mesmo, tal como foi feito no início desta seção.

Através dos experimentos anteriores e do lema 5, é possível se convencer de que ser um número construtível é sinônimo de ser o resultado de uma expressão com radicais envolvendo somente raízes quadradas, ou seja, um número como, por exemplo:

$$\sqrt{2},\ 5+\sqrt{3},\ 3\sqrt{\frac{1}{2}+\frac{7}{9}\sqrt{11}},\ \sqrt{5\sqrt{5}+\frac{9}{8}\sqrt{\sqrt{7}}},\ \text{etc.}$$

O lema e os experimentos estão longe de provar essa correspondência, porém podem convencer o aluno dessa relação, que é verdadeira e será provada na última seção deste capítulo. Pode-se explicar a um aluno que todos os números construtíveis são resultados de expressões radicais formadas somente por raízes quadradas e, reciprocamente, todos essas expressões radicais com raízes quadradas resultam em números construtíveis. Essa é a caracterização dos números construtíveis que se tinha por objetivo: a partir de agora, número construtível se torna sinônimo de *expressão com radicais de índice 2*, como os exemplos acima. O próximo passo é formalizar todas essas ideias e apresentar com rigor a caracterização dos números construtíveis. Será um processo um tanto longo, por isso é importante manter em mente os exemplos concretos de números construtíveis.

As estruturas algébricas que estão por trás da caracterização dos números construtíveis são cadeias de extensões de corpos. Para começar, seja $x_1 \in \mathbb{Q}$ tal que $x_1 > 0$ e $\sqrt{x_1} \notin \mathbb{Q}$. Então:

$$\mathbb{Q}(\sqrt{x_1}) = \left\{ a + b\sqrt{x_1} \;\middle|\; a,b \in \mathbb{Q} \right\},$$

juntamente com as operações usuais em $\mathbb{R}$, é uma extensão de corpo de $\mathbb{Q}$, pelo corolário 2.

Agora seja $x_2 \in \mathbb{Q}(\sqrt{x_1})$ tal que $x_2 > 0$ e $\sqrt{x_2} \notin \mathbb{Q}(\sqrt{x_1})$. Então:

$$\mathbb{Q}(\sqrt{x_1}, \sqrt{x_2}) \doteq \left\{ a + b\sqrt{x_2} \;\middle|\; a, b \in \mathbb{Q}(\sqrt{x_1}) \right\},$$

juntamente com as operações usuais dos reais, é uma extensão de corpo de $\mathbb{Q}(\sqrt{x_1})$, pelo teorema 6.

Procedendo de modo análogo, seja $x_3 \in \mathbb{Q}(\sqrt{x_1}, \sqrt{x_2})$ tal que

$$x_3 > 0 \;\text{ e }\; \sqrt{x_3} \notin \mathbb{Q}(\sqrt{x_1}, \sqrt{x_2}).$$

Então:

$$\mathbb{Q}(\sqrt{x_1}, \sqrt{x_2}, \sqrt{x_3}) \doteq \left\{ a + b\sqrt{x_3} \;\middle|\; a, b \in \mathbb{Q}(\sqrt{x_1}, \sqrt{x_2}) \right\}$$

é uma extensão de corpo de $\mathbb{Q}(\sqrt{x_1}, \sqrt{x_2})$, pelo teorema 6.

Repetindo o processo acima um número finito de vezes, pode-se obter várias extensões de corpos da forma

$$\mathbb{Q}(\sqrt{x_1}, ..., \sqrt{x_n}), n \in \mathbb{N}.$$

Note que são extensões sucessivas de $\mathbb{Q}$ e são formadas por números como aqueles que aparecem no exemplo 3. Afim de tornar o processo acima mais rigoroso, será apresentada a seguir uma definição por indução de $\mathbb{Q}(\sqrt{x_1}, ..., \sqrt{x_n})$ e, em seguida, um teorema que mostra que essas estruturas são de fato extensões de corpo umas das outras (e portanto extensões de corpo de $\mathbb{Q}$).

Definição 11. Defina:

(i) $E_0 \doteq \mathbb{Q}$

(ii) Para $n \in \mathbb{N}$ $(n \geq 1)$, seja $x_n \in E_{n-1}$ tal que $x_n > 0$ e $\sqrt{x_n} \notin E_{n-1}$. Então:

$$E_n \doteq E_{n-1}(\sqrt{x_n}) = \left\{ a + b\sqrt{x_n} \;\middle|\; a, b \in E_{n-1} \right\}.$$

Pelo *Princípio da Indução Finita*, segue de (i) e (ii) que E_n está definido para todo $n \in \mathbb{N} \cup \{0\}$. Por fim, para cada $n \in \mathbb{N}$, defina:

$$\mathbb{Q}(\sqrt{x_1}, ..., \sqrt{x_n}) \doteq E_n.$$

Proposição 8. Para todo $n \in \mathbb{N}$, E_n é uma extensão de corpo de E_{n-1}.

Demonstração. Considere o conjunto

$$X \doteq \{n \in \mathbb{N} \mid E_n \text{ é uma extensão de corpo de } E_{n-1}\} \subseteq \mathbb{N}.$$

O conjunto X possui as seguintes propriedades:

(i) Da definição de E_n, tem-se que $E_1 = E_0(\sqrt{x_1}) = \mathbb{Q}(\sqrt{x_1})$, onde x_1 é um racional tal que $x_1 > 0$ e $\sqrt{x_1} \notin \mathbb{Q}$. Portanto, pelo corolário 2, E_1 é uma extensão de corpo de E_0, ou seja, $1 \in X$.

(ii) Suponha agora que $n \in X$, ou seja, E_n é uma extensão de corpo de E_{n-1}. Será provado que $n+1 \in X$. Da hipótese de indução, tem-se que E_n é um subcorpo de $\mathbb{R}$. Da definição, $E_{n+1} = E_n(\sqrt{x_{n+1}})$, onde $x_{n+1} \in E_n$ é tal que $x_{n+1} > 0$ e $\sqrt{x_{n+1}} \notin E_n$. Portanto, pelo teorema 6, E_{n+1} é uma extensão de corpo de E_n, ou seja, $n+1 \in X$.

Pelo *Princípio da Indução Finita*, segue de (i) e (ii) que $X = \mathbb{N}$. Portanto, para todo $n \in \mathbb{N}$, E_n é uma extensão de corpo de E_{n-1}. □

As extensões de corpo E_n constituem o passo final para se chegar à caracterização dos números construtíveis. E para poder se referir a elas de modo formal e com fundamento matemático, é apresentada a definição a seguir.

Definição 12. Para cada $n \in \mathbb{N} \cup \{0\}$, E_n é chamada de *extensão quadrática iterada de* $\mathbb{Q}$.

Observação 5. O corpo dos racionais $E_0 = \mathbb{Q}$ e a extensão quadrática $E_1 = \mathbb{Q}(\sqrt{x_1})$ são incluídos na definição de *extensão quadrática iterada* para facilitar referências futuras.

Vale ressaltar que existem infinitas sequências $(E_n)_{n\in\mathbb{N}\cup\{0\}}$ de extensões quadráticas iteradas de $\mathbb{Q}$. Isso é fácil de se ver pois, desde que as condições sejam respeitadas, os números x_k podem assumir os mais diversos valores, gerando assim diferentes extensões quadráticas iteradas E_k e, portanto, diferentes sequências de extensões (E_n). Além disso, perceba que cada sequência de extensões quadráticas iteradas de $\mathbb{Q}$ é obtida através de uma recorrência, o que é um reflexo de a obtenção de pontos contrutíveis ser um processo recursivo, algo que foi destacado desde o início do capítulo anterior.

Finalmente, tem-se o necessário para formalizar a caracterização dos números construtíveis como "resultados de expressões radicais formadas apenas por raízes quadradas". A afirmação a seguir constitui o teorema 7, que será enunciado e provado na próxima e última seção deste capítulo, e é o teorema mais importante deste trabalho.

Todo número construtível é um elemento de alguma extensão quadrática iterada de $\mathbb{Q}$. *Reciprocamente, todo elemento de uma extensão quadrática iterada de* $\mathbb{Q}$ *é um número construtível.*

Assim, pode-se concluir que o corpo E dos números construtíveis é a união de todas as extensões quadráticas iteradas de $\mathbb{Q}$. Essa é a caracterização formal que se buscava! Se trata de algo extremamente não trivial e constitui a maior conquista desta dissertação. A demonstração do teorema 7 será feita na próxima seção, pois envolve uma série de definições e resultados necessários, que ficarão melhor organizados separadamente.

3.4 Demonstração da caracterização dos números construtíveis

Para iniciar esta seção, serão introduzidas algumas terminologias para facilitar a referência a determinadas situações.

Definição 13. Seja K um corpo qualquer. Denomina-se de *plano de K* o seguinte conjunto:

$$\mathscr{P}(K) \doteq \{(x,y) \mid x,y \in K\}.$$

Definição 14. Seja $F \subseteq E$ um subcorpo qualquer do corpo de números construtíveis. Fazer uma operação de construção *a partir do plano de F* significa:

(i) traçar uma reta construtível que passa por dois pontos do plano de F; ou

(ii) traçar uma circunferência construtível cujo centro é um ponto do plano de F e cujo raio é a distância entre dois pontos do plano de F.

Observação 6. Na definição acima, note que todo ponto do plano de F é um ponto construtível, pois suas coordenadas são números contrutíveis.

Lema 6. Seja $F \subseteq E$ um subcorpo qualquer do corpo de números construtíveis.

(i) Toda reta traçada a partir do plano de F possui uma equação da forma

$$ax + by + c = 0; \;\; a,b,c \in F.$$

(ii) Toda circunferência traçada a partir do plano de F possui uma equação da forma

$$x^2 + y^2 + dx + ey + f = 0; \;\; d,e,f \in F.$$

Demonstração. Sejam r e $\mathscr{C}$ uma reta e uma circunferência arbitrárias traçadas a partir do plano de F.

(i) Suponha que r não é paralela ao eixo y, e também não é o eixo y. Da geometria analítica, sabe-se que existem únicos $p,q \in \mathbb{R}$ tais que $y = px + q$ é uma equação da reta r. Pela definição 14, r passa por dois pontos do plano de F. Tome então dois pontos distintos do plano de F, $(x_1,y_1),(x_2,y_2) \in r$. Então:

$$\begin{cases} px_1 + q = y_1 \\ px_2 + q = y_2 \end{cases}.$$

Subtraindo a primeira equação da segunda, membro a membro, e isolando-se a incógnita p, conclui-se que

$$p = \frac{y_2 - y_1}{x_2 - x_1}.$$

Note que $x_2 - x_1 \neq 0$, pois a reta r não é paralela ao eixo y. Como x_1, x_2, y_1 e y_2 são elementos de F, segue que $p \in F$, pois F é corpo. Como $q = y_1 - px_1$, segue de modo análogo que $q \in F$.

Suponha agora que r é paralela ao eixo y ou é o próprio eixo y. De modo análogo, sabe-se que existe um único $c_0 \in \mathbb{R}$ tal que $x = c_0$ é uma equação de r. Qualquer ponto de r é da forma (c_0, y). Em particular, como há pelo menos um ponto do plano de F em r, a abscissa desse ponto também é c_0 e, portanto, $c_0 \in F$.

Em ambos os casos, foi obtida uma equação para r da forma $ax + by + c = 0$, onde $a, b, c \in F$.

(ii) Pela definição 14, o centro de $\mathscr{C}$ é um ponto do plano de F e seu raio é a distância entre dois pontos do plano de F. Chame o centro de $\mathscr{C}$ de (a,b) e seu raio de $r = PQ$, onde $P = (u_1, v_1)$ e $Q = (u_2, v_2)$ são pontos do plano de F. Pelo *Teorema de Pitágoras*,

$$r^2 = (u_2 - u_1)^2 + (v_2 - v_1)^2. \tag{3.2}$$

Como F é corpo, segue de 3.2 que $r^2 \in F$. Note que, apesar de o raio ser um número construtível, r pode não estar no subcorpo F, porém o seu quadrado estará com certeza. Da geometria analítica, sabe-se que, sendo (x,y) um ponto qualquer de $\mathscr{C}$,

$$(x-a)^2 + (y-b)^2 = r^2 \tag{3.3}$$

é uma equação de $\mathscr{C}$. Ao se expandir os quadrados, a equação 3.3 pode ser reescrita como:

$$x^2 - 2ax + a^2 + y^2 - 2by + b^2 = r^2. \tag{3.4}$$

Defina $d \doteq -2a$, $e \doteq -2b$ e $f \doteq a^2 + b^2 - r^2$. Como F é corpo, segue que $d, e, f \in F$, pois a, b e r^2 são elementos de F. Deste modo, pode-se reescrever a equação 3.4 assim:

$$x^2 + y^2 + dx + ey + f = 0,$$

que é, portanto, uma equação de $\mathscr{C}$ da forma que se buscava. □

Lema 7. Sejam F uma extensão quadrática iterada de $\mathbb{Q}$ e $F(\sqrt{x_1}),...,F(\sqrt{x_m})$ extensões quadráticas de F, onde $m \in \mathbb{N}$. Então existe um corpo G tal que:

(i) G é uma extensão quadrática iterada de $\mathbb{Q}$;

(ii) $F(\sqrt{x_k}) \subseteq G$, para todo $k \in \{1,...,m\}$.

Observe que, pela definição 10 de extensão quadrática de F, para cada $k \in \{1,...,m\}$, tem-se que $x_k > 0$ e $\sqrt{x_k} \notin F$.

Demonstração. Será feita uma prova por indução. Para isso, considere o conjunto a seguir: $X \doteq \{n \in \mathbb{N} \mid$ existe uma extensão quadrática iterada G_n de $\mathbb{Q}$ tal que $F(\sqrt{x_i}) \subseteq G_n$, para todo $i \in \{1,...,n\}\} \subseteq \mathbb{N}$. O conjunto X tem as seguintes propriedades.

(I) Se $n = 1$, defina $G_1 \doteq F(\sqrt{x_1})$. Como F é uma extensão quadrática iterada de $\mathbb{Q}$, segue da definição 11 que $F(\sqrt{x_1})$ também é uma extensão quadrática iterada de $\mathbb{Q}$. Além disso, é trivial que $F(\sqrt{x_1}) \subseteq G_1$. Portanto, $1 \in X$.

(II) Suponha que $n \in X$, ou seja, existe uma extensão quadrática iterada G_n de $\mathbb{Q}$ tal que $F(\sqrt{x_i}) \subseteq G_n$, para todo $i \in \{1,...,n\}$. Será provado que $n+1 \in X$. Há duas possibilidades a serem consideradas: (a) $\sqrt{x_{n+1}} \in G_n$ ou (b) $\sqrt{x_{n+1}} \notin G_n$. Cada caso será analisado separadamente.

(a) Suponha que $\sqrt{x_{n+1}} \in G_n$. Como $F \subseteq F(\sqrt{x_1})$ e $F(\sqrt{x_1}) \subseteq G_n$, segue que $F \subseteq G_n$. Logo, se $a,b \in F \subseteq G_n$, então $a + b\sqrt{x_{n+1}} \in G_n$, pois G_n é corpo. Portanto, $F(\sqrt{x_{n+1}}) \subseteq G_n$. Assim, neste caso basta tomar $G_{n+1} \doteq G_n$.

(b) Suponha que $\sqrt{x_{n+1}} \notin G_n$. Defina $G_{n+1} \doteq G_n(\sqrt{x_{n+1}})$. Como G_n é uma extensão quadrática iterada de $\mathbb{Q}$, segue da definição 11 que G_{n+1} também é uma extensão quadrática iterada de $\mathbb{Q}$. Além disso, para todo $i \in \{1,...,n\}$, $F(\sqrt{x_i}) \subseteq G_n$, pela hipótese de indução; e é trivial que $G_n \subseteq G_n(\sqrt{x_{n+1}})$. Logo, $F(\sqrt{x_i}) \subseteq G_n(\sqrt{x_{n+1}})$, para todo $i \in \{1,...,n\}$. Também é direto que $F(\sqrt{x_{n+1}}) \subseteq G_n(\sqrt{x_{n+1}})$, pois $F \subseteq G_n$. Portanto, $F(\sqrt{x_i}) \subseteq G_{n+1}$, para todo $i \in \{1,...,n+1\}$.

Assim, seja qual for o caso, (a) ou (b), existe uma extensão quadrática iterada G_{n+1} de $\mathbb{Q}$ tal que $F(\sqrt{x_i}) \subseteq G_{n+1}$, para todo $i \in \{1,...,n+1\}$. Portanto, $n+1 \in X$.

Pelo *Princípio da Indução Finita*, segue das propriedades (I) e (II) acima que $X = \mathbb{N}$. Portanto, para todo $m \in \mathbb{N}$, quaisquer que sejam as extensões quadráticas $F(\sqrt{x_1}),...,F(\sqrt{x_m})$ de F, existe um corpo G, que é uma extensão quadrática iterada de $\mathbb{Q}$ tal que $F(\sqrt{x_k}) \subseteq G$, para todo $k \in \{1,...,m\}$. □

Teorema 7 (Caracterização dos números construtíveis)**.** Todo número construtível é um elemento de alguma extensão quadrática iterada de $\mathbb{Q}$. Reciprocamente, todo elemento de uma extensão quadrática iterada de $\mathbb{Q}$ é um número construtível.

Demonstração. O teorema envolve uma proposição e sua recíproca, logo a sua demonstração é dividida em duas partes, e será iniciada pela implicação mais fácil, a de que todo elemento de uma extensão quadrática iterada de $\mathbb{Q}$ é um número construtível.

($\Leftarrow$) Como já foi observado, existem infinitas sequências (E_n) de extensões quadráticas iteradas de $\mathbb{Q}$. Para mostrar então que os elementos de qualquer extensão quadrática iterada de $\mathbb{Q}$ são números construtíveis, fixe uma sequência (E_n) arbitrária. Será provado por indução que os elementos de todo termo dessa sequência são números construtíveis. Para isso, defina:

$$X \doteq \{n \in \mathbb{N} \mid \text{todo elemento de } E_{n-1} \text{ é um número construtível}\} \subseteq \mathbb{N}.$$

O conjunto X possui as propriedades a seguir.

(i) Pelo teorema 2, todo elemento de $E_0 = \mathbb{Q}$ é um número construtível. Portanto, $1 \in X$.

(ii) Suponha que $n \in X$, ou seja, todo elemento de E_{n-1} é um número construtível. Será provado que $n+1 \in X$. Por definição, $E_n = E_{n-1}(\sqrt{x_n})$, para algum $x_n \in E_{n-1}$ tal que $x_n > 0$ e $\sqrt{x_n} \notin E_{n-1}$. Logo, segue da hipótese de indução que x_n é um número construtível. Pelo lema 5, tem-se então que $\sqrt{x_n}$ é um número construtível. Assim, se $a, b \in E_{n-1} \subseteq E$, então $a + b\sqrt{x_n} \in E$, pois E é corpo. Portanto, $E_{n-1}(\sqrt{x_n}) \subseteq E$, ou seja, todo elemento de E_n é um número construtível. Portanto, $n+1 \in X$.

Pelo *Princípio da Indução Finita*, segue de (i) e (ii) que $X = \mathbb{N}$. Portanto, para todo $n \in \mathbb{N} \cup \{0\}$, os elementos de E_n são números construtíveis. Como a sequência (E_n) foi tomada de modo arbitrário, segue que todo elemento de qualquer extensão quadrática iterada de $\mathbb{Q}$ é um número construtível.

($\Rightarrow$) Agora será mostrada a parte mais difícil do teorema e, para provar que todo número contrutível é um elemento de alguma extensão quadrática iterada de $\mathbb{Q}$, será provada uma afirmação mais forte:

Para todo $n \in \mathbb{N}$, existe um corpo F_n, que é uma extensão quadrática iterada de $\mathbb{Q}$ tal que todo número construtível que pode ser obtido em n ou menos operações de construção está em F_n.

É interessante observar já nesse momento que a ideia dessa afirmação está presente no que foi feito no início da seção anterior, ou seja, o que foi oferecido para ilustrar a ideia ao aluno consiste em casos particulares dessa proposição mais geral. Essa relação será melhor comentada e explorada ao final da demonstração do teorema.

A prova dessa afirmação mais forte será feita por indução. Para isso, defina o seguinte conjunto: $X \doteq \{n \in \mathbb{N} \mid$ existe um corpo F_n que é uma extensão quadrática iterada de $\mathbb{Q}$ tal que, se c é um número contrutível que pode ser obtido em n ou menos operações de construção, então $c \in F_n\} \subseteq \mathbb{N}$. Este conjunto possui as seguintes propriedades.

(I) Usando o que foi previamente explicado, é fácil provar que $1 \in X$. De fato, no início da seção anterior foi mostrado que os únicos números construtíveis que podem ser obtidos em uma operação de construção ou menos são 0 e 1. Logo, neste caso basta tomar $F_1 \doteq \mathbb{Q}$, que é por definição uma extensão quadrática iterada de $\mathbb{Q}$. Assim tem-se que $0, 1 \in F_1$ e, portanto, $1 \in X$.

Vale observar que se poderia tomar F_1 como qualquer outra extensão quadrática iterada de $\mathbb{Q}$. Por exemplo, se $F_1 = \mathbb{Q}(\sqrt{2})$ ou $F_1 = \mathbb{Q}(\sqrt{5}, \sqrt{7})$, a condição também se verifica. Assim, conclui-se que, se $F_n = \mathbb{Q}(\sqrt{x_1}, ..., \sqrt{x_m})$, então m pode ser muito maior do que n.

(II) Suponha que $n \in X$. Será provado que $n+1 \in X$.

Pela hipótese de indução, existe um corpo F_n, que é uma extensão quadrática iterada de $\mathbb{Q}$ tal que todo número construtível que pode ser obtido em n ou menos operações de construção está em F_n. Isso quer dizer que todos os pontos construtíveis obtidos em n ou menos operações de contrução pertencem ao plano de F_n. Para se fazer uma sequência de $n+1$ operações de construção, a última operação só pode ser feita a partir desses pontos preexistentes. Como esses pontos estão no plano de F_n, tem-se que um ponto obtido em $n+1$ operações de construção pode ser apenas:

(i) a interseção entre duas retas construtíveis concorrentes r_1 e r_2, traçadas a partir do plano de F_n; ou

(ii) uma interseção entre uma reta construtível r e uma circunferência construtível $\mathscr{C}$, traçadas a partir do plano de F_n; ou

(iii) uma interseção entre duas circunferências construtíveis distintas $\mathscr{C}_1$ e $\mathscr{C}_2$, traçadas a partir do plano de F_n.

É extremamente importante ressaltar que não é toda operação de construção feita a partir do plano de F_n que está inclusa nos itens acima, pelo seguinte: apesar de todo ponto construtível que pode ser obtido em n ou menos operações estar no plano de F_n, nem todo ponto do plano de F_n pode ser obtido em n ou menos operações. E mais: F_n é infinito, porém a quantidade de pontos contrutíveis que podem ser obtidos em n ou menos operações é finita. Portanto, os itens acima apenas implicam que todas as operações feitas a partir de pontos obtidos em n ou menos operações são feitas a partir de F_n, mas não vale a recíproca.

Assim, para se analisar os números construtíveis obtidos com $n+1$ operações de construção, basta considerar cada um dos três casos separadamente.

(i) Pelo lema 6, pode-se tomar as seguintes equações para r_1 e r_2, respectivamente:

$$a_1x+b_1y+c_1=0 \text{ e } a_2x+b_2y+c_2=0,$$

onde $a_i, b_i, c_i \in F_n$, para $i \in \{1,2\}$. Assim, encontrar o ponto de interseção entre r_1 e r_2 equivale a resolver o sistema a seguir.

$$\begin{cases} a_1x+b_1y+c_1=0 \\ a_2x+b_2y+c_2=0 \end{cases} \tag{3.5}$$

Note que a_1 e b_1 não são ambos nulos. Do contrário, se $a_1=b_1=0$, então r_1 não seria uma reta. Suponha então, sem perda de generalidade, que $b_1 \neq 0$. Deste modo, pode-se isolar a incógnita y na primeira equação do sistema do seguinte modo:

$$y=-\frac{a_1x+c_1}{b_1}. \tag{3.6}$$

No caso em que $b_1=0$, tem-se que $a_1 \neq 0$, o que permite isolar a incógnita x na primeira equação do sistema e então fazer o restante dos passos de modo análogo ao que será feito a seguir, bastando para isso inverter os papéis de x e y.

Agora, para encontrar o valor de x, basta substituir 3.6 na segunda equação do sistema 3.5, e então efetuar os cálculos abaixo.

$$a_2x+b_2\left(-\frac{a_1x+c_1}{b_1}\right)+c_2=0 \;\Rightarrow\; a_2x-\frac{a_1b_2}{b_1}x-\frac{b_2c_1}{b_1}+c_2=0 \;\Rightarrow$$

$$\left(a_2-\frac{a_1b_2}{b_1}\right)x=c_2-\frac{b_2c_1}{b_1} \;\Rightarrow\; \frac{a_2b_1-a_1b_2}{b_1}x=\frac{b_1c_2-b_2c_1}{b_1}$$

Note que $a_2b_1-a_1b_2 \neq 0$, pois as retas r_1 e r_2 são concorrentes. Portanto,

$$x=\frac{b_1c_2-b_2c_1}{a_2b_1-a_1b_2}. \tag{3.7}$$

Assim, segue de 3.7 e 3.6 que as coordenadas do ponto de interseção entre r_1 e r_2 são elementos de F_n, pois F_n é corpo.

Ao se variar as retas r_1 e r_2, os coeficientes a_i, b_i e c_i mudam e, portanto, pode-se obter diversos valores para x e y. Porém, independente dos valores das coordenadas, todas as interseções entre duas retas traçadas a partir do plano de F_n estarão no próprio plano de F_n. Isso é o suficiente por enquanto, pois a extensão F_{n+1} que se busca será obtida após a conclusão dos próximos dois casos, (ii) e (iii). Entretanto, se o objetivo fosse concluir cada caso separadamente, a extensão quadrática iterada de $\mathbb{Q}$ do item (i) seria o próprio F_n, ou seja, ao se lidar apenas com retas, não são gerados números construtíveis fora da extensão em que estão os coeficientes das mesmas.

(ii) Pelo lema 6, pode-se tomar as seguintes equações para r e $\mathscr{C}$, respectivamente:

$$ax+by+c=0 \text{ e } x^2+y^2+dx+ey+f=0,$$

onde $a,b,c,d,e,f \in F_n$. Assim, encontrar as interseções entre r e $\mathscr{C}$ equivale a resolver o sistema a seguir.

$$\begin{cases} ax+by+c=0 \\ x^2+y^2+dx+ey+f=0 \end{cases} \tag{3.8}$$

De modo análogo ao item anterior, tem-se que a e b não são ambos nulos. Suponha então, sem perda de generalidade, que $b \neq 0$. Deste modo, segue da primeira equação que

$$y = -\frac{ax+c}{b}. \tag{3.9}$$

Substituindo este valor de y na segunda equação do sistema 3.8, obtém-se:

$$\begin{aligned} 0 &= x^2 + \left(-\frac{ax+c}{b}\right)^2 + dx + e\left(-\frac{ax+c}{b}\right) + f \\ &= x^2 + \frac{a^2}{b^2}x^2 + \frac{2ac}{b^2}x + \frac{c^2}{b^2} + dx - \frac{ae}{b}x - \frac{ce}{b} + f \\ &= \left(1+\frac{a^2}{b^2}\right)x^2 + \left(\frac{2ac}{b^2} + d - \frac{ae}{b}\right)x + \left(\frac{c^2}{b^2} - \frac{ce}{b} + f\right) \\ &= \left(\frac{b^2+a^2}{b^2}\right)x^2 + \left(\frac{2ac-abe+db^2}{b^2}\right)x + \left(\frac{c^2-cbe+fb^2}{b^2}\right) \\ &= \left(a^2+b^2\right)x^2 + \left(2ac-abe+db^2\right)x + \left(c^2-cbe+fb^2\right) \end{aligned}$$

Defina $A \doteq a^2+b^2$, $B \doteq 2ac-abe+db^2$ e $C \doteq c^2-cbe+fb^2$. Assim, a última equação pode ser reescrita como:

$$Ax^2+Bx+C=0, \tag{3.10}$$

onde $A,B,C \in F_n$, pois F_n é corpo, e $A \neq 0$, pois a e b não são ambos nulos.

A equação 3.10 tem solução real se, e somente se,

$$s \doteq B^2 - 4AC \geq 0.$$

Como F_n é um corpo, tem-se que $s \in F_n$. Assim, se a reta r e a circunferência $\mathscr{C}$ se intersectam no plano real, segue que

$$x = \frac{-B \pm \sqrt{s}}{2A} \in \mathbb{R}. \tag{3.11}$$

Há duas possibilidades: (a) $\sqrt{s} \in F_n$ ou (b) $\sqrt{s} \notin F_n$. Cada caso será analisado separadamente.

(a) Se $\sqrt{s} \in F_n$, então segue de 3.11 e 3.9 que as coordenadas dos pontos de interseção entre r e $\mathscr{C}$ estão em F_n, pois F_n é corpo.

(b) Se $\sqrt{s} \notin F_n$, então segue de 3.11 e 3.9 que as coordenadas dos pontos de interseção entre r e $\mathscr{C}$ estão em $F_n(\sqrt{s})$, que é uma extensão quadrática iterada de $\mathbb{Q}$, uma vez que F_n é uma extensão quadrática iterada de $\mathbb{Q}$, pela hipótese de indução.

Ao se variar a reta r e a circunferência $\mathscr{C}$, os coeficientes a,b,c,d,e,f mudam e, portanto, pode-se obter diversos valores para s. Porém, há um número finito de pontos construtíveis que podem ser obtidos em n ou menos operações de construção e, portanto, há um número finito de retas e circunferências que podem ser traçadas a partir destes pontos (apesar de haver um número infinito de operações que podem ser feitas a partir de F_n). Assim, em particular, pode-se obter apenas uma quantidade finita de valores para s. Portanto, existem números

$$s_1, s_2, ..., s_p \in F_n,$$

tais que $s_i > 0$ e $\sqrt{s_i} \notin F_n$, para todo $i \in \{1, ..., p\}$, e cada número construtível resultante de uma interseção entre uma reta e uma circunferência traçadas a partir de pontos obtidos em n ou menos operações de construção está em uma das seguintes extensões quadráticas iteradas de $\mathbb{Q}$:

$$F_n(\sqrt{s_1}), F_n(\sqrt{s_2}), ..., F_n(\sqrt{s_p}).$$

Vale ressaltar que até mesmo os números construtíveis do caso (a) estão em uma das extensões acima, pois, por exemplo, $F_n \subseteq F_n(\sqrt{s_1})$ (qualquer s_i serviria para este argumento).

Note que ainda não foi obtida uma única extensão quadrática iterada de $\mathbb{Q}$ para se provar que $n+1 \in X$. O corpo F_{n+1} será obtido após se completar (i), (ii) e (iii), através da unificação de tudo o que estiver feito nos três itens.

(iii) Pelo lema 6, pode-se tomar as seguintes equações para $\mathscr{C}_1$ e $\mathscr{C}_2$, respectivamente:

$$x^2 + y^2 + d_1 x + e_1 y + f_1 = 0 \text{ e } x^2 + y^2 + d_2 x + e_2 y + f_2 = 0,$$

onde $d_i, e_i, f_i \in F_n$, para $i \in \{1,2\}$. Assim, encontrar as interseções entre $\mathscr{C}_1$ e $\mathscr{C}_2$ equivale a resolver o sistema a seguir.

$$\begin{cases} x^2 + y^2 + d_1 x + e_1 y + f_1 = 0 \\ x^2 + y^2 + d_2 x + e_2 y + f_2 = 0 \end{cases} \tag{3.12}$$

Subtraindo a segunda equação da primeira, obtém-se um sistema equivalente:

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases}, \tag{3.13}$$

onde $a \doteq d_1 - d_2, b \doteq e_1 - e_2, c \doteq f_1 - f_2, d \doteq d_2, e \doteq e_2$ e $f \doteq f_2$ são elementos de F_n.

Note que a e b não são ambos nulos. Do contrário, se $a = b = 0$, então $c = 0$ e, portanto, $d_1 = d_2$, $e_1 = e_2$ e $f_1 = f_2$, o que é um absurdo, pois as circunferências $\mathscr{C}_1$ e $\mathscr{C}_2$ são distintas, por hipótese. Logo, o sistema 3.13 é igual ao sistema 3.8, com as mesmas condições.

Portanto, de modo análogo ao que foi feito em (ii), existem números

$$t_1, t_2, ..., t_q \in F_n,$$

tais que $t_j > 0$ e $\sqrt{t_j} \notin F_n$, para $j \in \{1, ..., q\}$, e cada número construtível resultante de uma interseção entre duas circunferências traçadas a partir de pontos obtidos em n ou menos operações de construção está em uma das seguintes extensões quadráticas iteradas de $\mathbb{Q}$:

$$F_n(\sqrt{t_1}), F_n(\sqrt{t_2}), ..., F_n(\sqrt{t_q}).$$

Sumarizando o que foi feito em (i), (ii) e (iii), tem-se que cada número construtível resultante de operações de construção feitas a partir de pontos contrutíveis obtidos em n ou menos operações está em uma das extensões quadráticas iteradas de $\mathbb{Q}$ a seguir:

$$F_n(\sqrt{s_1}), F_n(\sqrt{s_2}), ..., F_n(\sqrt{s_p}), F_n(\sqrt{t_1}), F_n(\sqrt{t_2}), ..., F_n(\sqrt{t_q}).$$

Vale ressaltar que isso engloba, inclusive, os números construtíveis obtidos como em (i), pois $F_n \subseteq F_n(\sqrt{s_1})$, por exemplo (qualquer s_i ou t_j serviria para se usar o mesmo argumento).

Pelo lema 7, existe um corpo F_{n+1}, que é uma extensão quadrática iterada de $\mathbb{Q}$, tal que

$$F_n(\sqrt{s_i}) \subseteq F_{n+1} \text{ e } F_n(\sqrt{t_j}) \subseteq F_{n+1},$$

para todo $i \in \{1, ..., p\}$ e para todo $j \in \{1, ..., q\}$.

Note ainda que $F_n \subseteq F_{n+1}$, pois $F_n \subseteq F_n(\sqrt{s_1})$ e $F_n(\sqrt{s_1}) \subseteq F_{n+1}$ (qualquer s_i ou t_j serviria para este argumento).

Portanto, todos os números construtíveis obtidos em $n+1$ ou menos operações de contrução estão em F_{n+1}, ou seja, $n+1 \in X$.

Pelo *Princípio da Indução Finita*, segue de (I) e (II) que $X = \mathbb{N}$. Portanto, para todo $n \in \mathbb{N}$, existe um corpo F_n, que é uma extensão quadrática iterada de $\mathbb{Q}$ tal que todo número construtível que pode ser obtido em n ou menos operações de construção está em F_n.

Assim, fica provado que todo número construtível está em alguma extensão quadrática iterada de $\mathbb{Q}$, o que finaliza a demonstração. □

Corolário 3. Para cada $n \in \mathbb{N}$, existe um corpo F_n, que é uma extensão quadrática iterada de $\mathbb{Q}$ tal que todo número construtível que pode ser construído em n ou menos operações de construção está em F_n.

É importante contextualizar que a afirmação desse corolário é a generalização do que foi feito no início da seção 3.3. Deve-se observar que, em essência, o que foi feito *antes* do exemplo 3 é mostrar que essa proposição é válida para $n = 1$ e $n = 2$, e que pode se considerar $F_1 = \mathbb{Q}$ e $F_2 = \mathbb{Q}(\sqrt{3})$. Por sua vez, o que foi feito no exemplo 3 em si é ilustrar a afirmação acima para

uma sequência específica de operações de construção, que acaba resultando em uma extensão quadrática iterada específica. E esse mesmo exemplo pode servir para justificar o teorema 7, como se ilustra a seguir.

Imagine que se está no caso $n = 6$, de números construtíveis obtidos em 6 ou menos operações de construção. O exemplo 3 mostra uma sequência específica de 6 operações, que acabam por resultar na extensão quadrática iterada $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7})$. De modo análogo, outras sequências de 6 operações poderiam resultar em novas extensões quadráticas iteradas de $\mathbb{Q}$. Assim, seriam obtidas diversas extensões quadráticas iteradas de $\mathbb{Q}$ e então seria possível concluir, sem a necessidade do lema 7 e sem a necessidade de uma única extensão F_6, que cada número construtível que pode ser obtido em 6 ou menos operações de construção está em uma extensão quadrática iterada de $\mathbb{Q}$. Por fim, o argumento desse raciocínio informal seria de que o caso $n = 6$ não tem nada de especial e o mesmo aconteceria para $7, 8, 9$ ou qualquer outro número de operações de construção, de modo que todo e qualquer número construtível estaria, portanto, em alguma extensão quadrática iterada de $\mathbb{Q}$.

CAPÍTULO

4

DUPLICAÇÃO DO CUBO E TRISSECÇÃO DO ÂNGULO

Neste capítulo serão resolvidos dois dos problemas de construção: a duplicação do cubo e a trissecção do ângulo. Uma vez que se sabe que qualquer número construtível está em alguma extensão quadrática iterada de $\mathbb{Q}$, basta alguns pequenos passos para finalizar a solução desses dois problemas. O trecho restante a ser percorrido precisa ser apresentado de forma igualmente rigorosa a tudo o que foi feito durante todo o percurso até aqui e isso justifica a necessidade de um capítulo inteiro para a conclusão dos problemas, porém a ideia final é simples e será apresentada de forma resumida na primeira seção deste capítulo. Além da caracterização dos números construtíveis que foi feita no capítulo anterior, serão necessários alguns resultados sobre equações cúbicas para a formalização das soluções, que serão apresentados na segunda seção deste capítulo. *Mas por que cúbicas?* Na primeira seção, também será feita uma explicação bem didática sobre o surgimento de equações cúbicas na resolução desses problemas. Vale ressaltar que os resultados e demonstrações apresentados neste capítulo são inspiradas nas ideias apresentadas em Kazarinoff (2003), e foram recheadas de maiores explicações, modificadas com ideias proprias e escritas com um pouco mais de rigor.

4.1 Por que cúbicas?

Considere um cubo unitário, isto é, um cubo cuja aresta tenha medida igual a 1. O volume de um cubo é dado pelo cubo de sua aresta. Logo, o volume do cubo unitário é igual a 1. Suponha que seja possível construir com régua e compasso um novo cubo de aresta a cujo volume seja igual a 2, ou seja, o dobro do volume do cubo unitário. Isso implica que a aresta do cubo é um segmento de reta construtível e, portanto, a sua medida a é um *número construtível*, pois é a distância entre dois pontos construtíveis. Além disso, como o volume do cubo de aresta a é igual a a^3, obtém-se a seguinte igualdade: $a^3 = 2$.

Portanto, ao se supor que é possível duplicar o cubo unitário, obtém-se um número construtível a tal que $a^3 - 2 = 0$. Em outras palavras, para que seja possível construir com régua e compasso um cubo cujo volume é igual a 2, deve existir um número construtível que seja raiz da equação cúbica

$$x^3 - 2 = 0. \tag{4.1}$$

E eis que naturalmente aparece uma equação cúbica ao se explorar a duplicação do cubo! Será que realmente existe um número construtível que seja raiz dessa equação? É aí que reside o segredo da solução da duplicação do cubo: *A equação* (4.1) *não possui raiz construtível*. Para provar isso, será apresentado um teorema que garante que certas equações cúbicas que não tenham nenhuma raiz racional não terão nenhuma raiz que é um número construtível. Pode-se dizer então que este teorema é a via principal do trecho restante a ser percorrido. Para acessar essa via e aplicar o teorema à equação (4.1), será necessária uma proposição auxiliar que possibilite mostrar que essa equação não tem nenhuma raiz racional. Tendo esse acesso, o mapa mental do caminho a ser completado pode ser facilmente resumido: Basta provar a proposição e o teorema, e então mostrar que a equação (4.1) não tem raiz racional, o que implicará que essa equação não tem nenhuma raiz construtível e, portanto, não existe um número construtível a tal que $a^3 = 2$; deste modo, ficará demonstrado que não é possível construir com régua e compasso um cubo cujo volume seja igual a 2 e, portanto, é impossível duplicar o cubo unitário, o que resolve o problema da duplicação do cubo, como foi explicado no primeiro capítulo, pois mostra que nem todo cubo pode ser duplicado com régua e compasso. Simples assim! Por fim, é preciso dizer que, para provar o teorema que é a via principal, serão necessários três lemas sobre equações cúbicas. Tudo isso, incluindo teorema, proposição e lemas, será apresentado e provado na próxima seção.

Alguém estará se perguntando: *E a trissecção do ângulo?* O caminho a ser percorrido é exatamente o mesmo da duplicação do cubo! Ao se supor que é possível dividir um ângulo de 60° com apenas régua e compasso, também se chega em uma determinada equação cúbica que deveria ter uma raiz construtível mas que na realidade não tem, exatamente como ocorre com a equação (4.1). Porém, será um pouquinho mais trabalhoso chegar na equação cúbica da trissecção. Assim sendo, a duplicação do cubo foi escolhida nessa seção para ilustrar todo o trajeto restante a ser percorrido de modo simples e resumido, e através desse mesmo caminho os dois problemas serão resolvidos.

4.2 Equações cúbicas

Uma *equação cúbica* é uma equação polinomial do 3º grau. Toda equação cúbica (em uma variável) pode ser escrita na seguinte forma:

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0, \tag{4.2}$$

onde $a_i \in \mathbb{C}, i \in \{0,1,2,3\}$, e $a_3 \neq 0$. A equação acima é chamada de *forma geral* da equação cúbica. Entretanto, é suficiente estudar as equações cúbicas da forma

$$t^3 + pt + q = 0,$$

onde $p, q \in \mathbb{C}$, pois sempre é possível eliminar o termo de grau dois através de uma *mudança de variável*. Para provar essa afirmação, primeiro divida ambos os membros da equação (4.2) por a_3, obtendo assim a equação

$$x^3 + ax^2 + bx + c = 0, \tag{4.3}$$

onde $a \doteq \dfrac{a_2}{a_3}$, $b \doteq \dfrac{a_1}{a_3}$ e $c \doteq \dfrac{a_0}{a_3}$. Depois, faça a substituição $x = t + u$ na equação acima e desenvolva o seu primeiro membro:

$$\begin{aligned} x^3 + ax^2 + bx + c &= (t+u)^3 + a(t+u)^2 + b(t+u) + c \\ &= t^3 + 3t^2u + 3tu^2 + u^3 + at^2 + 2atu + au^2 + bt + bu + c \\ &= t^3 + (3u+a)t^2 + (3u^2 + 2au + b)t + (u^3 + au^2 + bu + c) \end{aligned} \tag{4.4}$$

Para eliminar o termo do 2º grau na nova variável t em (4.4), basta exigir $3u + a = 0$, o que implica em $u = -\dfrac{a}{3}$. Portanto, a *mudança de variável* adequada é dada por $x = t - \dfrac{a}{3}$. Por fim, substitua o valor de u em (4.4) e desenvolva:

$$\begin{aligned} x^3 + ax^2 + bx + c &= t^3 + \left[3\left(-\frac{a}{3}\right)^2 + 2a\left(-\frac{a}{3}\right) + b\right]t + \left(-\frac{a}{3}\right)^3 + a\left(-\frac{a}{3}\right)^2 + b\left(-\frac{a}{3}\right) + c \\ &= t^3 + \left(\frac{a^2}{3} - \frac{2a^2}{3} + b\right)t + \left(-\frac{a^3}{27} + \frac{a^3}{9} - \frac{ab}{3} + c\right) \\ &= t^3 + \left(-\frac{a^2}{3} + b\right)t + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) \\ &= t^3 + pt + q, \end{aligned} \tag{4.5}$$

onde

$$p \doteq -\frac{a^2}{3} + b \quad \text{e} \quad q \doteq \frac{2a^3}{27} - \frac{ab}{3} + c.$$

Portanto, de fato a equação $x^3 + ax^2 + bx + c = 0$ pode ser reduzida a uma nova equação da forma $t^3 + pt + q = 0$, que é mais simples e facilita o estudo das equações cúbicas.

Renomeando a incógnita e os coeficientes da equação $t^3 + pt + q = 0$, tem-se que o objeto de estudo desta seção é uma equação da seguinte forma:

$$x^3 + ax + b = 0, \tag{4.6}$$

onde $a, b \in \mathbb{C}$. A equação (4.6) é chamada de *forma reduzida* da equação cúbica. Perceba que a equação $x^3 - 2 = 0$ é um caso particular dessa equação, quando $a = 0$ e $b = -2$. Na quarta seção deste capítulo será visto que também surge um outro caso particular da equação (4.6) na solução da trissecção do ângulo. Assim, ao se estudar a forma reduzida de modo geral e não apenas a equação $x^3 - 2 = 0$ pontualmente, serão obtidas ferramentas para se resolver tanto a duplicação do cubo como a trissecção do ângulo (e quem sabe outros problemas de construção). Como o objetivo final é provar uma afirmação acerca das raízes dessas equações cúbicas, se faz necessário conhecer um pouco mais sobre suas raízes e como as mesmas se relacionam com os números construtíveis.

Para não se perder no meio de tantos resultados e formalismos que vêm a seguir, relembre do mapa mental, onde dois resultados compõem o trajeto restante a ser percorrido para se chegar às soluções da duplicação do cubo e da trissecção do ângulo. O primeiro e mais importante resultado é um teorema que garante que certas equações cúbicas não têm nenhuma raiz construtível. Este teorema é a via principal do trajeto e será apelidado de *Teorema da Raiz Construtível*, para facilitar futuras referências. O segundo resultado é uma proposição auxiliar que servirá para mostrar que as equações cúbicas da duplicação e da trissecção não possuem raízes racionais, que é uma hipótese importante do teorema. Esta proposição constitui, portanto, um acesso para a via principal, e será enunciada a seguir, antes do teorema. Vale observar que essa proposição é na realidade um caso particular do *Teorema das Raízes Racionais*, que fornece uma condição para as raízes racionais de acordo com os coeficientes de uma equação polinomial qualquer (com coeficientes inteiros).

Proposição 9. Considere uma equação cúbica reduzida com *coeficientes inteiros*:

$$x^3 + a_1 x + a_0 = 0, \quad a_1, a_0 \in \mathbb{Z}. \tag{4.7}$$

Sejam $p, q \in \mathbb{Z}$, $q \neq 0$, tais que $mdc(p,q) = 1$ e $\dfrac{p}{q}$ é uma raiz de 4.7. Então:

(i) p é um fator de a_0; e

(ii) $q = 1$ ou $q = -1$.

Demonstração. Como $\dfrac{p}{q}$ é uma raiz de 4.7, segue que

$$\left(\frac{p}{q}\right)^3 + a_1\left(\frac{p}{q}\right) + a_0 = 0.$$

Multiplicando ambos os membros dessa equação por q^3, obtém-se:

$$p^3 + a_1 pq^2 + a_0 q^3 = 0. \tag{4.8}$$

Note que todos os termos da igualdade acima são números inteiros, pois $a_1, a_0, p, q \in \mathbb{Z}$. A partir disso, basta olhar para esta igualdade de dois modos diferentes para provar cada item do lema.

(i) Primeiro, reescreva a igualdade 4.8 do seguinte modo:

$$p(p^2 + a_1 q^2) = -a_0 q^3.$$

Logo, p é um fator de $a_0 q^3$. Por hipótese, p não tem fator maior do que 1 em comum com q e, por consequência, não tem fator comum com q^3. Portanto, p é um fator de a_0.

(ii) De modo análogo ao item anterior, reescreva a igualdade 4.8 assim:

$$(a_1 pq + a_0 q^2)q = -p^3.$$

Logo, q é um fator de p^3 e, por consequência, q é um fator de p. Mas, por hipótese, o maior fator comum entre p e q é 1. Portanto, $q = 1$ ou $q = -1$. □

Vale observar que sempre pode-se supor $mdc(p,q) = 1$, pois se está pensando na *forma irredutível* da raiz racional, e toda fração pode ser simplificada até se obter a forma irredutível, onde numerador e denominador não têm fator comum maior do que 1.

O objetivo agora é enunciar e provar o *Teorema da Raiz Construtível*, mas para isso serão necessários três lemas, sendo que os dois primeiros, assim como a proposição anterior, são versões particulares de resultados mais gerais de álgebra.Enquanto os lemas são resultados específicos sobre a forma reduzida de uma equação cúbica, as suas versões generalizadas se aplicam a toda equação polinomial.

Para explicar a motivação e justificar a apresentação das versões mais simples neste capítulo, considere como exemplo o *Teorema Fundamental da Álgebra*. Tal teorema diz que toda equação polinomial em uma variável possui pelo menos uma raiz complexa e, como corolário, segue que toda equação polinomial de grau *n* possui exatamente *n* raízes complexas. Este teorema é extremamente importante para o ensino de álgebra como um todo, porém é um resultado muito mais forte do que se necessita neste capítulo. Além disso, é um teorema muito difícil de se provar a nível elementar. Tanto é que o mesmo é apresentado nos melhores materiais de ensino médio do país sem demonstração. No geral, se aceita o *Teorema Fundamental da Álgebra* como verdadeiro sem justificativa (com o argumento de que sua demonstração precisa de ferramentas de "matemática de nível superior") e então o corolário é demonstrado através de divisões sucessivas do polinômio. Naturalmente, o objetivo deste trabalho é fazer o oposto disso e não usar nenhuma afirmação sem demonstração, exceto é claro resultados elementares, como por exemplo fatos básicos e conhecidos sobre divisibilidade, polinômios, operações com polinômios e equações polinomiais do 2º grau.

Deste modo, ficam claros dois motivos para não se apresentar resultados mais gerais como o *Teorema Fundamental da Álgebra* neste capítulo. O primeiro motivo é que as versões

mais simples são suficientes para demonstrar tudo o que é necessário para concluir as soluções da duplicação do cubo e da trissecção do ângulo. E o segundo motivo é que as versões particulares são mais fáceis de se provar e, portanto, mais acessíveis a um professor do ensino básico ou a um aluno mais curioso. Assim, com inspiração no que foi falado no primeiro capítulo sobre as prováveis motivações de Euclides para estruturar *Os Elementos*, a mensagem ímplicita neste capítulo é: Eis tudo o que se precisa para resolver a duplicação do cubo e a trissecção do ângulo de modo básico e justificado.

Nesse espírito, o primeiro lema mostra a seguir que nem todo mundo precisa do *Teorema Fundamental da Álgebra*.

Lema 8. Se uma equação cúbica reduzida tem uma raiz r_1, então essa equação tem três raízes r_1, r_2 e r_3, que podem ou não serem distintas, e

$$x^3 + ax + b = (x - r_1)(x - r_2)(x - r_3). \tag{4.9}$$

Demonstração. Seja r_1 uma raiz da equação cúbica reduzida

$$x^3 + ax + b = 0, \tag{4.10}$$

onde a e b são números reais. Dividindo o polinômio $x^3 + ax + b$ por $x - r_1$, obtém-se:

$$x^3 + ax + b = (x - r_1)(x^2 + r_1 x + r_1^2 + a) + r_1^3 + ar_1 + b.$$

Como r_1 é raiz de 4.10, segue que $r_1^3 + ar_1 + b = 0$ e, portanto,

$$x^3 + ax + b = (x - r_1)(x^2 + r_1 x + r_1^2 + a). \tag{4.11}$$

Do ensino básico, sabe-se que a equação de segundo grau

$$x^2 + r_1 x + r_1^2 + a = 0$$

possui duas raízes r_2 e r_3, que podem ser obtidas pela *fórmula de Bháskara*, e

$$x^2 + r_1 x + r_1^2 + a = (x - r_2)(x - r_3). \tag{4.12}$$

Substituindo 4.12 em 4.11, obtém-se:

$$x^3 + ax + b = (x - r_1)(x - r_2)(x - r_3),$$

de onde segue que r_2 e r_3 são raízes de 4.10 (basta substituir x por r_2 ou r_3) e, portanto, a equação possui três raízes, que podem ou não serem distintas. □

Ainda no espírito de versões mais simples de resultados da álgebra abstrata, o segundo lema cobre mais um passo em direção à via principal do *Teorema da Raiz Construtível*.

Lema 9. Se uma equação cúbica reduzida tem uma raiz, então a soma de todas as suas raízes é igual a zero.

Demonstração. Pelo lema 8, se uma equação da forma 4.6 tem uma raiz, então essa equação tem 3 raízes r_1, r_2 e r_3 e, além disso,

$$x^3 + ax + b = (x - r_1)(x - r_2)(x - r_3). \tag{4.13}$$

Expandindo o segundo membro da igualdade acima, obtém-se:

$$\begin{aligned} x^3 + ax + b &= (x - r_1)(x^2 - r_2x - r_3x + r_2r_3) \\ &= x^3 - r_2x^2 - r_3x^2 + r_2r_3x - r_1x^2 + r_1r_2x + r_1r_3x - r_1r_2r_3 \\ &= x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_2r_3 + r_3r_1)x - r_1r_2r_3 \end{aligned}$$

Da igualdade de polinômios, segue que

$$-(r_1 + r_2 + r_3) = 0.$$

Portanto,

$$r_1 + r_2 + r_3 = 0,$$

ou seja, a soma de todas as raízes é igual a zero, como se queria provar. □

O terceiro e último lema relaciona equações cúbicas reduzidas de coeficientes inteiros com extensões quadráticas iteradas de $\mathbb{Q}$.

Lema 10. Considere uma equação cúbica reduzida com *coeficientes inteiros*:

$$x^3 + a_1x + a_0 = 0, \quad a_1, a_0 \in \mathbb{Z}. \tag{4.14}$$

Seja $a + b\sqrt{x_n}$, $b \neq 0$, um elemento qualquer de uma extensão quadrática iterada de $\mathbb{Q}$ tal que $a + b\sqrt{x_n}$ é uma raiz de 4.14. Então $a - b\sqrt{x_n}$ também é uma raiz de 4.14.

Demonstração. Seja $E_n = E_{n-1}(\sqrt{x_n})$ uma extensão quadrática iterada de $\mathbb{Q}$ arbitrária. Da definição 11, tem-se que $x_n \in E_{n-1}$, $x_n > 0$ e $\sqrt{x_n} \notin E_{n-1}$. Sejam a e b elementos arbitrários de E_{n-1} tais que $b \neq 0$ e $a + b\sqrt{x_n}$ é uma raiz da equação 4.14. Logo,

$$\left(a + b\sqrt{x_n}\right)^3 + a_1\left(a + b\sqrt{x_n}\right) + a_0 = 0. \tag{4.15}$$

Expandindo o binômio do primeiro membro da equação e reorganizando os termos, obtém-se:

$$\begin{aligned} &\left(a + b\sqrt{x_n}\right)^3 + a_1\left(a + b\sqrt{x_n}\right) + a_0 \\ &= a^3 + 3a^2b\sqrt{x_n} + 3ab^2x_n + b^3x_n\sqrt{x_n} + a_1a + a_1b\sqrt{x_n} + a_0 \\ &= \left(a^3 + 3ab^2x_n + a_1a + a_0\right) + \left(3a^2b + b^3x_n + a_1b\right)\sqrt{x_n} \end{aligned} \tag{4.16}$$

Defina $c \doteq a^3 + 3ab^2x_n + a_1a + a_0$ e $d \doteq 3a^2b + b^3x_n + a_1b$. Como $a_1, a_0 \in \mathbb{Z} \subseteq E_{n-1}$ e $a, b, x_n \in E_{n-1}$, segue que c e d são elementos de E_{n-1}, pois E_{n-1} é um corpo. Deste modo, segue de 4.15 e 4.16 que

$$c + d\sqrt{x_n} = 0. \tag{4.17}$$

Suponha que $d \neq 0$. Então, $\sqrt{x_n} = -\frac{c}{d}$, o que é um absurdo, pois $-\frac{c}{d}$ é um elemento de E_{n-1} e, por hipótese, $\sqrt{x_n} \notin E_{n-1}$. Portanto, $d = 0$. Segue de 4.17 que $c = 0$. Agora basta substituir $a - b\sqrt{x_n}$ no primeiro membro da equação 4.14 e efetuar os cálculos a seguir.

$$\begin{aligned}
&\left(a - b\sqrt{x_n}\right)^3 + a_1\left(a - b\sqrt{x_n}\right) + a_0 \\
&= a^3 - 3a^2b\sqrt{x_n} + 3ab^2x_n - b^3x_n\sqrt{x_n} + a_1a - a_1b\sqrt{x_n} + a_0 \\
&= \left(a^3 + 3ab^2x_n + a_1a + a_0\right) - \left(3a^2b + b^3x_n + a_1b\right)\sqrt{x_n} \\
&= c - d\sqrt{x_n} \\
&= 0
\end{aligned}$$

Portanto, $a - b\sqrt{x_n}$ também é raiz de 4.14, como se queria provar. □

Por fim, a caracterização dos números construtíveis feita no capítulo anterior e os três lemas acima serão usados para demonstrar o teorema a seguir, que mostra que determinadas equações cúbicas não possuem nenhuma raiz que é um número construtível.

Teorema 8 (Teorema da Raiz Construtível)**.** Considere uma equação cúbica reduzida com *coeficientes inteiros*:

$$x^3 + a_1x + a_0 = 0, \quad a_1, a_0 \in \mathbb{Z}. \tag{4.18}$$

Suponha que essa equação não tem nenhuma raiz racional. Então nenhum número construtível é uma raiz dessa equação.

Demonstração. Suponha por absurdo que existe um número construtível que é raiz de 4.18. Ou seja, pelo teorema 7, existe uma raiz de 4.18 que está em alguma extensão quadrática iterada de $\mathbb{Q}$. Seja n o menor índice tal que $E_n = E_{n-1}(\sqrt{x_n})$ contém uma raiz de 4.18. Note que $n \neq 0$, pois a equação 4.18 não tem nenhuma raiz racional, por hipótese. Tome então uma raiz $u \in E_n$ da equação 4.18. Logo, existem $a, b \in E_{n-1}$ tais que

$$u = a + b\sqrt{x_n}.$$

Note que $b \neq 0$. Caso contrário, se $b = 0$, então $u = a \in E_{n-1}$, o que é um absurdo, pois n é o menor índice de uma extensão que contém uma raiz de 4.18, por hipótese. Pelo lema 10, o número $v \doteq a - b\sqrt{x_n}$ também é uma raiz de 4.18. Pelo lema 8, existe uma terceira raiz w de 4.18 e, pelo lema 9, tem-se que $u + v + w = 0$. Logo,

$$\left(a + b\sqrt{x_n}\right) + \left(a - b\sqrt{x_n}\right) + w = 0.$$

Assim, $w = -2a$. Como E_{n-1} é um corpo, segue que $w \in E_{n-1}$, o que é um absurdo, pois por hipótese n é o menor índice de uma extensão quadrática iterada de $\mathbb{Q}$ que contém uma raiz de 4.18. Portanto, nenhum número construtível é raiz da equação 4.18. □

Com a proposição 9 e o teorema 8 em mãos, pode-se finalmente concluir as soluções da duplicação do cubo e da trissecção do ângulo, que serão feitas, respectivamente, nas seções 3 e 4 a seguir.

4.3 Duplicação do cubo

Através da via principal construída na seção anterior, o teorema a seguir retoma a discussão da primeira seção deste capítulo e mostra que é impossível duplicar o cubo unitário, concluindo assim o trajeto restante da solução da duplicação do cubo.

Teorema 9. Não é possível fazer a duplicação de um cubo de volume igual a 1 usando apenas régua e compasso.

Demonstração. Suponha por absurdo que é possível construir com régua e compasso um cubo cujo volume seja igual a 2. Então, pelo que foi explicado na seção 4.1, pode-se concluir que a equação cúbica

$$x^3 - 2 = 0 \tag{4.19}$$

tem uma raiz que é um número construtível. Porém, será provado agora que nenhum número construtível é raiz desta equação.

Primeiro, note que 4.19 é uma equação cúbica reduzida com coeficientes inteiros:

$$x^3 + a_1 x + a_0 = 0,$$

onde $a_1 = 0$ e $a_0 = -2$. Suponha que $\frac{p}{q}$ é uma raiz de 4.19, onde $p, q \in \mathbb{Z}$, $q \neq 0$ e $mdc(p,q) = 1$. Pela proposição 9, segue que:

(i) p é fator de -2, ou seja, $p \in \{-2, -1, 1, 2\}$;

(ii) $q = 1$ ou $q = -1$.

Assim, combinando as possibilidades de p e q, obtém-se que:

$$\frac{p}{q} \in \{-2, -1, 1, 2\}. \tag{4.20}$$

Ou seja, se a equação 4.19 tiver alguma raiz racional, então obrigatoriamente deve ser um dos valores acima. Então, agora basta testar se algum desses valores é raiz da equação, através da substituição de cada um deles na equação.

$$(-2)^3 - 2 = -8 - 2 = -10 \neq 0 \qquad 1^3 - 2 = 1 - 2 = -1 \neq 0$$
$$(-1)^3 - 2 = -1 - 2 = -3 \neq 0 \qquad 2^3 - 2 = 8 - 2 = 6 \neq 0$$

Logo, nenhum valor de 4.20 é raiz da equação 4.19 e, por consequência, esta equação não tem solução racional. Pelo teorema 8, nenhum número construtível é raiz da equação 4.19, o que é um absurdo. Portanto, não é possível construir um cubo cujo volume seja igual a 2 do modo desejado, ou seja, é impossível duplicar o cubo unitário usando apenas régua e compasso. □

Observação 7. Perceba que a medida da aresta do cubo de volume 2 é igual a $\sqrt[3]{2}$, embora isso não tenha sido explicitado. Assim, no fundo o que se queria provar, e foi provado, é que $\sqrt[3]{2}$ não é um número construtível, ou seja, é impossível construir com apenas régua e compasso um segmento de reta cuja medida seja igual a $\sqrt[3]{2}$.

O teorema acima conclui a solução do problema da duplicação do cubo, como já explicado anteriormente, pois a impossibilidade da duplicação do cubo unitário prova que nem todo cubo pode ser duplicado com apenas régua e compasso. Então podemos dizer com todas as palavras: *O problema da duplicação do cubo está resolvido sim! E sua solução mostra que é impossível duplicar todo cubo usando apenas régua e compasso!*

4.4 Trissecção do ângulo

De modo análogo ao que foi feito na duplicação do cubo, para provar que não se pode trissectar todo ângulo com régua e compasso, basta exibir um ângulo que não pode ser trissectado. Isso será feito através do teorema a seguir.

Teorema 10. Não é possível fazer a trissecção de um ângulo de medida igual a 60° usando apenas régua e compasso.

Demonstração. Considere um ângulo cuja medida seja igual a 60°. Suponha por absurdo que seja possível dividi-lo em três ângulos de mesma medida usando apenas régua e compasso. Isso implica que o ângulo de 20° é construtível, ou seja, pela definição 4, existem semirretas $\overrightarrow{AB}$ e $\overrightarrow{AC}$, onde A, B e C são pontos construtíveis, tais que $\widehat{BAC} = 20^\circ$. Chame de r a reta construtível que passa por A e B, e de s a reta construtível que passa por A e C. Trace a reta construtível t que passa por C e é perpendicular à reta s. Chame de D a interseção entre as retas r e t, que é portanto um ponto construtível. Essas construções estão ilustradas na figura 8. Pela figura, é fácil ver que

$$\cos 20^\circ = \frac{AC}{AD}.$$

Logo, $\cos 20^\circ$ é um número construtível, pois é o quociente de números construtíveis (AC e AD

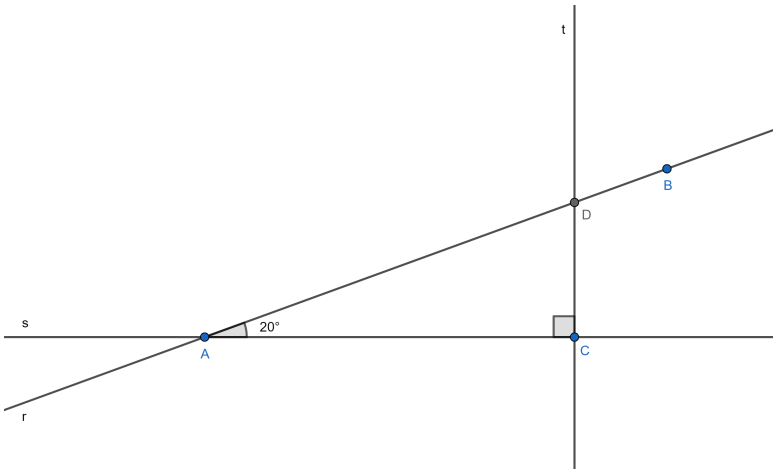


Figura 8 – Construção do cosseno do ângulo de 20°.

correspondem a distâncias entre pontos construtíveis). Defina então o seguinte número:

$$c \doteq 2\cos 20^\circ.$$

Note que c também é um número construtível, pois é o produto de números construtíveis. Além disso, como $60^\circ = 3 \cdot 20^\circ$, pela *fórmula do arco triplo* tem-se que

$$\cos 60^\circ = 4\cos^3 20^\circ - 3\cos 20^\circ.$$

Substituindo $\cos 60^\circ = \frac{1}{2}$ e $\cos 20^\circ = \frac{c}{2}$ na igualdade acima, obtém-se

$$4 \cdot \left(\frac{c}{2}\right)^3 - 3 \cdot \left(\frac{c}{2}\right) = \frac{1}{2},$$

de onde segue que

$$c^3 - 3c - 1 = 0.$$

Portanto, o número construtível c é raiz da seguinte equação cúbica:

$$x^3 - 3x - 1 = 0, \tag{4.21}$$

que será chamada de *equação de trissecção*. Entretanto, será provado agora que essa equação não tem raiz construtível, de modo análogo ao que foi feito para se mostrar a impossibilidade da duplicação do cubo.

Primeiro, note que 4.21 é uma equação cúbica reduzida com coeficientes inteiros:

$$x^3 + a_1 x + a_0 = 0,$$

onde $a_1 = -3$ e $a_0 = -1$. Suponha que $\frac{p}{q}$ é uma raiz de 4.21, onde $p, q \in \mathbb{Z}$, $q \neq 0$ e $mdc(p,q) = 1$. Pela proposição 9, segue que:

(i) p é fator de -1, ou seja, $p = 1$ ou $p = -1$;

(ii) $q = 1$ ou $q = -1$.

Assim, combinando as possibilidades de p e q, obtém-se que:

$$\frac{p}{q} \in \{-1, 1\}. \tag{4.22}$$

Ou seja, se a equação de trissecção tiver alguma raiz racional, então obrigatoriamente deve ser um dos valores acima. Então, agora basta substituir cada um desses valores na equação 4.21 para testar se algum deles é raiz da equação.

$$(-1)^3 - 3 \cdot (-1) - 1 = -1 + 3 - 1 = 1 \neq 0 \qquad 1^3 - 3 \cdot 1 - 1 = 1 - 3 - 1 = -3 \neq 0$$

Logo, nenhum valor de 4.22 é raiz da equação 4.21 e, por consequência, esta equação não tem solução racional. Pelo teorema 8, nenhum número construtível é raiz da equação de trissecção, o que é um absurdo. Portanto, não é possível construir um ângulo cuja medida seja igual a 20° do modo desejado, ou seja, é impossível trissectar um ângulo de 60° usando apenas régua e compasso. □

Observação 8. Perceba que foi provado que o número $\cos 20^\circ$ não é um número construtível, ou seja, não está em nenhuma extensão quadrática iterada de $\mathbb{Q}$.

O teorema acima conclui a solução do problema da trissecção do ângulo, como já explicado anteriormente, pois a impossibilidade da trissecção do ângulo de 60° prova que nem todo ângulo pode ser trissectado com apenas régua e compasso. Então também podemos dizer com todas as palavras: *O problema da trissecção do ângulo está resolvido sim! E sua solução mostra que é impossível trissectar todo ângulo usando apenas régua e compasso!* Vale salientar novamente que alguns ângulos podem ser trissectados com apenas régua e compasso, porém o que se está dizendo é que não existe um procedimento geral para fazer a trissecção de um ângulo arbitrário usando somente régua e compasso.

CAPÍTULO

5

ESPAÇOS VETORIAIS

A partir de agora o objetivo é resolver o problema da construção de polígonos regulares com apenas régua e compasso. Para isso será necessária uma teoria mais refinada e mais difícil do que a que foi usada para resolver a duplicação do cubo e a trissecção do ângulo. O modo de apresentar essa teoria segue de perto o que é feito em Kazarinoff (2003), com alguns acréscimos e adaptações pensados com o objetivo de facilitar a compreensão do professor de matemática do ensino básico. O tópico inicial nessa dura mas prazerosa (na maioria das vezes) e compensadora jornada será o conceito de *espaço vetorial*, que é uma estrutura algébrica que generaliza alguns aspectos de certos conjuntos com o objetivo de facilitar o estudo dos mesmos, assim como foi feito anteriormente quando da introdução do conceito de *corpo*. Neste capítulo, será apresentado o básico da teoria de espaços vetoriais necessário para resolver o problema da construção de polígonos regulares com régua e compasso.

5.1 O que é espaço vetorial?

Nesta seção, será apresentada a definição rigorosa de *espaço vetorial*, seguida de alguns exemplos que buscam ilustrar o conceito e dar uma ideia do tipo de conjuntos que são espaços vetoriais. Basicamente, o espaço vetorial é uma *estrutura algébrica*, ou seja, um conjunto dotado de operações que satisfazem certas propriedades. A ideia não é nova. No capítulo 3, foi apresentada a definição de *corpo*, que é uma estrutura algébrica que generaliza as propriedades das quatro operações básicas no conjunto dos números reais. Quando foi introduzido o conceito de corpo, partiu-se dos números reais para primeiro se ter uma ideia concreta do que se buscava tratar para então generalizar o conceito de forma mais abstrata, porque lá não se tinha nenhuma noção do que era uma estrutura algébrica e se buscava apresentar uma pela primeira vez. Porém, agora que já se tem uma ideia do assunto, será feita uma abordagem mais direta, como já mencionado. Primeiramente será feita a definição de maneira abstrata e só depois serão exibidos de modo breve alguns exemplos concretos de espaços vetoriais.

Definição 15. Seja F um corpo. Então, um conjunto não vazio V será dito um *espaço vetorial sobre F* quando for dotado de: uma operação entre quaisquer dois elementos do próprio conjunto, chamada de *adição*; e uma operação entre um elemento qualquer do corpo F e um elemento qualquer do conjunto V, chamada de *multiplicação por escalar*; operações essas que satisfazem as propriedades a seguir, onde u, v e w são elementos arbitrários de V, e α e β são elementos arbitrários de F.

1. $u+v \in V$ (fechamento da adição);
2. $u+(v+w) = (u+v)+w$ (associatividade da adição);
3. Existe um elemento $0 \in V$ tal que $u+0 = u$ (elemento neutro da adição);
4. Para cada u em V, existe um elemento $-u$ em V tal que $u+(-u) = 0$ (elemento inverso da adição);
5. $u+v = v+u$ (comutatividade da adição);
6. $\alpha \cdot u \in V$ (fechamento da multiplicação por escalar);
7. $\alpha \cdot (\beta \cdot u) = (\alpha\beta) \cdot u$ (associatividade da multiplicação por escalar);
8. $1 \cdot u = u$, onde 1 é o elemento neutro da multiplicação do corpo F (elemento neutro da multiplicação por escalar);
9. $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$ (distributividade da multiplicação por escalar com relação à adição em V);
10. $(\alpha+\beta) \cdot u = \alpha \cdot u + \beta \cdot u$ (distributividade da multiplicação por escalar com relação à adição em F).

No contexto de espaços vetoriais, os elementos de V são chamados de *vetores* e foram representados em negrito na definição acima, enquanto que os elementos de F são chamados de *escalares* e foram representados por letras do alfabeto grego. Em particular, o elemento neutro 0 da adição em V é chamado de *vetor nulo* e o elemento inverso $-u$ da adição em V é chamado de *vetor oposto de u*.

É importante diferenciar também as operações do corpo F e as operações do espaço vetorial, pois isso foi feito apenas pelo contexto e optou-se por não usar símbolos distintos para não poluir a escrita. Vale destacar que $\alpha+\beta$ e $\alpha \cdot \beta$ correspondem, respectivamente, à soma e ao produto de escalares, ou seja, representam as operações de adição e multiplicação do corpo F, pois α e β são elementos de F; enquanto que $u+v$ e $\alpha \cdot u$ correspondem, respectivamente, à soma de vetores e ao produto de escalar por vetor, ou seja, representam as operações de adição e multiplicação por escalar do espaço vetorial V, pois u e v são elementos de V, e α é um elemento

de F. Deste modo, deve-se atentar quando se trata de uma operação em V ou de uma operação em F, pois podem ser operações distintas, mesmo que aqui tenha se escolhido usar o mesmo símbolo para simplificar a escrita. Além disso, mesmo que não se use negrito ou letras do alfabeto grego, a distinção entre uma operação em V e uma operação em F ficará clara pelo contexto. E quando houver ambiguidade, será esclarecido de qual operação se trata. Por fim, assim como é comum escrever $\alpha\beta$ ao invés de $\alpha \cdot \beta$, por abreviação, muitas vezes se escreve αu no lugar de $\alpha \cdot u$.

De modo análogo, é importante diferenciar o elemento neutro da adição em F e o elemento neutro da adição em V, apesar de que, neste caso, além do contexto, também foram usados símbolos "diferentes" (um deles apenas foi escrito em negrito). Mas vale destacar que o símbolo 0 corresponde ao *escalar* zero, ou seja, representa o elemento neutro da adição entre escalares do corpo F; enquanto que o símbolo 0 corresponde ao *vetor* nulo, ou seja, representa o elemento neutro da adição entre vetores do espaço vetorial V. Deste modo, deve-se atentar quando se trata do escalar zero ou do vetor nulo, pois podem ser elementos distintos em alguns espaços vetoriais. Além disso, analogamente ao que foi dito sobre as operações, mesmo que não seja usado o destaque em negrito e os dois elementos sejam representados pelo mesmo símbolo 0, a distinção entre o escalar zero e o vetor nulo ficará clara pelo contexto. E quando houver ambiguidade, será esclarecido de qual elemento neutro se trata.

É fácil provar que o elemento neutro da adição em V é único e por isso a sua notação como 0 e também o seu nome *vetor nulo* estão bem definidos, no sentido em que não há problemas em identificar um único objeto com uma única representação e um único nome (o que não daria para fazer com dois objetos distintos e uma única representação). De fato, supondo a existência de outro elemento neutro $0' \in V$, obtém-se que $0' = 0' + 0 = 0 + 0' = 0$, ou seja, $0' = 0$, o que mostra que a suposta existência de "outro" elemento neutro da adição implica no fato de que o "outro" vetor é, na realidade, o vetor "que já se tinha", i.e., existe um único vetor nulo.

De modo análogo, para cada $u \in V$, o elemento inverso da adição em V é único e por isso a sua notação como $-u$ e também o seu nome *vetor oposto de* $-u$ estão bem definidos. De fato, supondo a existência de dois elementos inversos u_1 e u_2 de u, obtém-se que $u_1 = u_1 + 0 = u_1 + (u + u_2) = (u_1 + u) + u_2 = 0 + u_2 = u_2$, ou seja, $u_1 = u_2$, o que mostra que a suposta existência de "dois" elementos inversos da adição para determinado vetor implica no fato de que os "dois" vetores são, na realidade, o mesmo vetor, i.e., existe um único vetor oposto de u.

Também é fácil provar que o produto do escalar 0 por qualquer vetor é igual ao vetor nulo, ou seja, $0 \cdot u = 0$ para todo $u \in V$; e, de modo análogo, o produto de qualquer escalar pelo vetor nulo é igual ao vetor nulo, ou seja, $\alpha \cdot 0 = 0$ para todo $\alpha \in F$.

Há várias outras propriedades usadas frequentemente que não são difíceis de provar, como por exemplo leis de cancelamento e tantas outras. Enfim, o fato é que com os poucos axiomas de um espaço vetorial se pode deduzir muitas propriedades elementares que são tão

comuns e tão rotineiras que às vezes nem se percebe que estão sendo usadas em espaços vetoriais específicos que nem mesmo se sabia que eram espaços vetoriais. E essa é uma ótima deixa para elencar alguns exemplos concretos de espaços vetoriais que, além de fornecerem uma ideia mais clara de quais estruturas são espaços vetoriais, também darão uma noção melhor de todas as propriedades elementares que já se conhece (mesmo que inconscientemente) e que podem ser usadas na manipulação de escalares e vetores sem a necessidade de se fazer aqui uma lista de várias páginas com todas elas.

Exemplo 4. Existem muitos exemplos de espaços vetoriais frequentes, mas talvez o mais conhecido seja aquele formado pelos pontos de $\mathbb{R}^2$:

$$\mathbb{R}^2 = \{(x,y) \mid x,y \in \mathbb{R}\}.$$

Juntamente com as operações de adição e multiplicação por escalar definidas, respectivamente, por $(x_1,y_1)+(x_2,y_2) = (x_1+x_2, y_1+y_2)$ e $\alpha(x,y) = (\alpha x, \alpha y)$, onde $\alpha \in \mathbb{R}$, $V = \mathbb{R}^2$ é um espaço vetorial sobre $\mathbb{R}$, o que não é difícil de provar. Note que o vetor nulo de $\mathbb{R}^2$ é o elemento $(0,0)$, enquanto que o elemento neutro da adição em $\mathbb{R}$ é o número 0.

Exemplo 5. Seja $V = P_1(\mathbb{R})$ o conjunto formado por todos os polinômios de grau menor ou igual a 1 com coeficientes reais. Juntamente com as operações usuais de adição de polinômios e multiplicação de um número real por um polinômio, V é um espaço vetorial sobre $\mathbb{R}$, o que também é fácil de demonstrar. Note que o vetor nulo de $P_1(\mathbb{R})$ é o polinômio identicamente nulo $p(x) \equiv 0$.

Exemplo 6. Um exemplo de espaço vetorial bem importante neste trabalho é a extensão quadrática $\mathbb{Q}(\sqrt{2})$. Juntamente com as operações de adição e multiplicação por escalar definidas, respectivamente, por $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2}) = (a_1+a_2)+(b_1+b_2)\sqrt{2}$ e $\alpha(a+b\sqrt{2}) = \alpha a + \alpha b\sqrt{2}$, onde $\alpha \in \mathbb{Q}$, $V = \mathbb{Q}(\sqrt{2})$ é um espaço vetorial sobre $\mathbb{Q}$. Note que o vetor nulo de $\mathbb{Q}(\sqrt{2})$ é o número $0 = 0+0\cdot\sqrt{2}$, ou seja, neste caso o vetor nulo coincide com o elemento neutro da adição em $\mathbb{Q}$. De modo análogo, qualquer extensão quadrática de $\mathbb{Q}$ é um espaço vetorial sobre $\mathbb{Q}$. E mais geralmente ainda, se V é uma extensão quadrática $F(\sqrt{x})$ de um corpo F, então V é um espaço vetorial sobre F, de onde segue que qualquer extensão quadrática iterada E_n de $\mathbb{Q}$ é um espaço vetorial sobre E_{n-1}, para todo número natural n.

Ao observar os exemplos acima, fica claro o quão útil é a generalização do conceito de espaço vetorial. Com apenas uma estrutura algébrica, é possível concentrar os estudos na mesma e deduzir várias propriedades mais facilmente, que poderão ser usadas para todos os exemplos anteriores e vários outros de uma só vez, e isso evita muita repetição e cálculos desnecessários. Além disso, o terceiro exemplo já dá um gostinho do porquê há um interesse particular em espaços vetoriais neste trabalho.

5.2 Dependência linear e independência linear

Nesta seção são apresentados alguns subconjuntos especiais de um espaço vetorial necessários para desenvolver o conceito de dimensão de um espaço vetorial que será visto na próxima seção.

Definição 16. Seja V um espaço vetorial sobre um corpo F. Um conjunto finito de vetores $\{u_1,...,u_n\}$ em V é *linearmente dependente sobre F* se, e somente se, existem escalares $\alpha_1,...,\alpha_n$, não todos nulos (i.e., pelo menos um deles é diferente de zero), tais que

$$\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0.$$

Se não existirem tais escalares, o conjunto $\{u_1,...,u_n\}$ é *linearmente independente sobre F*, ou seja, neste caso, qualquer igualdade $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0$ implica que todos os escalares são iguais a zero, i.e., $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$.

Por praticidade, será comum dizer que "os vetores $u_1,...,u_n$ são linearmente dependentes (ou independentes) sobre F" com o significado de que o conjunto $\{u_1,...,u_n\}$ é linearmente dependente (ou independente) sobre F. E por economia, muitas vezes a escrita da expressão *linearmente dependente (ou linearmente independente) sobre F* será abreviada como *LD (ou LI) sobre F*. Além disso, quando não houver ambiguidade, a expressão "sobre F" pode ser omitida ao se falar em conjuntos linearmente dependentes ou independentes, a menos que seja necessário especificar sobre qual corpo o espaço vetorial está sendo considerado.

Exemplo 7. Seja $V = \mathbb{R}^2$ o espaço vetorial sobre $\mathbb{R}$ descrito no exemplo 4. O conjunto $\{(1,1),(2,2)\}$ é LD sobre $\mathbb{R}$, porque existem os números reais 2 e -1 tais que

$$2\cdot(1,1) + (-1)\cdot(2,2) = (0,0).$$

Por outro lado, o conjunto $\{(1,0),(0,1)\}$ é LI sobre $\mathbb{R}$, pois se existem escalares $\alpha,\beta \in \mathbb{R}$ tais que

$$\alpha\cdot(1,0) + \beta\cdot(0,1) = (0,0),$$

então $(\alpha,\beta) = (0,0)$, de onde segue que $\alpha = \beta = 0$.

Exemplo 8. Seja $V = P_1(\mathbb{R})$ o espaço vetorial sobre $\mathbb{R}$ descrito no exemplo 5. O conjunto $\{x\}$ é LI sobre $\mathbb{R}$, porque, se $a\cdot x = 0$, então $a = 0$. O conjunto $\{1,x\}$ também é LI sobre $\mathbb{R}$, pois se existem escalares $a,b \in \mathbb{R}$ tais que

$$a\cdot 1 + b\cdot x = 0,$$

então segue da igualdade de polinômios que $a = b = 0$. Por outro lado, o conjunto $\{1,x,5x+3\}$ é LD sobre $\mathbb{R}$, porque existem os números reais -3, -5 e 1 tais que

$$(-3)\cdot 1 + (-5)\cdot x + 1\cdot(5x+3) = 0.$$

Exemplo 9. Seja $V = \mathbb{Q}(\sqrt{2})$ o espaço vetorial sobre $\mathbb{Q}$ descrito no exemplo 6. O conjunto $\{1, \sqrt{2}\}$ é LI sobre $\mathbb{Q}$. De fato, sejam $a, b \in \mathbb{Q}$ tais que

$$a \cdot 1 + b \cdot \sqrt{2} = 0. \tag{5.1}$$

Suponha por absurdo que $b \neq 0$. Então, isolando $\sqrt{2}$ no primeiro membro da igualdade acima, obtém-se que

$$\sqrt{2} = -\frac{a}{b},$$

o que é um absurdo, porque, como $\mathbb{Q}$ é um corpo, $-\frac{a}{b} \in \mathbb{Q}$, mas $\sqrt{2}$ não é um número racional. Logo, $b = 0$. Substituindo $b = 0$ na igualdade 5.1, segue que $a = 0$. Portanto, a igualdade $a \cdot 1 + b \cdot \sqrt{2} = 0$ implica que $a = b = 0$, o que mostra que $\{1, \sqrt{2}\}$ é LI, pela definição.

Para finalizar esta seção, será provado um teorema que apresenta uma caracterização de dependência linear necessária para as demonstrações de alguns resultados importantes ao longo deste e do próximo capítulo. Antes porém, é definido o conceito de *combinação linear*.

Definição 17. Sejam V um espaço vetorial sobre F e $u_1, ..., u_n$ vetores em V. Então $u \in V$ é uma *combinação linear sobre F de $u_1, ..., u_n$* se, e somente se, existem escalares $\alpha_1, ..., \alpha_n \in F$ tais que

$$u = \alpha_1 u_1 + ... + \alpha_n u_n.$$

Observação 9. Note que, na definição acima, *não* há exigência sobre os escalares serem não todos nulos, ou seja, pode acontecer de todos serem iguais a zero e continua sendo uma combinação linear. Porém, perceba que, se u é uma combinação linear de $u_1, ..., u_n$, então

$$1 \cdot u - \alpha_1 u_1 - ... - \alpha_n u_n = 0.$$

Portanto, como pelo menos o coeficiente de u é diferente de zero, segue da igualdade acima que o conjunto $\{u, u_1, ..., u_n\}$ é LD sobre F.

Teorema 11 (Caracterização de Dependência Linear)**.** Seja $\{u_1, ..., u_n\}$ um conjunto finito de vetores não nulos em um espaço vetorial V sobre F tal que $n \geq 2$, ou seja, há pelo menos dois vetores no conjunto. Então, o conjunto $\{u_1, ..., u_n\}$ é LD sobre F se, e somente se, existe um inteiro k, $2 \leq k \leq n$, tal que u_k é uma combinação linear sobre F de $u_1, ..., u_{k-1}$.

Demonstração. Por um lado, suponha que existe um inteiro k, $2 \leq k \leq n$, tal que u_k é uma combinação linear sobre F de $u_1, ..., u_{k-1}$. Ou seja, existem escalares $\alpha_1, ..., \alpha_{k-1} \in F$ tais que

$$u_k = \alpha_1 u_1 + ... + \alpha_{k-1} u_{k-1}.$$

Logo,

$$\alpha_1 u_1 + ... + \alpha_{k-1} u_{k-1} - u_k = 0. \tag{5.2}$$

Há dois casos a serem considerados: (i) $k < n$ e (ii) $k = n$.

(i) Se $k < n$, segue de 5.2 que

$$\alpha_1 u_1 + ... + \alpha_{k-1} u_{k-1} + (-1) \cdot u_k + 0 \cdot u_{k+1} + ... + 0 \cdot u_n = 0.$$

(ii) Se $k = n$, segue de 5.2 que

$$\alpha_1 u_1 + ... + \alpha_{k-1} u_{k-1} + (-1) \cdot u_n = 0.$$

Portanto, seja qual for o caso, perceba que existem escalares $\alpha_1, ..., \alpha_n \in F$, não todos nulos pois $a_k = -1$, tais que $\alpha_1 u_1 + ... + \alpha_n u_n = 0$, ou seja, o conjunto $\{u_1, ..., u_n\}$ é LD sobre F, pela definição.

Por outro lado, suponha que o conjunto $\{u_1, ..., u_n\}$ é LD sobre F, ou seja, existem escalares $\alpha_1, ..., \alpha_n \in F$, não todos nulos, tais que

$$\alpha_1 u_1 + ... + \alpha_n u_n = 0. \tag{5.3}$$

Seja $k \leq n$ o maior índice tal que $\alpha_k \neq 0$. Suponha por absurdo que $k = 1$, ou seja, $\alpha_2 = ... = \alpha_n = 0$. Logo, segue de 5.3 que $\alpha_1 u_1 = 0$, o que implica em $u_1 = 0$, que é um absurdo, pois todos os vetores $u_1, ..., u_n$ são não nulos, por hipótese. Portanto, $2 \leq k \leq n$.

Além disso, como $\alpha_{k+1} = ... = \alpha_n = 0$, segue de 5.3 que

$$\alpha_1 u_1 + ... + \alpha_k u_k = 0.$$

Então, isolando u_k no primeiro membro da igualdade acima, obtém-se:

$$u_k = -\frac{\alpha_1}{\alpha_k} u_1 - \frac{\alpha_2}{\alpha_k} u_2 - ... - \frac{\alpha_{k-1}}{\alpha_k} u_{k-1}.$$

Note que $-\dfrac{\alpha_i}{\alpha_k} \in F$, para todo $i \in \{1, ..., k-1\}$, pois F é corpo e $\alpha_1, ..., \alpha_k \in F$. Portanto, u_k é uma combinação linear sobre F de $u_1, ..., u_{k-1}$, onde $2 \leq k \leq n$, como se queria demonstrar. □

5.3 Bases e dimensão

O que foi feito nas seções anteriores permite chegar em um conceito chave para a solução do problema de construção de polígonos regulares com régua e compasso, que é o conceito de *dimensão de um espaço vetorial*. Para definir o que é *dimensão*, primeiro é necessário definir o que é uma *base*.

Definição 18. Seja V um espaço vetorial sobre F. Uma *base finita para* V é um conjunto finito $B = \{u_1, ..., u_n\}$ de vetores em V que satisfaz as duas propriedades a seguir:

(i) B é LI sobre F; e

(ii) qualquer vetor é uma combinação linear sobre F dos elementos de B.

Observação 10. Neste trabalho, serão estudados apenas espaços vetoriais com bases finitas, por isso será dito apenas *base* ao invés de *base finita*.

Note que o conceito de base apresenta duas características fundamentais. Por um lado, é um conjunto a partir do qual todo elemento de V pode ser obtido. Por outro lado, por ser um conjunto LI, segue do teorema 11 que nenhum vetor de B é combinação linear de outros elementos da base. Assim, esses dois aspectos juntos garantem que a base apresenta a quantidade mínima de vetores necessária para obter a partir dos mesmos todos os elementos do espaço vetorial V. Essa quantidade mínima de vetores que produzem todo o espaço vetorial será chamada de *dimensão de* V. Ou seja, a dimensão de um espaço vetorial será igual ao número de vetores de uma base para V, porém, para este conceito ficar bem definido, é necessário assegurar antes que qualquer base possui o mesmo número de elementos. Do contrário, se duas bases distintas para V possuíssem quantidades diferentes de elementos, não haveria como definir um único número para ser a dimensão do espaço vetorial V.

O teorema a seguir garante que duas bases quaisquer para V possuem o mesmo número de elementos. E isso implica que, se uma determinada base para V possui n elementos, então toda base para V também possui n elementos. A demonstração deste teorema será omitida.

Teorema 12. Seja V um espaço vetorial sobre F. Se $B = \{u_1, ..., u_m\}$ e $C = \{v_1, ..., v_n\}$ são bases para V, então $m = n$, i.e., as duas bases possuem o mesmo número de elementos.

Definição 19. Um espaço vetorial V tem *dimensão finita* se, e somente se, possui uma base finita. Nesse caso, a *dimensão de* V é igual ao número de elementos de uma base para este espaço vetorial.

Sendo assim, o conceito de dimensão de um espaço vetorial de dimensão finita está bem definido, pois todas as bases possuem o mesmo número de elementos, pelo teorema 12. A seguir são apresentados alguns exemplos.

Exemplo 10. O conjunto $B = \{(1,0),(0,1)\}$ é uma base para o espaço vetorial $\mathbb{R}^2$ sobre $\mathbb{R}$. No exemplo 7 foi provado que B é LI sobre $\mathbb{R}$. Então só falta mostrar que qualquer vetor de $\mathbb{R}^2$ é uma combinação linear de $(1,0)$ e $(0,1)$, mas isso é fácil, pois se (a,b) é um elemento qualquer de $\mathbb{R}^2$, então

$$(a,b) = a\cdot(1,0) + b\cdot(0,1),$$

onde $a,b \in \mathbb{R}$. Portanto, $\mathbb{R}^2$ é um espaço vetorial de dimensão 2.

Exemplo 11. No exemplo 8 foi provado que $\{x\}$ é um conjunto LI em $P_1(\mathbb{R})$, porém nem todo elemento de $P_1(\mathbb{R})$ é uma combinação linear de x. Por exemplo, se $p(x) \equiv 1$, não existe nenhum número real a tal que $1 = a\cdot x$. Isso mostra que $\{x\}$ não é uma base para $P_1(\mathbb{R})$. Por outro lado, qualquer elemento $p(x) \equiv ax+b$ de $P_1(\mathbb{R})$ é uma combinação linear de 1, x e $5x+3$. De fato:

$$ax+b = a\cdot x + b\cdot 1 + 0\cdot(5x+3).$$

Porém, foi provado no exemplo 8 que $\{1,x,5x+3\}$ é um conjunto LD em $P_1(\mathbb{R})$ e, portanto, não é uma base para este espaço vetorial.

Os exemplos dos dois conjuntos $\{x\}$ e $\{1,x,5x+3\}$ mostram que os conceitos de independência linear e combinação linear para qualquer vetor do espaço vetorial não vêm sempre acompanhados, ou seja, um pode ocorrer sem que o outro ocorra. Além disso, tais exemplos mostram que, para ser uma base para o espaço vetorial, um conjunto deve satisfazer obrigatoriamente os dois requisitos, o que ocorre com o conjunto $B = \{x,1\}$ em $P_1(\mathbb{R})$. De fato, foi provado no exemplo 8 que B é LI sobre $\mathbb{R}$, e é fácil mostrar que qualquer elemento $p(x) \equiv ax+b$ em $P_1(\mathbb{R})$ é uma combinação linear de x e 1:

$$ax+b = a\cdot x + b\cdot 1,$$

onde $a,b \in \mathbb{R}$. Logo, $B = \{x,1\}$ é uma base para $P_1(\mathbb{R})$, que tem, portanto, dimensão 2.

Exemplo 12. O conjunto $B = \{1,\sqrt{2}\}$ é uma base para o espaço vetorial $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. De fato, no exemplo 9 foi provado que B é LI sobre $\mathbb{Q}$ e, além disso, é fácil ver que qualquer elemento $a+b\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$ é uma combinação linear de 1 e $\sqrt{2}$:

$$a+b\sqrt{2} = a\cdot 1 + b\cdot\sqrt{2},$$

onde $a,b \in \mathbb{Q}$. Portanto, $\mathbb{Q}(\sqrt{2})$ é um espaço vetorial de dimensão 2.

Ao estudar este último exemplo, surge uma vontade de generalizar a conclusão acima para toda extensão quadrática de $\mathbb{Q}$. Na próxima seção, será apresentado algo ainda mais geral:

uma base finita para cada extensão quadrática iterada de $\mathbb{Q}$ vista como um espaço vetorial sobre $\mathbb{Q}$.

5.4 Extensões quadráticas iteradas como espaços vetoriais sobre os racionais

Uma vez apresentado o básico da teoria sobre espaços vetoriais de dimensão finita necessária para este trabalho, é possível caracterizar toda extensão quadrática iterada de $\mathbb{Q}$ como um espaço vetorial de dimensão finita. Isso será feito através do teorema a seguir, que é o objetivo desta seção e a conclusão deste capítulo sobre espaços vetoriais.

Teorema 13. Seja E_n uma extensão quadrática iterada de $\mathbb{Q}$ arbitrária, para algum número natural n. Então E_n é um espaço vetorial sobre $\mathbb{Q}$ de dimensão 2^n.

Demonstração. Em primeiro lugar, é trivial que qualquer extensão quadrática iterada E_n é um espaço vetorial sobre $\mathbb{Q}$, para todo natural n. De fato, a adição de vetores em E_n e a multiplicação por escalar são, respectivamente, a adição e a multiplicação usuais dos números reais, que claramente são operações que satisfazem todos os axiomas de espaço vetorial, inclusive os fechamentos das operações, visto que $u+v \in E_n$ e $\alpha u \in E_n$, para todos u e v em E_n, e todo α em $\mathbb{Q}$, pois E_n é um corpo e $\mathbb{Q} \subseteq E_n$.

Em segundo lugar, para mostrar que o espaço vetorial E_n sobre $\mathbb{Q}$ tem dimensão finita igual a 2^n será feita uma prova por indução sobre n. Para isso, defina o seguinte conjunto:

$$X = \{n \in \mathbb{N} \mid E_n \text{ tem dimensão } 2^n\} \subseteq \mathbb{N}.$$

Será provado que esse subconjunto dos naturais possui as duas propriedades a seguir:

(I) $1 \in X$;

(II) Se $n \in X$, então $n+1 \in X$.

Pelo que foi visto na seção anterior, para mostrar que um espaço vetorial tem dimensão finita m, basta exibir uma base finita B para este espaço vetorial tal que B tenha m elementos.

(I) Como já fazem alguns capítulos que as extensões quadráticas iteradas de $\mathbb{Q}$ foram apresentadas, vale lembrar que, por definição,

$$E_1 = E_0(\sqrt{x_1}) = \mathbb{Q}(\sqrt{x_1}) = \left\{ a + b\sqrt{x_1} \;\middle|\; a,b \in \mathbb{Q} \right\},$$

para algum $x_1 \in \mathbb{Q}$ tal que $x_1 > 0$ e $\sqrt{x_1} \notin \mathbb{Q}$. Será provado que o conjunto finito

$$B \doteq \{1, \sqrt{x_1}\}$$

é uma base para E_1 em duas partes (i) e (ii).

(i) O conjunto B é LI sobre $\mathbb{Q}$. De fato, sejam $a,b \in \mathbb{Q}$ tais que

$$a \cdot 1 + b \cdot \sqrt{x_1} = 0. \tag{5.4}$$

Suponha por absurdo que $b \neq 0$. Então, isolando $\sqrt{x_1}$ no primeiro membro da igualdade acima, obtém-se que

$$\sqrt{x_1} = -\frac{a}{b},$$

o que é um absurdo, porque, como $\mathbb{Q}$ é um corpo, $-\frac{a}{b} \in \mathbb{Q}$, mas, pela definição de E_1, $\sqrt{x_1} \notin \mathbb{Q}$. Logo, $b = 0$. Substituindo $b = 0$ na igualdade 5.4, segue que $a = 0$. Portanto, a igualdade $a \cdot 1 + b \cdot \sqrt{x_1} = 0$ implica que $a = b = 0$, ou seja, B é LI sobre $\mathbb{Q}$, como se queria mostrar.

A demonstração de que B é LI sobre $\mathbb{Q}$ soou familiar, porque isso já foi feito no exemplo 9 para o caso particular em que $x_1 = 2$. Essa repetição foi elaborada para que o leitor tivesse um exemplo concreto mais fácil de entender. Deste modo, ao estudar esta parte mais abstrata, o mundo não parece tão estranho e tão distante.

(ii) É trivial que qualquer elemento $a + b\sqrt{x_1}$ de $\mathbb{Q}(\sqrt{x_1})$ é uma combinação linear de 1 e $\sqrt{x_1}$ sobre $\mathbb{Q}$:

$$a + b\sqrt{x_1} = a \cdot 1 + b \cdot \sqrt{x_1},$$

onde $a,b \in \mathbb{Q}$, o que também já foi feito no exemplo 12 para o caso particular em que $x_1 = 2$.

Logo, segue de (i) e (ii) que $B = \left\{1, \sqrt{x_1}\right\}$ é uma base para E_1. Portanto, o espaço vetorial E_1 sobre $\mathbb{Q}$ tem dimensão 2, que é igual a 2^1, ou seja, $1 \in X$, o que conclui a demonstração da propriedade (I).

(II) Suponha que $n \in X$, ou seja, E_n tem dimensão 2^n. Será provado que $n+1 \in X$. Pela definição de extensão quadrática iterada de $\mathbb{Q}$, tem-se que

$$E_{n+1} = E_n(\sqrt{x_{n+1}}) = \left\{ a + b\sqrt{x_{n+1}} \;\middle|\; a,b \in E_n \right\},$$

para algum $x_{n+1} \in E_n$ tal que $x_{n+1} > 0$ e $\sqrt{x_{n+1}} \notin E_n$. Para a simbologia não ficar tão carregada, x_{n+1} será denotado simplesmente por x.

Da hipótese de indução, segue que existe um subconjunto finito A de E_n com 2^n elementos que é uma base para o espaço vetorial E_n sobre $\mathbb{Q}$. Os 2^n elementos da base A serão denotados assim:

$$A \doteq \{e_1, e_2, ..., e_{2^n}\},$$

onde $e_i \in E_n$, para todo $i \in \{1,2,...,2^n\}$. A partir dos elementos de A, defina o seguinte conjunto:

$$B \doteq \left\{e_1, e_2, ..., e_{2^n},\ \ e_1\sqrt{x}, e_2\sqrt{x}, ..., e_{2^n}\sqrt{x}\right\}.$$

Perceba que B é um subconjunto finito de E_{n+1}, pois E_{n+1} é corpo, $\sqrt{x} \in E_{n+1}$ e $e_i \in E_n \subseteq E_{n+1}$, para todo $i \in \{1,2,...,2^n\}$. Além disso, note que B tem o dobro do número de elementos de A, ou seja, B possui $2 \cdot 2^n = 2^{n+1}$ elementos. Afirma-se: o conjunto B é uma base para o espaço vetorial E_{n+1} sobre $\mathbb{Q}$. A demonstração dessa afirmação será feita em duas etapas (i) e (ii).

(i) O conjunto B é LI sobre $\mathbb{Q}$. De fato, suponha que existam 2^{n+1} escalares

$$a_1, a_2, ..., a_{2^n}, \;\; b_1, b_2, ..., b_{2^n} \in \mathbb{Q}$$

tais que

$$a_1e_1 + a_2e_2 + ... + a_{2^n}e_{2^n} \;\; + \;\; b_1\left(e_1\sqrt{x}\right) + b_2\left(e_2\sqrt{x}\right) + ... + b_{2^n}\left(e_{2^n}\sqrt{x}\right) = 0. \tag{5.5}$$

Usando as propriedades associativa e distributiva, obtém-se:

$$\left(a_1e_1 + a_2e_2 + ... + a_{2^n}e_{2^n}\right) \;\; + \;\; \left(b_1e_1 + b_2e_2 + ... + b_{2^n}e_{2^n}\right)\sqrt{x} = 0. \tag{5.6}$$

A partir da igualdade acima, defina:

$$a \doteq a_1e_1 + a_2e_2 + ... + a_{2^n}e_{2^n} \quad \text{e} \quad b \doteq b_1e_1 + b_2e_2 + ... + b_{2^n}e_{2^n}.$$

Perceba que a e b são elementos de E_n, pois E_n é corpo, $e_i \in E_n$ e $a_i, b_i \in \mathbb{Q} \subseteq E_n$, para todo $i \in \{1,2,...,2^n\}$. Deste modo, a igualdade 5.6 pode ser reescrita como

$$a + b\sqrt{x} = 0, \tag{5.7}$$

onde $a, b \in E_n$. Suponha por absurdo que $b \neq 0$. Então, isolando $\sqrt{x}$ no primeiro membro da igualdade acima, obtém-se que

$$\sqrt{x} = -\frac{a}{b},$$

o que é um absurdo, porque, como E_n é um corpo, $-\frac{a}{b} \in E_n$, mas, pela definição de E_{n+1}, $\sqrt{x} = \sqrt{x_{n+1}} \notin E_n$. Logo, $b = 0$. Substituindo $b = 0$ na igualdade 5.7, segue que $a = 0$. Das definições de a e b, tem-se então que

$$a_1e_1 + a_2e_2 + ... + a_{2^n}e_{2^n} = 0 \quad \text{e} \quad b_1e_1 + b_2e_2 + ... + b_{2^n}e_{2^n} = 0.$$

Como A é uma base para E_n, tem-se que A é um conjunto LI sobre $\mathbb{Q}$ e, por isso, as duas igualdades acima implicam, respectivamente, que

$$a_1 = a_2 = ... = a_{2^n} = 0 \quad \text{e} \quad b_1 = b_2 = ... = b_{2^n} = 0.$$

Portanto, a igualdade 5.5 implica que

$$a_1 = ... = a_{2^n} \;\; = \;\; b_1 = ... = b_{2^n} = 0,$$

ou seja, B é LI sobre $\mathbb{Q}$, como se queria mostrar.

Novamente, note que a processo acima pareceu familiar, porque a parte em que se prova que $a = b = 0$ é análoga à respectiva parte da etapa (i) da propriedade (I).

(ii) Qualquer elemento de E_{n+1} é uma combinação linear sobre $\mathbb{Q}$ dos elementos de B. Para mostrar isso, seja $u = a + b\sqrt{x}$ um elemento arbitrário de E_{n+1}, onde $a, b \in E_n$. Todo elemento de E_n é uma combinação linear sobre $\mathbb{Q}$ dos elementos de A, pois A é uma base para E_n. Sendo assim, existem escalares

$$a_1, a_2, ..., a_{2^n} \in \mathbb{Q} \quad \text{e} \quad b_1, b_2, ..., b_{2^n} \in \mathbb{Q}$$

tais que

$$a = a_1e_1 + a_2e_2 + ... + a_{2^n}e_{2^n} \quad \text{e} \quad b = b_1e_1 + b_2e_2 + ... + b_{2^n}e_{2^n}.$$

Deste modo, u pode ser reescrito como

$$u = (a_1e_1 + a_2e_2 + ... + a_{2^n}e_{2^n}) \ + \ (b_1e_1 + b_2e_2 + ... + b_{2^n}e_{2^n})\sqrt{x}.$$

Usando as propriedades distributiva e associativa, obtém-se:

$$u = a_1e_1 + a_2e_2 + ... + a_{2^n}e_{2^n} \ + \ b_1\left(e_1\sqrt{x}\right) + b_2\left(e_2\sqrt{x}\right) + ... + b_{2^n}\left(e_{2^n}\sqrt{x}\right),$$

ou seja, u é uma combinação linear sobre $\mathbb{Q}$ dos elementos de B, como se queria provar.

Logo, segue de (i) e (ii) que B é uma base para E_{n+1}. Portanto, o espaço vetorial E_{n+1} sobre $\mathbb{Q}$ tem dimensão 2^{n+1}, ou seja, $n+1 \in X$, o que conclui a demonstração da propriedade (II).

Assim, pelo *Princípio da Indução Finita*, segue das propriedades (I) e (II) acima provadas que $X = \mathbb{N}$. Portanto, qualquer extensão quadrática iterada E_n de $\mathbb{Q}$ é um espaço vetorial de dimensão 2^n, para todo número natural n. □

Observação 11. Note que o teorema acima foi provado para qualquer extensão quadrática iterada E_n de $\mathbb{Q}$ de índice n natural, ou seja, $n \geq 1$. E lembre-se que $E_0 = \mathbb{Q}$, por definição. O teorema também vale para $n = 0$, pois é claro que $\mathbb{Q}$ é um espaço vetorial sobre si mesmo e, além disso, $\{1\}$ é uma base para $\mathbb{Q}$. De fato, se $a \in \mathbb{Q}$ e $a \cdot 1 = 0$, então $a = 0$, o que mostra que $\{1\}$ é LI sobre $\mathbb{Q}$; além disso, é trivial que qualquer número racional a é uma combinação linear de 1 sobre $\mathbb{Q}$, pois $a = a \cdot 1$, e $a \in \mathbb{Q}$. Portanto, $E_0 = \mathbb{Q}$ é um espaço vetorial sobre $\mathbb{Q}$ de dimensão 1. Por fim, como $2^0 = 1$, pode-se dizer que E_0 tem dimensão 2^0, ou seja, o teorema vale para $n = 0$, como se queria demonstrar.

O caso $n = 0$ poderia ser incluído diretamente no enunciado e na demonstração do teorema acima. Porém, foi uma escolha não incluir 0 como primeiro valor de n, porque, enquanto que é trivial a demonstração de que $\{1\}$ é base para E_0, a demonstração do caso $n = 1$ no processo de indução fornece um representante para o primeiro valor que melhor ilustra a ideia

da demonstração para o caso geral de modo simples e intuitivo. Uma vez que se entende o caso particular $n = 1$, a demonstração do caso mais geral pode ser melhor visualizada e compreendida. Espera-se que assim, com este passo a passo que começou lá atrás no exemplo 6, a conclusão tenha sido mais natural e aceitável e, quem sabe, bonita e elegante aos olhos do leitor.

O teorema apenas provado já fornece uma ideia boa do porquê foi necessário apresentar aqui o conceito de espaço vetorial de dimensão finita, mas o seu propósito ficará ainda mais claro ao ser usado para provar um critério para decidir se determinados números reais *podem ou não* serem números construtíveis. Esse critério é o grande objetivo do próximo capítulo e será a conclusão final da álgebra necessária para resolver os problemas de construção com régua e compasso.

CAPÍTULO

6

CORPOS ALGÉBRICOS

Após muito trabalho, este é o capítulo que finaliza toda a teoria de álgebra necessária para a solução dos problemas de construção com régua e compasso. É um capítulo com desfecho emocionante pois reúne todos os conceitos e teoremas construídos ao longo de vários capítulos em um belo resultado final. Aqui serão estudadas extensões de corpo de $\mathbb{Q}$ mais gerais do que as extensões quadráticas iteradas de $\mathbb{Q}$, que são as *extensões algébricas de* $\mathbb{Q}$. Os números reais podem ser divididos em dois tipos de números que serão definidos a seguir na primeira seção deste capítulo: *números algébricos* e *números transcendentes*.

6.1 Números algébricos, Fatoração e Irredutibilidade

Definição 20. Um número real u é *algébrico* se, e somente se, u é uma raiz de alguma equação polinomial com coeficientes racionais, isto é, existem números $a_0, a_1, ..., a_n \in \mathbb{Q}$, $a_n \neq 0$, $n \geq 1$, tais que

$$a_0 + a_1 u + ... + a_n u^n = 0.$$

Um número real u é *transcendente* se, e somente se, u não é algébrico.

Um bom exemplo de número algébrico é o número $\sqrt{2}$ e um bom exemplo de número transcendente é o número π. Porém, é uma tarefa um tanto avançada e difícil provar que π é transcendente. É claro que todos os números racionais são algébricos, mas os números irracionais podem ser algébricos, como $\sqrt{2}$, ou transcendentes, como π.

Mas o que os números algébricos têm a ver com os problemas de construção com régua e compasso? Primeiro perceba que todo elemento $a + b\sqrt{d}$ de uma extensão quadrática $\mathbb{Q}(\sqrt{d})$ é um número algébrico, pois é uma raiz da equação

$$x^2 - 2ax - b^2 d + a^2 = 0.$$

Também é possível provar que todo elemento de qualquer extensão quadrática iterada de $\mathbb{Q}$ é algébrico, mas isso não será usado neste trabalho, então não há necessidade de apresentar uma demonstração neste momento. Ou seja, *todos os números construtíveis são algébricos*, o que faz sentido pois, como foi visto no capítulo 2, os números construtíveis são exatamente aqueles que se originam de equações polinomiais cujos coeficientes são números construtíveis, ou seja, é um processo recursivo que têm início com números construtíveis iniciais que são números racionais.

Porém, o que realmente será importante para a solução dos problemas de construção é a *relação* existente entre as raízes de certas equações polinomiais e os elementos das extensões quadráticas iteradas de $\mathbb{Q}$. O interesse nessa relação não é novidade. Basta lembrar do modo como a relação entre as equações cúbicas e as extensões quadráticas iteradas de $\mathbb{Q}$ foi usada para resolver a duplicação do cubo e a trissecção do ângulo. Inclusive, vale a pena retomar a equação da duplicação para fazer uma analogia e fornecer uma motivação para o estudo que será conduzido neste capítulo. Como foi visto, se fosse possível duplicar o cubo unitário, existiria um número construtível que é raiz da equação cúbica

$$x^3 - 2 = 0.$$

Um modo de encontrar uma raiz dessa equação é tentar *fatorar* o polinômio $x^3 - 2$ em um produto de polinômios de grau 1 e grau 2 com coeficientes racionais, porque, se uma fatoração assim fosse possível, existiriam números racionais a, b, c, d, e, com $-\dfrac{b}{a} > 0$, tais que

$$x^3 - 2 = (ax + b)(cx^2 + dx + e), \tag{6.1}$$

e então $-\dfrac{b}{a}$ seria uma raiz racional positiva da equação $x^3 - 2 = 0$, ou seja, haveria um número construtível positivo cujo cubo é igual a 2, e assim o problema da duplicação do cubo unitário com régua e compasso estaria resolvido. De modo alternativo, se $\Delta = d^2 - 4ce \geq 0$, as raízes de $cx^2 + dx + e = 0$ também são números construtíveis, pois

$$x = \frac{-d \pm \sqrt{\Delta}}{2c},$$

o que também forneceria uma solução para duplicar o cubo unitário com apenas régua e compasso.

No entanto, foi provado no capítulo 4 que a equação $x^3 - 2 = 0$ não tem raiz racional e, portanto, o polinômio $x^3 - 2$ não pode ser fatorado como em 6.1. Então, de modo implícito, essa impossibilidade de fatorar $x^3 - 2$ em polinômios com coeficientes racionais foi o segredo para mostrar que o cubo unitário não pode ser duplicado com régua e compasso. Essa tal impossibilidade tão fundamental de fatorar $x^3 - 2$ como em 6.1 é traduzida através do conceito de *irredutibilidade* de um polinômio: será dito que o polinômio $x^3 - 2$ é *irredutível sobre* $\mathbb{Q}$.

Este exemplo tão próximo e tão prático mostra de modo claro como surgem os conceitos de *fatoração* e *irredutibilidade* no estudo das construções geométricas com régua e compasso, e

porque essas ideias são fundamentais para a solução de tais problemas. Com isso, tem-se uma forte motivação para se mergulhar no estudo desses tópicos.

Para começar, será dito que um polinômio com coeficientes racionais é um polinômio *sobre* $\mathbb{Q}$. Todos os polinômios que serão estudados aqui são polinômios sobre $\mathbb{Q}$, então frequentemente essa informação será omitida.

Um polinômio $d(x)$ é um *divisor* (*fator*) de um polinômio $p(x)$ sobre $\mathbb{Q}$ se, e somente se, $d(x)$ tem coeficientes racionais e existe um polinômio $q(x)$ sobre $\mathbb{Q}$ tal que

$$d(x)q(x) \equiv p(x).$$

Nessa mesma situação, pode-se dizer também que $p(x)$ é um *múltiplo* de $d(x)$.

Um divisor de um polinômio $p(x)$ é um *divisor impróprio* se for um número racional $a \neq 0$ ou um múltiplo não nulo $ap(x)$ de $p(x)$, pois, para qualquer polinômio $p(x)$, tem-se que

$$a \cdot \left[\frac{1}{a}p(x)\right] \equiv p(x) \quad \text{e} \quad [ap(x)] \cdot \frac{1}{a} \equiv p(x),$$

onde $a \in \mathbb{Q}$ e $a \neq 0$. Os divisores de $p(x)$ que não são impróprios são chamados de *divisores próprios*.

Definição 21. Um polinômio sobre $\mathbb{Q}$ é *irredutível sobre* $\mathbb{Q}$ se, e somente se, todos os seus divisores são impróprios. Um polinômio sobre $\mathbb{Q}$ é *redutível sobre* $\mathbb{Q}$ se, e somente se, possui divisores próprios.

Definição 22. Um polinômio é *mônico* se, e somente se, o coeficiente do seu termo de maior grau é igual a 1. Assim, o polinômio

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

é um polinõmio mônico de grau n (se $n = 0$, então $a_0 = 1$).

Para fornecer uma lista finita de divisores de um polinômio, a convenção adotada é listar apenas divisores próprios que sejam mônicos. Do contrário, haveria infinitos divisores a serem listados, pois, se $d(x)$ é um divisor de $p(x)$, então $ad(x)$ também é um divisor de $p(x)$, onde $a \in \mathbb{Q}$ e $a \neq 0$.

Em seguida será definido o *mdc* de dois polinômios sobre $\mathbb{Q}$ arbitrários.

Definição 23. Sejam $a(x)$ e $b(x)$ dois polinômios sobre $\mathbb{Q}$. Um polinômio mônico $d(x)$ é um *máximo divisor comum* de $a(x)$ e $b(x)$ se as duas condições a seguir forem satisfeitas:

(i) $d(x)$ é um divisor de $a(x)$ e de $b(x)$;

(ii) se $c(x)$ é um divisor de $a(x)$ e de $b(x)$, então $c(x)$ é um divisor de $d(x)$.

A seguir serão apresentados três teoremas sobre divisão e fatoração de polinômios que correspondem a propriedades conhecidas da divisão e fatoração de números inteiros. Sendo assim, não são resultados difíceis de acreditar. Tais teoremas consistem em propriedades básicas de polinômios e suas demonstrações serão omitidas, pois fogem dos objetivos deste trabalho.

Teorema 14 (Algoritmo da divisão para polinômios)**.** Sejam $a(x)$ e $b(x)$ polinômios arbitrários, com $b(x) \neq 0$. Então existem únicos polinômios $q(x)$ e $r(x)$ tais que

$$a(x) \equiv b(x)q(x) + r(x), \tag{6.2}$$

onde $r(x)$ é o polinômio nulo ou é um polinômio com grau menor do que o grau de $b(x)$.

Os polinômios $q(x)$ e $r(x)$ são chamados, respectivamente, de *quociente* e *resto* da divisão de $a(x)$ por $b(x)$.

Teorema 15 (Teorema de Bézout)**.** Sejam $a(x)$ e $b(x)$ polinômios não nulos. Então *existe um único mdc* $d(x)$ de $a(x)$ e $b(x)$. Além disso, existem polinômios $s(x)$ e $t(x)$ tais que

$$d(x) \equiv s(x)a(x) + t(x)b(x). \tag{6.3}$$

Teorema 16 (Fatoração única para polinômios)**.** Todo polinômio não nulo $p(x)$ pode ser fatorado de modo único como um produto de um número diferente de zero vezes um produto de polinômios mônicos irredutíveis.

Uma vez que se tem o algoritmo da divisão para polinômios, fica fácil provar a proposição abaixo, conhecida como *teste da raiz*, porém, como tudo aqui nesta parte de polinômios, a sua demonstração será omitida.

Proposição 10 (Teste da raiz)**.** Seja $p(x)$ um polinômio não nulo. Então: $p(\alpha) = 0$ se, e somente se, $p(x) = (x - \alpha)q(x)$, para algum polinômio $q(x)$.

Por fim, para finalizar esta primeira seção, será apresentado um critério de irredutibilidade, que é bem famoso por ser muito fácil de aplicar.

Teorema 17 (Critério de Eisenstein)**.** Seja $p(x)$ um polinômio de grau $n \geq 2$ com coeficientes inteiros. Suponha que existe um número primo q tal que

(i) todo coeficiente de $p(x)$ é divisível por q, exceto o coeficiente de x^n; e

(ii) o termo constante de $p(x)$ não é divisível por q^2.

Então $p(x)$ é irredutível sobre $\mathbb{Q}$.

Embora o *Critério de Eisenstein* não seja um resultado nada intuitivo e tampouco fácil de acreditar, a sua demonstração será omitida. Em suma, toda a teoria necessária sobre polinômios será aceita e usada livremente, pois seu desenvolvimento e suas demonstrações fogem dos objetivos desta dissertação. Assim, sem poluir o texto com as demonstrações dos resultados sobre polinômios, essa segunda parte do trabalho, rumo à solução do problema de construção de polígonos regulares, ficará mais curta, o que tornará o caminho mais claro ao leitor.

Como exemplo de aplicação do *Critério de Eisenstein*, vale a pena retomar a equação polinomial $x^3 - 2 = 0$ da duplicação do cubo, que foi usada como exemplo no início desta seção. Considerando o polinômio $p(x) = x^3 - 2$ e o número primo $q = 2$, é fácil perceber que: o coeficiente 1 não é divisível por 2; e o coeficiente -2 é divisível por 2, mas não é divisível por $2^2 = 4$. Portanto, pelo *Critério de Eisenstein*, o polinômio $x^3 - 2$ é irredutível sobre $\mathbb{Q}$, algo que já havia sido mencionado, mas que só agora está definido e provado de modo rigoroso.

Do mesmo modo que a chave para resolver o problema da duplicação do cubo foi uma equação cúbica envolvendo implicitamente um polinômio irredutível, o segredo para resolver o problema da construção de polígonos regulares também será equações polinomiais desse tipo. Assim sendo, com todas essas definições e todos esses resultados sobre polinômios em mãos, o objetivo agora é estudar a relação entre equações polinomiais da forma $p(x) = 0$, onde $p(x)$ é um polinômio irredutível sobre $\mathbb{Q}$, e os elementos das extensões quadráticas iteradas de $\mathbb{Q}$. Na seção a seguir, são dados os primeiros passos em direção a esse objetivo.

6.2 Corpos algébricos

No início da seção anterior foram definidos os números algébricos e então as coisas caminharam de modo natural em direção às equações polinomiais da forma $p(x) = 0$, onde $p(x)$ é um polinômio irredutível sobre $\mathbb{Q}$. Agora, o primeiro resultado desta seção mostra como os conceitos de número algébrico e polinômio irredutível se entrelaçam.

Teorema 18. Se um número real u é algébrico, então existe um único polinômio mônico irredutível $p(x)$ sobre $\mathbb{Q}$ tal que $p(u) = 0$.

Além disso, se $f(x)$ é um polinômio sobre $\mathbb{Q}$ e $f(u) = 0$, então $f(x)$ é um múltiplo de $p(x)$. Reciprocamente, se $f(x)$ é um múltiplo de $p(x)$, então $f(u) = 0$.

Demonstração. Seja u um número real algébrico. Pela definição de número algébrico, existe pelo menos um polinômio $a(x)$ sobre $\mathbb{Q}$ com grau maior ou igual a 1 tal que $a(u) = 0$. Pelo teorema 16, $a(x)$ pode ser fatorado de modo único como:

$$a(x) = c \cdot p_1(x) \cdot \ldots \cdot p_m(x),$$

onde $c \in \mathbb{Q}$, $c \neq 0$ e $p_i(x)$ é um polinômio mônico irredutível, para todo $i \in \{1, \ldots, m\}$. Como $a(u) = 0$, segue que

$$c \cdot p_1(u) \cdot \ldots \cdot p_m(u) = 0.$$

Logo, existe pelo menos um valor de $i \in \{1, \ldots, m\}$ tal que $p_i(u) = 0$, pois $c \neq 0$. Ou seja, existe pelo menos um polinômio mônico irredutível sobre $\mathbb{Q}$, que será denotado por $p(x)$, tal que $p(u) = 0$.

Acima só foi provada a existência de $p(x)$. Para mostrar que $p(x)$ é único, será necessário provar antes a segunda parte do teorema, e então a mesma será utilizada para demonstrar a unicidade.

Suponha que o grau de $p(x)$ é n. Se um polinômio $b(x)$ sobre $\mathbb{Q}$ tiver grau menor do que n, então $b(u)$ não pode ser zero. De fato, seja $b(x)$ um polinômio sobre $\mathbb{Q}$ de grau menor do que n. Então, como $p(x)$ é irredutível, segue que o *mdc* de $b(x)$ e $p(x)$ é igual a 1. Logo, pelo teorema 15, existem polinômios $s(x)$ e $t(x)$ tais que

$$1 \equiv s(x)b(x) + t(x)p(x).$$

Substituindo $x = u$ na igualdade acima, obtém-se:

$$1 = s(u)b(u) + t(u)p(u).$$

Mas como $p(u) = 0$, segue que

$$s(u)b(u) = 1,$$

e portanto $b(u)$ não pode ser igual a zero, como se queria mostrar. Com este fato será possível demonstrar a segunda parte do teorema.

Seja $f(x)$ um polinômio sobre $\mathbb{Q}$ tal que $f(u) = 0$. Fazendo a divisão de $f(x)$ por $p(x)$, sabe-se pelo teorema 14 que existem únicos polinômios $q(x)$ e $r(x)$ sobre $\mathbb{Q}$ tais que

$$f(x) \equiv p(x)q(x) + r(x), \tag{6.4}$$

onde $r(x)$ é o polinômio nulo ou é um polinômio com grau menor do que n, que é o grau de $p(x)$. Substituindo $x = u$ na igualdade acima, obtém-se:

$$f(u) = p(u)q(u) + r(u).$$

Como $p(u) = 0$ e $f(u) = 0$, segue que

$$r(u) = 0.$$

Deste modo, conclui-se que $r(x)$ é obrigatoriamente o polinômio nulo, pois, caso contrário, pelo que foi provado no parágrafo anterior, $r(u)$ não poderia ser igual a zero, pois o grau de $r(x)$ seria menor do que n. Portanto, substituindo $r(x) \equiv 0$ em 6.4, segue que

$$f(x) \equiv p(x)q(x),$$

ou seja, $f(x)$ é um múltiplo de $p(x)$.

A recíproca é trivial, pois é claro que, se $f(x) \equiv p(x)q(x)$ é um múltiplo de $p(x)$, para algum polinômio $q(x)$ sobre $\mathbb{Q}$, então

$$f(u) = p(u)q(u) = 0 \cdot q(u) = 0,$$

ou seja, $f(u) = 0$, como se queria mostrar.

Para finalizar a demonstração do teorema, basta provar a unicidade do polinômio $p(x)$. Para isso, suponha que $p^*(x)$ seja outro polinômio mônico irredutível sobre $\mathbb{Q}$ tal que $p^*(x) = 0$. Então, pelo que foi provado acima, $p^*(x)$ é um múltiplo de $p(x)$, i.e.,

$$p^*(x) \equiv p(x)q(x),$$

para algum polinômio $q(x)$ sobre $\mathbb{Q}$. Supondo que $q(x)$ não é uma constante, conclui-se que $p^*(x)$ tem divisores próprios, o que é um absurdo, pois $p^*(x)$ é irredutível; logo, $q(x) \equiv a$, para algum $a \in \mathbb{Q}$. Supondo que $a \neq 1$, conclui-se que $p^*(x) = ap(x)$ não é mônico, o que é um absurdo; logo, $a = 1$. Portanto, $p^*(x) = p(x)$, ou seja, $p(x)$ é único, como se queria demonstrar. □

Agora será definido um importante conceito, que constitui um segundo passo em direção ao objetivo de estabelecer uma relação entre as raízes de certas equações polinomiais e as extensões quadráticas iteradas de $\mathbb{Q}$.

Definição 24. O *grau* de um número algébrico u é o grau do único polinômio mônico irredutível *determinado por* u, i.e., do polinômio mônico irredutível $p(x)$ tal que $p(u) = 0$.

Corolário 4. Seja u um número algébrico de grau n. Se existem números $c_0, c_1, ..., c_{n-1} \in \mathbb{Q}$ tais que $c_0 + c_1 u + ... + c_{n-1} u^{n-1} = 0$, então $c_0 = c_1 = ... = c_{n-1} = 0$.

Demonstração. Basta definir $b(x) \equiv c_0 + c_1 x + ... + c_{n-1} x^{n-1}$ e então perceber que $b(x)$ é um polinômio sobre $\mathbb{Q}$ de grau menor do que n tal que $b(u) = 0$. Portanto, pelo que foi feito na demonstração do teorema acima, $b(x)$ é identicamente nulo, i.e., $c_0 = c_1 = ... = c_{n-1} = 0$, como se queria mostrar. □

Com o que foi feito até agora, é possível mostrar que cada número algébrico *determina* um corpo de números reais, e isso será feito através do teorema a seguir.

Teorema 19. Se $u \in \mathbb{R}$ é um número algébrico, então o subconjunto de $\mathbb{R}$ definido por

$$\mathscr{F}(u) = \{f(u) \mid f(x) \text{ é um polinômio sobre } \mathbb{Q}\},$$

juntamente com as operações usuais dos números reais, formam um corpo.

Demonstração. Basta provar que $\mathscr{F}(u)$ é um subcorpo de $\mathbb{R}$ através das condições de (i) a (v) da proposição 6. Sejam $f(u)$ e $g(u)$ elementos arbitrários de $\mathscr{F}(u)$, i.e., $f(x)$ e $g(x)$ são polinômios sobre $\mathbb{Q}$.

(i) $f(u) + g(u) = (f+g)(u)$ e $(f+g)(x)$ é um polinômio sobre $\mathbb{Q}$. Logo, a soma de dois elementos quaisquer de está em $\mathscr{F}(u)$.

(ii) $-f(u) = (-f)(u)$ e $-f(x)$ é um polinômio sobre $\mathbb{Q}$. Logo, o inverso aditivo de um elemento qualquer está em $\mathscr{F}(u)$.

(iii) $f(u)g(u) = (fg)(u)$ e $(fg)(x)$ é um polinômio sobre $\mathbb{Q}$. Logo, o produto de dois elementos quaisquer está em $\mathscr{F}(u)$.

(iv) $1 = 1 \cdot u^0 = h(u)$, onde $h(x) \equiv 1$ é um polinômio sobre $\mathbb{Q}$. Logo, $1 \in \mathscr{F}(u)$.

(v) Suponha que $f(u) \neq 0$. Se $p(x)$ é o único polinômio mônico irredutível tal que $p(u) = 0$, então, pelo teorema 18, $f(x)$ não é um múltiplo de $p(x)$ e, portanto, o *mdc* de $f(x)$ e $g(x)$ é 1. Logo, pelo teorema 15, existem polinômios $s(x)$ e $t(x)$ sobre $\mathbb{Q}$ tais que

$$1 \equiv s(x)f(x) + t(x)p(x).$$

Substituindo $x = u$ na igualdade acima, obtém-se

$$1 = s(u)f(u) + t(u)p(u).$$

Mas como $p(u) = 0$, segue que

$$s(u)f(u) = 1,$$

i.e., $s(u) = f(u)^{-1}$, pela definição de inverso multiplicativo. Como $s(x)$ é um polinômio sobre $\mathbb{Q}$, segue que o inverso multiplicativo de um elemento qualquer está em $\mathscr{F}(u)$.

Pela proposição 6, segue de (i), (ii), (iii), (iv) e (v) que $\mathscr{F}(u)$ é um subcorpo de $\mathbb{R}$ e, portanto, é um corpo com as operações usuais dos números reais. □

Com isso, pode-se definir finalmente o conceito que dá título a este capítulo!

Definição 25. Será dito que o corpo $\mathscr{F}(u)$ é *gerado por u*. Além disso, um *corpo algébrico* é um corpo gerado por algum número algébrico.

Antes de caminhar para a última seção deste capítulo é necessário definir mais um conceito importante, o que será feito na seção a seguir.

6.3 Grau de um corpo algébrico

O objetivo desta seção é definir um conceito chave para a solução do problema de construção de polígonos regulares, que é o *grau de um corpo algébrico*. A ideia é simples: o grau de um corpo algébrico $\mathscr{F}(u)$ será o grau do número algébrico u que o gera. Porém, como sempre, para que este conceito esteja bem definido, alguns cuidados são necessários, cuidados esses que começam com a demonstração do teorema a seguir.

Teorema 20. Seja u um número algébrico de grau n. Então, o corpo algébrico $\mathscr{F}(u)$ é um espaço vetorial sobre $\mathbb{Q}$ de dimensão n.

Demonstração. Sejam u um número algébrico e $p(x)$ o polinômio mônico irredutível unicamente determinado por u. Seja n o grau de $p(x)$. É trivial que $\mathscr{F}(u)$ é um espaço vetorial sobre $\mathbb{Q}$. De fato, a adição de vetores em $\mathscr{F}(u)$ é a adição usual de números reais e a multiplicação por escalar é a multiplicação usual de números reais, que claramente são operações que satisfazem todos os axiomas de espaço vetorial, inclusive os fechamentos das operações, visto que $f(u)+g(u) = (f+g)(u)$ e $\alpha f(u) = (\alpha f)(u)$, $\alpha \in \mathbb{Q}$, são elementos de $\mathscr{F}(u)$, porque $f(x)+g(x)$ e $\alpha f(x)$ são polinômios sobre $\mathbb{Q}$.

Para mostrar que $\mathscr{F}(u)$ tem dimensão n, será provado agora que $B = \left\{1, u, u^2, ..., u^{n-1}\right\}$ é uma base para $\mathscr{F}(u)$. Já se tem que B é LI sobre $\mathbb{Q}$, pois, se $c_0, c_1, ..., c_{n-1}$ são números racionais tais que

$$c_0 \cdot 1 + c_1 \cdot u + ... + c_{n-1} \cdot u^{n-1} = 0,$$

então, pelo corolário 4, $c_0 = c_1 = ... = c_{n-1} = 0$. Para completar a demonstração, basta mostrar que qualquer elemento de $\mathscr{F}(u)$ é uma combinação linear sobre $\mathbb{Q}$ dos elementos de B.

Seja $f(u)$ um elemento qualquer de $\mathscr{F}(u)$. Como $f(x)$ é um polinômio sobre $\mathbb{Q}$, segue do teorema 14 que existem únicos polinômios $q(x)$ e $r(x)$ sobre $\mathbb{Q}$ tais que

$$f(x) \equiv p(x) \cdot q(x) + r(x),$$

onde $r(x) \equiv 0$ ou o grau de $r(x)$ é menor do que n. Substituindo $x = u$, obtém-se:

$$f(u) = r(u),$$

pois $p(u) = 0$. Como $r(x)$ tem grau menor do que n, existem números racionais $c_{n-1}, ..., c_1, c_0$ tais que $r(x) = c_{n-1}x^{n-1} + ... + c_1 + c_0$ e, portanto, $r(u)$ é da forma

$$r(u) = c_{n-1}u^{n-1} + ... + c_1 u + c_0.$$

Logo, de $f(u) = r(u)$ segue que

$$f(u) = c_{n-1}u^{n-1} + ... + c_1 u + c_0,$$

ou seja, $f(u)$ é uma combinação linear sobre $\mathbb{Q}$ dos elementos de B.

Portanto, $B = \{1, u, u^2, ..., u^{n-1}\}$ é uma base para $\mathscr{F}(u)$ e, como B tem n elementos, segue que o espaço vetorial $\mathscr{F}(u)$ sobre $\mathbb{Q}$ tem dimensão n. □

Agora vai ficar claro como o teorema acima vai ajudar nos cuidados necessários para que o *grau* de um corpo algébrico esteja bem definido. Suponha que dois números algébricos diferentes u e v gerem o mesmo corpo algébrico $\mathscr{F} \doteq \mathscr{F}(u) = \mathscr{F}(v)$. Neste caso, o grau de $\mathscr{F}$ que se busca definir rigorosamente será o grau de u ou o grau de v? Suponha que o grau de u seja n e o grau de v seja m. Pelo teorema acima, os conjuntos

$$B = \{1, u, u^2, ..., u^{n-1}\} \quad \text{e} \quad C = \{1, v, v^2, ..., v^{m-1}\}$$

são bases para o espaço vetorial $\mathscr{F}$. Porém, pelo teorema 12, as duas bases têm o mesmo número de elementos. Portanto, $n = m$, i.e., o grau de u é igual ao grau de v. Isso mostra que é possível definir o grau de $\mathscr{F}$ como sendo o grau de u e o grau de v, porque são iguais.

Assim, a conclusão é que, qualquer que seja o número algébrico u que gera um corpo algébrico $\mathscr{F} = \mathscr{F}(u)$, o grau de u não muda e, portanto, a definição a seguir pode ser enunciada rigorosamente sem problemas, e o conceito de grau de um corpo algébrico ficará bem definido.

Definição 26. O *grau* de um corpo algébrico $\mathscr{F}(u)$ é o grau do número algébrico u que o gera.

Com o conceito de grau de um corpo algébrico em mãos, pode-se caminhar para a última seção deste capítulo, que finalizará a teoria de álgebra necessária para a solução dos problemas de construção com régua e compasso.

6.4 Extensão quadrática iterada como espaço vetorial sobre um corpo algébrico

Como já foi comentado na primeira seção deste capítulo, todos os números construtíveis são algébricos, mas este fato não é necessário para este trabalho e então não será usado, pois assim não é preciso prová-lo. Entretanto, nem todo número algébrico é construtível, e um exemplo óbvio é o número $\sqrt[3]{2}$, que é uma raiz da equação $x^3 - 2 = 0$ e portanto é algébrico, mas não é construtível, como foi provado no capítulo 4.

O objetivo desta seção, que é no fundo o grande propósito deste capítulo, é construir um critério para decidir se um dado número algébrico *pode ou não* ser um número construtível. Para o desenvolvimento deste critério, os conceitos de extensão quadrática iterada de $\mathbb{Q}$, corpo algébrico e espaço vetorial de dimensão finita serão todos usados em conjunto, o que é algo extremamente satisfatório, pois reúne e assim dá sentido às três grandes estruturas construídas com muito trabalho ao longo de vários capítulos desta dissertação. Além disso, após arquitetar tantos conceitos algébricos, esse critério finalmente colocará um ponto final na bela teoria matemática aqui desenhada para resolver os problemas de construção com régua e compasso.

Seja então um número algébrico u de grau m. Busca-se decidir se *u pode ou não* ser construtível. Para isso, suponha que u é um número construtível. Então u está em alguma extensão quadrática iterada E_k de $\mathbb{Q}$. Além disso, como u é algébrico, é claro que u também está no corpo algébrico $\mathscr{F}(u)$ gerado por ele. Ou seja, se u é um número algébrico construtível, há dois grandes corpos relacionados a ele que o contêm: $\mathscr{F}(u)$ e E_k (para algum inteiro $k \geq 0$).

Note que, como $u \in E_k$, toda combinação linear

$$c_{m-1}u^{m-1} + ... + c_1u + c_0,$$

onde $c_{m-1}, ..., c_1, c_0 \in \mathbb{Q}$, está em E_k, pois E_k é um corpo e $\mathbb{Q} \subseteq E_k$. Ou seja, qualquer elemento $f(u)$ de $\mathscr{F}(u)$ está em E_k. Logo, tem-se o seguinte:

$$\mathbb{Q} \subseteq \mathscr{F}(u) \subseteq E_k.$$

Já foi visto que $\mathscr{F}(u)$ e E_k são *espaços vetoriais sobre* $\mathbb{Q}$. Mais ainda, foi provado que a dimensão de $\mathscr{F}(u)$ *sobre* $\mathbb{Q}$ é m e a dimensão de E_k *sobre* $\mathbb{Q}$ é 2^k. Acontece que E_k também pode ser visto como um *espaço vetorial sobre* $\mathscr{F}(u)$, que tem dimensão finita, e isso será mostrado através do lema a seguir. Com este lema será possível enunciar e provar uma condição necessária (mas não suficiente) para o número algébrico u ser um número construtível, e essa condição determinará o critério para decidir se um dado número algébrico *pode ou não* ser um número construtível.

Lema 11. Seja u um número algébrico e suponha que u é construtível, i.e., u está em uma extensão quadrática iterada E_k de $\mathbb{Q}$, para algum inteiro $k \geq 0$. Então E_k é um espaço vetorial sobre $\mathscr{F}(u)$ de dimensão finita.

Demonstração. Sejam u um número algébrico e $\mathscr{F}(u)$ o corpo algébrico gerado por u. Suponha que u é construtível. Então, pelo teorema 7, u está em uma extensão quadrática iterada E_k de $\mathbb{Q}$, para algum número inteiro $k \geq 0$.

Pelo teorema 13, sabe-se que E_k é um espaço vetorial sobre $\mathbb{Q}$ de dimensão finita. É fácil ver que E_k também é um espaço vetorial sobre $\mathscr{F}(u)$. A adição de vetores em E_k sobre $\mathscr{F}(u)$ continua sendo a mesma de E_k sobre $\mathbb{Q}$, então trivialmente satisfaz os axiomas de espaço vetorial. Já a multiplicação por escalar agora é a multiplicação usual de $\mathbb{R}$ entre um escalar $f(u) \in \mathscr{F}(u)$ e um vetor $v \in E_k$, que claramente também satisfaz os axiomas de espaço vetorial, inclusive o fechamento da multiplicação por escalar, visto que $f(u) \cdot v \in E_k$, para todo $f(u) \in \mathscr{F}(u)$ e todo $v \in E_k$, pois $\mathscr{F}(u) \subseteq E_k$ e E_k é um corpo.

Além disso, também pelo teorema 13, sabe-se que a dimensão do espaço vetorial E_k sobre $\mathbb{Q}$ é igual a 2^k. Logo, existe um subconjunto finito $A \subseteq E_k$, com 2^k elementos, tal que A é uma base para E_k. Os elementos de A podem ser assim representados:

$$A \doteq \{e_1, ..., e_{2^k}\}.$$

Como A é uma base para E_k *sobre* $\mathbb{Q}$, segue da definição de base que A é LI *sobre* $\mathbb{Q}$ e qualquer elemento de E_k é uma combinação linear *sobre* $\mathbb{Q}$ dos elementos de A. Há duas possibilidades para o conjunto A:

(I) A é LI *sobre* $\mathscr{F}(u)$; ou

(II) A é LD *sobre* $\mathscr{F}(u)$.

É óbvio que uma coisa ou outra acontece, pela própria definição de conjuntos linearmente dependentes e independentes. Os casos (I) e (II) serão analisados separadamente: o objetivo é provar que em ambos os casos o espaço vetorial E_k sobre $\mathscr{F}(u)$ tem dimensão finita.

Caso (I): Suponha que A é LI *sobre* $\mathscr{F}(u)$. Neste caso, basta tomar $B \doteq A$. Será provado que B é uma base para o espaço vetorial E_k *sobre* $\mathscr{F}(u)$ em duas etapas (i) e (ii).

(i) É trivial que B é LI sobre $\mathscr{F}(u)$, pela hipótese do caso (I).

(ii) Qualquer elemento de E_k é combinação linear sobre $\mathscr{F}(u)$ dos elementos de B. Para mostrar isso, considere um elemento arbitrário $v \in E_k$. Todo elemento de E_k é combinação linear sobre $\mathbb{Q}$ dos elementos de A, pois A é uma base para E_k sobre $\mathbb{Q}$. Sendo assim, existem escalares

$$a_1, ..., a_{2^k} \in \mathbb{Q}$$

tais que

$$v = a_1 e_1 + ... + a_{2^k} e_{2^k}.$$

Porém, como $\mathbb{Q} \subseteq \mathscr{F}(u)$, segue que $a_i \in \mathscr{F}(u)$, para todo $i \in \{1,...,2^k\}$, ou seja, v é combinação linear sobre $\mathscr{F}(u)$ dos elementos de B, como se queria provar.

Logo, segue de (i) e (ii) que B é uma base para E_k *sobre* $\mathscr{F}(u)$. Definindo $v_i \doteq e_i$, para todo $i \in \{1,...,2^k\}$, e $n \doteq 2^k$, tem-se que $B = \{v_1,...,v_n\}$ possui n elementos. Portanto, neste cenário, o espaço vetorial E_k *sobre* $\mathscr{F}(u)$ tem dimensão $n = 2^k$, o que conclui o primeiro caso.

Caso (II): Suponha que A é LD *sobre* $\mathscr{F}(u)$. Como A é LI sobre $\mathbb{Q}$, é claro que existe pelo menos um vetor não nulo $e_j \in A$, pois do contrário existiriam escalares $a_1,...,a_{2^k} \in \mathbb{Q}$, não todos nulos, tais que

$$a_1 \cdot 0 + ... + a_{2^k} \cdot 0 = 0.$$

De fato, bastaria tomar $a_i \doteq 1$, para todo $i \in \{1,...,2^k\}$. Chamando e_j de v, perceba que o subconjunto $\{v\}$ de A é LI sobre $\mathscr{F}(u)$ pois, se existir $\alpha \in \mathscr{F}(u)$ tal que $\alpha v = 0$, então segue das propriedades vistas no início do capítulo anterior que $\alpha = 0$, porque $v \neq 0$ e E_k é um espaço vetorial sobre $\mathscr{F}(u)$.

A conclusão do parágrafo anterior é que existe um subconjunto não vazio de A, i.e., com pelo menos um elemento de A, que é LI sobre $\mathscr{F}(u)$. Sendo assim, defina n como o maior número inteiro para o qual existe um subconjunto com n elementos de A que são LI sobre $\mathscr{F}(u)$. Pelo que foi apenas mostrado, tem-se que $n \geq 1$. Seja B um tal subconjunto de A com n elementos que é LI sobre $\mathscr{F}(u)$. Os elementos de B serão denotados assim:

$$B \doteq \{v_1,...,v_n\}.$$

Afirma-se: o conjunto B é uma base para o espaço vetorial E_k sobre $\mathscr{F}(u)$. A demonstração dessa afirmação será feita em duas etapas (i) e (ii).

(i) O conjunto B é LI sobre $\mathscr{F}(u)$, fato este que decorre da própria construção de B.

(ii) Qualquer elemento de E_k é combinação linear sobre $\mathscr{F}(u)$ dos elementos de B. Para mostrar isso, seja e_j um elemento arbitrário de A tal que $e_j \notin B$. Tal elemento existe pois, se todo elemento de A estivesse em B, então B seria igual a A, o que é um absurdo, porque A é LD sobre $\mathscr{F}(u)$, pela hipótese do caso (II), e B é LI sobre $\mathscr{F}(u)$, pela construção do conjunto B. Perceba então que o conjunto

$$\{e_j, v_1, ..., v_n\}$$

é LD sobre $\mathscr{F}(u)$, pois n é o maior número de elementos de A que formam um conjunto LI sobre $\mathscr{F}(u)$. Sendo assim, segue da definição de dependência linear que existem escalares $\alpha_j, \alpha_{1j}, \alpha_{2j}, ..., \alpha_{nj} \in \mathscr{F}(u)$, não todos nulos, tais que

$$\alpha_j e_j + \alpha_{1j} v_1 + \alpha_{2j} v_2 + ... + \alpha_{nj} v_n = 0. \tag{6.5}$$

Suponha por absurdo que $\alpha_j = 0$. Substituindo na igualdade acima, obtém-se:

$$\alpha_{1j}v_1 + \alpha_{2j}v_2 + ... + \alpha_{nj}v_n = 0.$$

Como B é LI sobre $\mathscr{F}(u)$, segue que $\alpha_{1j} = \alpha_{2j} = ... = \alpha_{nj} = 0$. Ou seja,

$$\alpha_j = \alpha_{1j} = \alpha_{2j} = ... = \alpha_{nj} = 0,$$

o que é um absurdo, pois os escalares não são todos nulos. Logo, $\alpha_j \neq 0$. Deste modo, é possível isolar e_j no primeiro membro da igualdade 6.5, obtenso assim:

$$e_j = -\frac{\alpha_{1j}}{\alpha_j}v_1 - \frac{\alpha_{2j}}{\alpha_j}v_2 - ... - \frac{\alpha_{nj}}{\alpha_j}v_n. \tag{6.6}$$

Note que $-\frac{\alpha_{ij}}{\alpha_j} \in \mathscr{F}(u)$, para todo $i \in \{1,2,...,n\}$, pois $\mathscr{F}(u)$ é corpo e $\alpha_i, \alpha_j \in \mathscr{F}(u)$, para todo $i \in \{1,...,n\}$. Portanto, qualquer elemento $e_j \in A$ que não esteja em B é uma combinação linear sobre $\mathscr{F}(u)$ dos elementos de B.

Agora considere um elemento arbitrário $v \in E_k$. Como A é uma base para E_k sobre $\mathbb{Q}$, existem escalares

$$a_1, ..., a_{2^k} \in \mathbb{Q}$$

tais que

$$v = a_1e_1 + ... + a_{2^k}e_{2^k}. \tag{6.7}$$

Alguns elementos e_i de A estão em B (foram denotados $v_1, ..., v_n$) e outros não. Porém, pelo que foi provado acima, sabe-se que cada elemento e_j que não está em B pode ser escrito como uma combinação linear sobre $\mathscr{F}(u)$ dos elementos $v_1, ..., v_n$ de B. Assim, ao substituir cada $e_j \notin B$ por tal combinação linear na igualdade 6.7 e reagrupar os termos, usando as propriedades distributiva e associativa, obtém-se que v é combinação linear sobre $\mathscr{F}(u)$ dos elementos $v_1, ..., v_n$ de B, como se queria mostrar, pois todos os coeficientes envolvidos estarão em $\mathscr{F}(u)$ devido ao fato de que $\mathscr{F}(u)$ é um corpo e $a_i \in \mathbb{Q} \subseteq \mathscr{F}(u)$, para todo $i \in \{1, ..., 2^k\}$. Ou seja, todo elemento $v \in E_k$ é tal que

$$v = b_1v_1 + ... + b_nv_n, \tag{6.8}$$

onde $b_1, ..., b_n \in \mathscr{F}(u)$ e $1 \leq n < 2^k$ (já foi visto que B não pode ser igual a A e por isso n é estritamente menor do que 2^k).

Logo, segue de (i) e (ii) que B é uma base para E_k sobre $\mathscr{F}(u)$. Portanto, neste cenário, o espaço vetorial E_k *sobre* $\mathscr{F}(u)$ tem dimensão $n < 2^k$, o que conclui o segundo caso.

Assim, seja qual for o caso, a conclusão é que E_k é um espaço vetorial sobre $\mathscr{F}(u)$ de dimensão finita, como se queria demonstrar, e, além disso, a sua dimensão é igual a $n \leq 2^k$. □

Seguindo o raciocínio do início desta seção, uma vez provado que E_k é um espaço vetorial sobre $\mathscr{F}(u)$ de dimensão finita, é possível finalmente estabelecer um critério para decidir se o número algébrico *u pode ou não* ser um número construtível. O que ocorre é que, se u for um número construtível, haverá uma condição necessária sobre o grau de u, que será formalizada através do teorema a seguir.

Teorema 21 (Critério de construtibilidade)**.** Seja u um número algébrico de grau m. Se u for um número construtível, então m será igual a uma potência de base 2.

Demonstração. Seja u um número algébrico de grau m, onde m é um número inteiro maior ou igual a 1. Pelo teorema 20, o corpo algébrico $\mathscr{F}(u)$ gerado por u é um espaço vetorial sobre $\mathbb{Q}$ de dimensão m. Seja então $A = \{u_1, ..., u_m\}$ uma base para $\mathscr{F}(u)$ sobre $\mathbb{Q}$.

Suponha que u é um número construtível. Então, pelo teorema 7, u está em uma extensão quadrática iterada E_k de $\mathbb{Q}$, para algum número inteiro $k \geq 0$. Pelo teorema 13, E_k é um espaço vetorial sobre $\mathbb{Q}$ de dimensão 2^k.

Por outro lado, pelo lema 11, E_k também é um espaço vetorial sobre $\mathscr{F}(u)$ de dimensão n, para algum número natural n tal que $1 \leq n \leq 2^k$. Seja então $B = \{v_1, ..., v_n\}$ uma base para E_k sobre $\mathscr{F}(u)$.

A partir disso, considere um elemento arbitrário $v \in E_k$. Olhando v como um elemento do espaço vetorial E_k sobre $\mathscr{F}(u)$, existem escalares $b_1, ..., b_n \in \mathscr{F}(u)$ tais que

$$v = b_1 v_1 + ... + b_n v_n. \tag{6.9}$$

Por sua vez, cada escalar b_j, $j \in \{1, ..., n\}$, pode ser visto como um vetor do espaço vetorial $\mathscr{F}(u)$ sobre $\mathbb{Q}$. Então, existem escalares $a_{j1}, ..., a_{jm} \in \mathbb{Q}$ tais que

$$b_j = a_{j1} u_1 + a_{j2} u_2 + ... + a_{jm} u_m, \tag{6.10}$$

para todo $j \in \{1, ..., n\}$. Substituindo cada b_j em 6.9, obtém-se:

$$v = (a_{11} u_1 + a_{12} u_2 + ... + a_{1m} u_m) v_1 + ... + (a_{n1} u_1 + a_{n2} u_2 + ... + a_{nm} u_m) v_n.$$

Usando as propriedades distributiva e associativa, a igualdade acima pode ser reescrita assim:

$$v = a_{11}(u_1 v_1) + a_{12}(u_2 v_1) + ... + a_{1m}(u_m v_1) + ... + a_{n1}(u_1 v_n) + a_{n2}(u_2 v_n) + ... + a_{nm}(u_m v_n).$$

Perceba que cada produto $u_i v_j$ é um elemento de E_k, pois E_k é um corpo, $u_i \in \mathscr{F}(u) \subseteq E_k$ e $v_j \in E_k$, para todo $i \in \{1, ..., m\}$ e todo $j \in \{1, ..., n\}$. Perceba também que a igualdade acima mostra que qualquer elemento v de E_k é combinação linear *sobre* $\mathbb{Q}$ dos elementos $u_i v_j$, pois $a_{ji} \in \mathbb{Q}$, para todo $i \in \{1, ..., m\}$ e todo $j \in \{1, ..., n\}$. Além disso, como há m possibilidades para u_i e n possibilidades para v_j, é possível concluir, pelo *Princípio Fundamental da Contagem*, que há um total de mn produtos da forma $u_i v_j$. Sendo assim, defina:

$$C \doteq \{u_1 v_1, u_2 v_1, ..., u_m v_1, ..., u_1 v_n, u_2 v_n, ..., u_m v_n\}.$$

O conjunto C é formado por todos os produtos da forma $u_i v_j$ e, portanto, é um conjunto finito com mn elementos de E_k. Será provado que C é uma base para o espaço vetorial E_k sobre $\mathbb{Q}$. Já se sabe que todo vetor de E_k é combinação linear sobre $\mathbb{Q}$ dos elementos de C. Então basta mostrar que C é LI sobre $\mathbb{Q}$. Para isso, suponha que existam escalares

$$c_{11}, c_{12}, ..., c_{1m}, ..., c_{n1}, c_{n2}, ..., c_{nm} \in \mathbb{Q}$$

tais que

$$c_{11}(u_1 v_1) + c_{12}(u_2 v_1) + ... + c_{1m}(u_m v_1) + ... + c_{n1}(u_1 v_n) + c_{n2}(u_2 v_n) + ... + c_{nm}(u_m v_n) = 0.$$

Usando as propriedades associativa e distributiva, a igualdade acima pode ser reescrita assim:

$$(c_{11}u_1 + c_{12}u_2 + ... + c_{1m}u_m) v_1 + ... + (c_{n1}u_1 + c_{n2}u_2 + ... + c_{nm}u_m) v_n = 0.$$

Note que o coeficiente que acompanha cada v_j está em $\mathscr{F}(u)$, pois $\mathscr{F}(u)$ é um corpo e $c_{ji} \in \mathbb{Q} \subseteq \mathscr{F}(u)$, para todo $i \in \{1, ..., m\}$ e todo $j \in \{1, ..., n\}$. Porém, $B = \{v_1, ..., v_n\}$ é LI sobre $\mathscr{F}(u)$. Então:

$$c_{j1}u_1 + c_{j2}u_2 + ... + c_{jm}u_m = 0,$$

para todo $j \in \{1, ..., n\}$. Por sua vez, como $A = \{u_1, ..., u_m\}$ é LI sobre $\mathbb{Q}$, segue da igualdade acima que

$$c_{j1} = c_{j2} = ... = c_{jm} = 0,$$

para todo $j \in \{1, ..., n\}$, ou seja, C é LI sobre $\mathbb{Q}$. Logo, C é uma base para o espaço vetorial E_k sobre $\mathbb{Q}$, como se queria provar. Além disso, C tem mn elementos. Por outro lado, como foi dito início da demonstração, o espaço vetorial E_k sobre $\mathbb{Q}$ tem dimensão 2^k. Portanto,

$$mn = 2^k, \tag{6.11}$$

onde m é o grau de u e n é a dimensão de E_k sobre $\mathscr{F}(u)$. Segue da igualdade acima que m é um divisor de 2^k. Porém, os únicos divisores de uma potência de base 2 são potências de base 2. Portanto, m é igual a uma potência de base 2, como se queria demonstrar. □

Se alguém estiver buscando uma estampa para fazer uma camiseta em homenagem a este trabalho, com certeza a estampa deve ser a igualdade 6.11:

$$mn = 2^k.$$

Essa igualdade é e sempre foi a meta deste trabalho. É emocionante e belo chegar neste momento, sabendo de todo o estudo feito para chegar até aqui. Foram construídos vários conceitos e provados diversos resultados ao longo de vários capítulos... Para chegar finalmente nessa igualdade! Seria uma bela camiseta!

Com este último, grande e belo resultado em mãos, podemos gritar aos quatro ventos: *O GRAU DE UM NÚMERO ALGÉBRICO CONSTRUTÍVEL É UMA POTÊNCIA DE BASE 2!!!* Ou seja, uma condição necessária para um número algébrico ser construtível é que o seu grau seja igual a uma potência de base 2. Porém, é importante dizer que essa não é uma condição suficiente. Por isso, foi dito desde o início que esse seria um critério para decidir se um dado número algébrico *pode ou não* ser um número construtível. Funciona assim a receita: 1. Pegue um número algébrico e veja o seu grau; 2. Se o grau for uma potência de base 2, então este número *pode* ser construtível, mas isso não garante que ele seja construtível; 3. Se o grau não for uma potência de base 2, então este número *não pode* ser construtível, e isso é garantido, ou seja, *o número algébrico com certeza não é construtível*.

É o último passo 3 que será usado no próximo capítulo. Este *Critério de Construtibilidade* coloca um ponto final em toda a teoria de álgebra construída neste trabalho. Com isso, é possível finalmente resolver o *problema da construção de polígonos regulares com régua e compasso*.

CAPÍTULO

7

CONSTRUÇÃO DE POLÍGONOS REGULARES

Se $n > 2$ é um número natural, então construir um polígono regular com n lados usando apenas régua e compasso é equivalente a dividir um círculo em n partes iguais com esses instrumentos, o que é o mesmo que construir um ângulo de medida igual a

$$\frac{360^\circ}{n}.$$

Se um ângulo é construtível, então o seno e o cosseno desse ângulo são números construtíveis e, por consequência, a tangente desse ângulo também é um número construtível. Devido a isso, neste capítulo serão analisados casos em que $\text{tg}\left(\frac{360^\circ}{n}\right)$ é ou não um número construtível.

Definição 27 (Polígono construtível)**.** Um polígono é *construtível* se pode ser construído com apenas régua e compasso.

A definição acima tem por objetivo facilitar a escrita, pois ao invés de ter que dizer que *determinado polígono regular pode ou não ser construído com apenas régua e compasso* poderá ser dito simplesmente que *determinado polígono regular é ou não é construtível*.

7.1 Equação dos polígonos regulares

Do mesmo modo que as equações cúbicas desempenharam um papel central nas soluções dos problemas da duplicação do cubo e da trissecção do ângulo, as equações polinomiais serão essenciais para a solução do problema da construção de polígonos regulares. E de modo análogo à *equação da duplicação do cubo* e à *equação da trissecção do ângulo*, nesta primeira seção será apresentada através do lema a seguir a *equação dos polígonos regulares*.

Lema 12 (Equação dos polígonos regulares)**.** Se $q > 1$ é um número inteiro ímpar, então

$$\operatorname{tg}\frac{360^\circ}{q}, \operatorname{tg}\frac{2\cdot 360^\circ}{q}, ..., \operatorname{tg}\frac{(q-1)\cdot 360^\circ}{q}$$

são as raízes da equação polinomial a seguir, que será dita *equação dos polígonos regulares*:

$$x^{q-1} - \frac{q(q-1)\cdot ...\cdot 3}{(q-2)!}x^{q-3} + \frac{q(q-1)\cdot ...\cdot 5}{(q-4)!}x^{q-5} - ... + (-1)^{\frac{q+1}{2}}\frac{q(q-1)(q-2)}{3!}x^2 + (-1)^{\frac{q-1}{2}}q = 0,$$

onde cada coeficiente é um número inteiro. O polinômio do primeiro membro da equação acima será chamado de $C_q(x)$.

Demonstração. Seja $q > 1$ um inteiro *ímpar*. Por um lado, pela *fórmula de De Moivre*,

$$(\cos\theta + i\operatorname{sen}\theta)^q = \cos(q\theta) + i\operatorname{sen}(q\theta).$$

Por outro lado, pela *fórmula do binômio de Newton*,

$$\begin{aligned}
(\cos\theta + i\operatorname{sen}\theta)^q &= \sum_{k=0}^{q}\binom{q}{k}\cos^{q-k}\theta\cdot i^k\operatorname{sen}^k\theta \\
&= \binom{q}{0}\cos^{q-0}\theta\ \operatorname{sen}^0\theta + i\binom{q}{1}\cos^{q-1}\theta\ \operatorname{sen}\theta \\
&- \binom{q}{2}\cos^{q-2}\theta\ \operatorname{sen}^2\theta - i\binom{q}{3}\cos^{q-3}\theta\ \operatorname{sen}^3\theta \\
&+ \binom{q}{4}\cos^{q-4}\theta\ \operatorname{sen}^4\theta + i\binom{q}{5}\cos^{q-5}\theta\ \operatorname{sen}^5\theta \\
&- \binom{q}{6}\cos^{q-6}\theta\ \operatorname{sen}^6\theta - i\binom{q}{7}\cos^{q-7}\theta\ \operatorname{sen}^7\theta \\
&\qquad\vdots \qquad\qquad\qquad \vdots \\
&+ (-1)^{\frac{k}{2}}\binom{q}{k}\cos^{q-k}\theta\ \operatorname{sen}^k\theta + (-1)^{\frac{k}{2}}\,i\binom{q}{k+1}\cos^{q-k-1}\theta\ \operatorname{sen}^{k+1}\theta \\
&\qquad\vdots \qquad\qquad\qquad\qquad \vdots \\
&+ (-1)^{\frac{q-1}{2}}\binom{q}{q-1}\cos^{q}\theta\ \operatorname{sen}^{q-1}\theta + (-1)^{\frac{q-1}{2}}\,i\binom{q}{q}\cos^{q-q}\theta\ \operatorname{sen}^{q}\theta.
\end{aligned}$$

Vale lembrar que dois números complexos são iguais se, e somente se, suas partes reais são iguais e suas partes imaginárias são iguais. Assim, segue das igualdades acima que:

$$\operatorname{sen}(q\theta) = q\cos^{q-1}\theta\ \operatorname{sen}\theta - \binom{q}{3}\cos^{q-3}\theta\ \operatorname{sen}^3\theta + \binom{q}{5}\cos^{q-5}\theta\ \operatorname{sen}^5\theta - ... + (-1)^{\frac{q-1}{2}}\operatorname{sen}^q\theta.$$

Dividindo ambos os membros da igualdade acima por $\cos^q\theta$, obtém-se:

$$\frac{\operatorname{sen}(q\theta)}{\cos^q\theta} = q\frac{\cos^{q-1}\theta\ \operatorname{sen}\theta}{\cos^q\theta} - \binom{q}{3}\frac{\cos^{q-3}\theta\ \operatorname{sen}^3\theta}{\cos^q\theta} + \binom{q}{5}\frac{\cos^{q-5}\theta\ \operatorname{sen}^5\theta}{\cos^q\theta} - ... + (-1)^{\frac{q-1}{2}}\frac{\operatorname{sen}^q\theta}{\cos^q\theta}.$$

Logo,

$$\frac{\operatorname{sen}(q\theta)}{\cos^q\theta} = q\frac{\operatorname{sen}\theta}{\cos\theta} - \binom{q}{3}\frac{\operatorname{sen}^3\theta}{\cos^3\theta} + \binom{q}{5}\frac{\operatorname{sen}^5\theta}{\cos^5\theta} - \ldots + (-1)^{\frac{q-1}{2}}\frac{\operatorname{sen}^q\theta}{\cos^q\theta}.$$

Como a tangente de um ângulo é igual à razão entre o seno e o cosseno desse ângulo, tem-se:

$$\frac{\operatorname{sen}(q\theta)}{\cos^q\theta} = q\operatorname{tg}\theta - \binom{q}{3}\operatorname{tg}^3\theta + \binom{q}{5}\operatorname{tg}^5\theta - \ldots + (-1)^{\frac{q-1}{2}}\operatorname{tg}^q\theta. \tag{7.1}$$

Agora perceba que, se θ é um dos ângulos

$$0\cdot\frac{360^\circ}{q}, 1\cdot\frac{360^\circ}{q}, 2\cdot\frac{360^\circ}{q}, \ldots, (q-1)\cdot\frac{360^\circ}{q},$$

então $\operatorname{sen}(q\theta) = \operatorname{sen}(k\cdot 360^\circ) = 0$, para todo $k \in \{0,1,\ldots,q-1\}$, e $\cos\theta \neq 0$. Logo, se θ é igual a dos ângulos acima, segue que

$$\frac{\operatorname{sen}(q\theta)}{\cos^q\theta} = 0. \tag{7.2}$$

Deste modo, denotando $x \doteq \operatorname{tg}\theta$, segue de 7.1 e 7.2 que:

$$qx - \binom{q}{3}x^3 + \binom{q}{5}x^5 - \ldots + (-1)^{\frac{q-1}{2}}x^q = 0.$$

Colocando x em evidência na equação acima, obtém-se:

$$x\cdot\left[q - \binom{q}{3}x^2 + \binom{q}{5}x^4 - \ldots + (-1)^{\frac{q-1}{2}}x^{q-1}\right] = 0.$$

Portanto, $\operatorname{tg}\frac{0\cdot 360^\circ}{q} = \operatorname{tg} 0^\circ$ é raiz de $x = 0$, enquanto que

$$\operatorname{tg}\frac{360^\circ}{q}, \operatorname{tg}\frac{2\cdot 360^\circ}{q}, \ldots, \operatorname{tg}\frac{(q-1)\cdot 360^\circ}{q}$$

são as raízes de

$$(-1)^{\frac{q-1}{2}}x^{q-1} + (-1)^{\frac{q-3}{2}}\binom{q}{q-2}x^{q-3} + (-1)^{\frac{q-5}{2}}\binom{q}{q-4}x^{q-5} + \ldots + \binom{q}{5}x^4 - \binom{q}{3}x^2 + q = 0,$$

como se queria demonstrar. Nas aplicações futuras, o sinal de cada coeficiente não fará diferença, mas para deixar a equação acima idêntica à do enunciado, basta multiplicar ambos os membros da mesma por $(-1)^{\frac{q-1}{2}}$ e então obtém-se:

$$x^{q-1} - \binom{q}{q-2}x^{q-3} + \binom{q}{q-4}x^{q-5} - \ldots + (-1)^{\frac{q+3}{2}}\binom{q}{5}x^4 + (-1)^{\frac{q+1}{2}}\binom{q}{3}x^2 + (-1)^{\frac{q-1}{2}}q = 0,$$

onde cada coeficiente é um número inteiro, pois é um número binomial. □

A *equação dos polígonos regulares* é de extrema importância e será usada em alguns teoremas que serão apresentados na seção a seguir sobre a não construtibilidade de determinados polígonos regulares e por isso o resultado acima foi chamado de lema. Entretanto, é visível como foi trabalhoso obter tal equação! Inclusive, é interessante observar que a *equação da trissecção*

também deu trabalho. Apenas a *equação da duplicação* foi fácil de obter. É claro que, comparada ao *critério de construtibilidade*, que levou capítulos para ser construído, a equação dos polígonos regulares soa como um passeio no parque. Sem contar que tanto a *fórmula de De Moivre* quanto a *fórmula do binômio de Newton* são ensinadas no Ensino Médio. Então, mesmo que o caso geral feito aqui seja muito intricado para um aluno do ensino médio, um caso particular para algum número ímpar q específico é totalmente acessível e fácil de justificar.

7.2 Construção de polígonos regulares com régua e compasso

Finalmente é chegado o momento! Através do teorema a seguir, será provado que é impossível construir certos polígonos regulares usando somente régua e compasso. Depois de tudo o que foi visto, a demonstração parecerá fácil, mas tenha em mente que serão usadas duas ferramentas poderosas: o gigante *critério de construtibilidade* e a formosa *equação dos polígonos regulares*. Então, no fundo, todo o trabalho da demonstração do teorema abaixo está presente nas demonstrações dessas duas ferramentas, e todo o restante é apenas um jogo de quebra-cabeça: basta juntar as peças!

Teorema 22. Seja p um número primo ímpar tal que p *não* é da forma 2^h+1, para algum número inteiro $h \geq 0$. Então *não* é possível construir um polígono regular com p lados usando somente régua e compasso.

Demonstração. Seja p um número primo ímpar tal que p *não* é da forma 2^h+1, para algum número inteiro $h \geq 0$. Suponha por absurdo que um p-ágono regular é construtível.

Por um lado, segue do argumento feito no início deste capítulo que é construtível o número

$$u \doteq \operatorname{tg} \frac{360^\circ}{p}.$$

Por outro lado, u é um número algébrico, pois, pelo lema 12, u é uma raiz da da equação

$$C_p(x) = 0,$$

onde $C_p(x)$ é um polinômio sobre $\mathbb{Q}$ de grau $p-1$ que tem somente coeficientes inteiros:

$$C_p(x) \equiv x^{p-1} - \binom{p}{p-2}x^{p-3} + \binom{p}{p-4}x^{p-5} - \ldots + (-1)^{\frac{p+3}{2}}\binom{p}{5}x^4 + (-1)^{\frac{p+1}{2}}\binom{p}{3}x^2 + (-1)^{\frac{p-1}{2}}\,p.$$

A ideia agora é usar o *Critério de Eisenstein* para mostrar que o polinômio $C_p(x)$ é irredutível sobre $\mathbb{Q}$. Note que, por hipótese, p é um primo ímpar, ou seja, $p \geq 3$, de onde segue que $p-1 \geq 2$. Portanto, $C_p(x)$ é um polinômio de grau maior ou igual a 2 com coeficientes inteiros. Resta provar que existe um número primo que satisfaz as condições (i) e (ii) do teorema 17, o que será feito a seguir para o primo p.

(i) Não é difícil argumentar que, por p ser um número primo, o coeficiente binomial

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

é divisível por p, para todo k tal que $1 \leq k \leq p-1$. De fato, como p é primo e todos os números em $k!$ e $(p-k)!$ são menores do que p, segue que não há nenhum fator p no

denominador de $\binom{p}{k}$. Logo, como $p! = p(p-1)!$ tem um fator p e $k!(p-k)!$ não tem fator p, segue que $\binom{p}{k}$ é divisível por p, para todo k tal que $1 \leq k \leq p-1$. Portanto, todos os coeficientes de $C_p(x)$ são divisíveis por p, exceto o coeficiente do termo de maior grau, x^{p-1}, que é igual a 1 e não é divisível por p.

(ii) O termo constante de $C_p(x)$, que é igual a $(-1)^{\frac{p-1}{2}}\, p$, claramente não é divisível por p^2.

Então, pelo *Critério de Eisenstein*, $C_p(x)$ é irredutível sobre $\mathbb{Q}$. Deste modo, como $C_p(x)$ é mônico, segue do teorema 18 que $C_p(x)$ é o único polinômio mônico irredutível sobre $\mathbb{Q}$ tal que $C_p(u) = 0$. Portanto, o grau de u é igual a $p-1$.

Porém, como u é construtível, segue do *Critério de construtibilidade* que o grau de u é uma potência de 2. Logo,

$$p - 1 = 2^k,$$

para algum número inteiro $k \geq 0$. Isolando p no primeiro membro da igualdade acima, obtém-se:

$$p = 2^k + 1,$$

o que é um absurdo, pois p *não* é dessa forma, por hipótese. Portanto, *não* é possível construir um polígono regular com p lados usando somente régua e compasso, como se queria demonstrar. □

Observação 12. O teorema acima fornece muitos polígonos regulares que não podem ser construídos com apenas régua e compasso. Por exemplo, não se pode construir um heptágono regular com régua e compasso, pois $p = 7$ não é da forma $2^k + 1$ ou, em outras palavras, $p - 1 = 6$ não é uma potência de base 2. O mesmo ocorre com 11, 13, 19 e vários outros números primos.

Assim, se pensarmos do mesmo modo que na duplicação do cubo e na trissecção do ângulo, o teorema acima já conclui a solução do problema da construção de polígonos regulares, pois a impossibilidade da construção do heptágono regular prova que nem todo polígono regular pode ser construído com apenas régua e compasso. É claro que o teorema entregou muito mais do que seu "equivalente" na duplicação do cubo, pois enquanto lá foi provado que apenas o cubo unitário não pode ser duplicado, aqui já se provou que existem vários polígonos regulares que não são construtíveis. Mas isso não importa, porque a impossibilidade de construir apenas um polígono regular já é suficiente para mostrar que não se pode fazer para todos. Então, assim como foi dito na duplicação do cubo e na trissecção do ângulo, aqui também podemos dizer com todas as palavras: *O problema da construção de polígonos regulares está resolvido sim! E sua solução mostra que é impossível construir todo polígono regular usando apenas régua e compasso!* Vale observar que alguns polígonos regulares podem ser construídos com apenas régua e compasso, porém o que se está dizendo é que não existe um procedimento geral para fazer a construção de um polígono regular arbitrário usando somente régua e compasso.

A conclusão do parágrafo anterior é análoga ao que foi concluído na duplicação do cubo e na trissecção do ângulo. Mas na realidade, a solução completa do problema da construção de polígonos regulares com régua e compasso vai bem mais além desse desfecho. Assim, ao invés de parar por aqui como foi feito nas soluções dos outros dois problemas de construção, serão dados mais alguns passos em direção ao topo da montanha de onde será possível ter uma vista mais ampla da construção de polígonos regulares com régua e compasso. O objetivo da próxima seção é apresentar uma *caracterização completa dos polígonos regulares construtíveis*.

7.3 Caracterização dos polígonos regulares construtíveis

É comum trabalhar na escola a construção de triângulos equiláteros, quadrados e hexágonos regulares com régua e compasso. O aluno mais curioso poderia perguntar: *Se não é possível construir todos, quais polígonos regulares podem ser construídos com apenas régua e compasso?* Essa é uma excelente pergunta e será respondida até o final desta seção. Assim que o objetivo a partir de agora é provar uma parte dos resultados que, juntos, darão uma resposta completa a esse questionamento, ou seja, fornecerão uma *caracterização dos polígonos regulares construtíveis*. Com efeito, serão provados todos os resultados necessários a menos de um grande teorema, enunciado e provado por Carl Friedrich Gauss.

Após o grande primeiro passo dado através do último teorema, alguém poderia perguntar: *Se os primos ímpares que não são da forma* 2^k+1 *foram um empecilho na construção de polígonos regulares com apenas régua e compasso, o que ocorre quando o primo é da forma* 2^k+1*?* Eis que Gauss provou em sua *Disquisitiones Arithmeticae* que, se p é um primo da forma 2^k+1, para algum inteiro $k>0$, então o p-ágono regular é construtível (embora não tenha provado que se p não é dessa forma, então o p-ágono regular não é construtível). Porém, a demonstração de Gauss não será feita aqui, pois foge do escopo deste trabalho.

Um fato conhecido da *Teoria dos Números* é que, se k é um número inteiro positivo e 2^k+1 é um número primo, então k é uma potência de base 2, ou seja, o primo é da forma $F_n = 2^{2^n}+1$, para algum inteiro $n \geq 0$. Os primos dessa forma são chamados de *primos de Fermat* e apenas 5 números primos assim são conhecidos:

$$\begin{aligned} F_0 &= 2^{2^0}+1 = 3 \\ F_1 &= 2^{2^1}+1 = 5 \\ F_2 &= 2^{2^2}+1 = 17 \\ F_3 &= 2^{2^3}+1 = 257 \\ F_4 &= 2^{2^4}+1 = 65537 \end{aligned}$$

Esses números foram estudados por Pierre de Fermat, que fez a conjectura de que todo número da forma $2^{2^n}+1$ seria primo. Porém, Leonhard Euler provou em 1732 que $2^{2^5}+1$ não é primo. Não se sabe quantos primos de Fermat existem.

Em suma, no que diz respeito aos p-ágonos regulares, onde p é um número primo, o teorema a seguir é a versão mais completa do teorema 22, porém este resultado não será demonstrado aqui, como já explicado.

Teorema 23. Seja $p>2$ um número primo. Então: um p-ágono regular é construtível se, e somente se, p é um primo de Fermat.

Ou seja, quando se trata da construção de polígonos regulares com um número primo p de lados, a condição de que p seja um primo de Fermat é *necessária e suficiente*. Uma curiosidade

é que, além de provar que essa condição é *suficiente*, Gauss também enunciou que essa condição é *necessária*, porém nunca publicou uma demonstração. Pierre Wantzel provou que a condição é necessária em 1837.

Deste modo, com o incrível resultado de Gauss, ficam cobertos todos os p-ágonos regulares onde p é primo. Mas se n não é primo, o que ocorre com a construtibilidade dos n-ágonos regulares? Os próximos resultados buscam cobrir os demais polígonos regulares.

Teorema 24. Sejam p um número primo ímpar e $k > 1$ um número inteiro. Então *não* é possível construir um polígono regular com p^k lados usando somente régua e compasso.

Demonstração. Sejam p um número primo ímpar e $k > 1$ um número inteiro. Suponha por absurdo que o p^k-ágono regular é construtível, ou seja, o ângulo abaixo é construtível:

$$\frac{360^\circ}{p^k}.$$

Construindo-se com régua e compasso p^{k-1} ângulos com a medida acima, obtém-se que $\frac{360^\circ}{p}$ é um ângulo construtível, pois

$$\frac{360^\circ}{p} = p^{k-1} \cdot \frac{360^\circ}{p^k}.$$

Ou seja, o p-ágono regular é construtível. Segue do teorema 22 que p é um primo da forma $2^h + 1$, para algum inteiro $h > 0$.

De modo análogo, é possível construir com régua e compasso p^{k-2} ângulos de medida $\frac{360^\circ}{p^k}$ e assim obter que $\frac{360^\circ}{p^2}$ é um ângulo construtível, pois

$$\frac{360^\circ}{p^2} = p^{k-2} \cdot \frac{360^\circ}{p^k}.$$

Por um lado, segue do argumento feito no início deste capítulo que é construtível o número

$$u \doteq \operatorname{tg} \frac{360^\circ}{p^2}.$$

Por outro lado, u é um número algébrico, pois, pelo lema 12, u é uma raiz da equação

$$C_{p^2}(x) = 0,$$

onde $C_{p^2}(x)$ é um polinômio mônico sobre $\mathbb{Q}$ de grau $p^2 - 1 \geq 8$ que tem somente coeficientes inteiros. Na realidade, o lema 12 garante muito mais do que isso. Pelo lema, os números

$$\operatorname{tg} \frac{1 \cdot 360^\circ}{p^2}, \operatorname{tg} \frac{2 \cdot 360^\circ}{p^2}, \operatorname{tg} \frac{3 \cdot 360^\circ}{p^2}, \ldots, \operatorname{tg} \frac{(p^2-1) \cdot 360^\circ}{p^2}$$

são as raízes da equação polinomial $C_{p^2}(x) = 0$. Note que, dentre essas raízes, estão os $p-1$ números

$$\operatorname{tg}\frac{p\cdot 360^\circ}{p^2}, \operatorname{tg}\frac{2p\cdot 360^\circ}{p^2}, \operatorname{tg}\frac{3p\cdot 360^\circ}{p^2}, \ldots, \operatorname{tg}\frac{(p-1)p\cdot 360^\circ}{p^2}.$$

Cancelando o fator p, os números acima podem ser reescritos assim:

$$\operatorname{tg}\frac{360^\circ}{p}, \operatorname{tg}\frac{2\cdot 360^\circ}{p}, \operatorname{tg}\frac{3\cdot 360^\circ}{p}, \ldots, \operatorname{tg}\frac{(p-1)\cdot 360^\circ}{p}. \tag{7.3}$$

Como esses números são raízes de $C_{p^2}(x) = 0$, segue da proposição 10 que

$$C_{p^2}(x) \equiv \left(x - \operatorname{tg}\frac{360^\circ}{p}\right)\left(x - \operatorname{tg}\frac{2\cdot 360^\circ}{p}\right)\cdot\ldots\cdot\left(x - \operatorname{tg}\frac{(p-1)\cdot 360^\circ}{p}\right)\cdot Q(x), \tag{7.4}$$

para algum polinômio $Q(x)$ tal que o grau de $Q(x)$ é igual a

$$\left(p^2-1\right) - (p-1) = p^2 - p.$$

Por outro lado, também pelo lema 12, os números de 7.3 são as $p-1$ raízes da equação polinomial $C_p(x) = 0$, onde $C_p(x)$ é um polinômio mônico com coeficientes inteiros de grau $p-1 \geq 2$. De modo análogo ao que foi feito acima, tem-se que

$$C_p(x) \equiv \left(x - \operatorname{tg}\frac{360^\circ}{p}\right)\left(x - \operatorname{tg}\frac{2\cdot 360^\circ}{p}\right)\cdot\ldots\cdot\left(x - \operatorname{tg}\frac{(p-1)\cdot 360^\circ}{p}\right). \tag{7.5}$$

Substituindo 7.5 em 7.4, obtém-se:

$$C_{p^2}(x) \equiv C_p(x)Q(x). \tag{7.6}$$

Se $x = u$, a igualdade acima fica assim:

$$0 = C_p(u)Q(u).$$

Porém, como u não é um dos números de 7.3, segue que $C_p(u) \neq 0$. Logo,

$$Q(u) = 0,$$

ou seja, o número u é uma raiz do polinômio $Q(x)$. Como $C_{p^2}(x)$ e $C_p(x)$ são mônicos e têm coeficientes inteiros, segue de 7.6 que $Q(x)$ também é mônico e tem coeficientes inteiros.

Perceba que tudo isso mostra que $C_{p^2}(x)$ é redutível sobre $\mathbb{Q}$ e por isso ele não serviria para o propósito dessa demonstração, como $C_p(x)$ serviu na demonstração do teorema 22. Devido a isso, foi construído o polinômio $Q(x)$, que tem as características necessárias para concluir esta demonstração.

A ideia agora é usar o *Critério de Eisenstein* para mostrar que o polinômio $Q(x)$ é irredutível sobre $\mathbb{Q}$. Note que, por hipótese, p é um primo ímpar, ou seja, $p \geq 3$, de onde segue que $p^2 - p \geq 6$. Portanto, $Q(x)$ é um polinômio de grau maior ou igual a 2 com coeficientes inteiros. Resta provar que existe um número primo que satisfaz as condições (i) e (ii) do teorema 17, o que será feito a seguir para o primo p.

(i) O termo de maior grau de $Q(x)$ é x^{p^2-p}, cujo coeficiente é igual a 1 e, portanto, não é divisível por p. Para mostrar que todos os coeficientes dos outros termos de $Q(x)$ são divisíveis por p, lembre-se primeiro que, como foi provado na demonstração do teorema 22, todos os coeficientes de $C_p(x)$ são divisíveis por p, exceto o coeficiente de x^{p-1}, que é igual a 1. Logo, $C_p(x)$ pode ser escrito como:

$$C_p(x) \equiv x^{p-1} - pb(x), \tag{7.7}$$

para algum polinômio $b(x)$ com coeficientes inteiros. De modo análogo, todos os coeficientes de $C_{p^2}(x)$ são divisíveis por p^2, exceto o coeficiente de x^{p^2-1}, que é igual a 1. Logo, $C_{p^2}(x)$ pode ser escrito como:

$$C_{p^2}(x) \equiv x^{p^2-1} - p^2a(x), \tag{7.8}$$

para algum polinômio $a(x)$ com coeficientes inteiros. Além disso, o polinômio mônico $Q(x)$ de grau p^2-p pode ser escrito como:

$$Q(x) \equiv x^{p^2-p} + c(x), \tag{7.9}$$

para algum polinômio $c(x)$ com coeficientes inteiros. Perceba que o que se deseja mostrar é que todos os coeficientes de $c(x)$ são divisíveis por p. Então, substituindo 7.8, 7.7 e 7.9 em 7.6, obtém-se:

$$x^{p^2-1} - p^2a(x) \equiv \Big[x^{p-1} - pb(x)\Big] \cdot \Big[x^{p^2-p} + c(x)\Big].$$

Logo, aplicando a propriedade distributiva, tem-se que:

$$x^{p^2-1} - p^2a(x) \equiv x^{p^2-1} + x^{p-1}c(x) - pb(x)x^{p^2-p} - pb(x)c(x).$$

Cancelando os termos iguais e isolando o termo $x^{p-1}c(x)$ em um dos membros da igualdade acima, obtém-se:

$$x^{p-1}c(x) \equiv pb(x)x^{p^2-p} + pb(x)c(x) - p^2a(x).$$

Por fim, colocando p em evidência no segundo membro da igualdade acima, segue que:

$$x^{p-1}c(x) \equiv p\Big[b(x)x^{p^2-p} + b(x)c(x) - pa(x)\Big].$$

Note que todos os coeficientes do polinômio do segundo membro são divisíveis por p. Logo, da igualdade de polinômios segue que todos os coeficientes do polinômio do primeiro membro são divisíveis por p, que são exatamente os coeficientes de $c(x)$. Portanto, todos os coeficientes de $Q(x)$ são divisíveis por p, exceto o termo de maior grau.

(ii) Pelo lema 12, o termo constante de $C_p(x)$ é $(-1)^{\frac{p-1}{2}}\,p$. De modo análogo, o termo constante de $C_{p^2}(x)$ é $(-1)^{\frac{p^2-1}{2}}\,p^2$. Logo, o termo constante de $Q(x)$ é $(-1)^{\frac{p^2-p}{2}}\,p$, pois por 7.6 o

produto entre o termo constante de $C_p(x)$ e o termo constante de $Q(x)$ deve resultar no termo constante de $C_{p^2}(x)$, e:

$$(-1)^{\frac{p-1}{2}}\, p \cdot (-1)^{\frac{p^2-p}{2}}\, p = (-1)^{\frac{(p-1)+(p^2-p)}{2}}\, p^2 = (-1)^{\frac{p^2-1}{2}}\, p^2.$$

Sendo assim, o termo constante de $Q(x)$ não é divisível por p^2.

Então, pelo *Critério de Eisenstein*, segue de (i) e (ii) que o polinômio $Q(x)$ é irredutível sobre $\mathbb{Q}$. Deste modo, como $Q(x)$ é mônico, segue do teorema 18 que $Q(x)$ é o único polinômio mônico irredutível sobre $\mathbb{Q}$ tal que $Q(u) = 0$. Portanto, o grau de u é igual a $p^2 - p$.

Porém, como u é construtível, segue do *Critério de construtibilidade* que o grau de u é uma potência de base 2. Logo,

$$p^2 - p = 2^k,$$

para algum número inteiro $k \geq 0$. Colocando p em evidência na igualdade acima, obtém-se:

$$p(p-1) = 2^k.$$

Isso implica que p é uma potência de 2, o que é um absurdo, pois p é um primo ímpar. Portanto, *não* é possível construir um polígono regular com p^k lados usando somente régua e compasso, como se queria demonstrar. □

Observação 13. O teorema acima fornece uma infinidade de polígonos regulares que não podem ser construídos com apenas régua e compasso. Por exemplo, é impossível construir um eneágono regular com régua e compasso, pois $9 = 3^2$ e 3 é um primo ímpar. O mesmo ocorre com n-ágonos regulares, onde n é igual a $5^2 = 25$, $3^3 = 27$, $7^2 = 49$ e infinitos outros.

O teorema 23 garante que, se p é um primo ímpar, o p-ágono regular é construtível se, e somente se, p é um primo de Fermat; enquanto que o teorema 24 garante que nenhuma potência de um primo ímpar p irá produzir um p^k-ágono regular construtível, onde $k > 1$ é um número inteiro. Assim, no que diz respeito à construção de um n-ágono regular com régua e compasso, já foram resolvidos os casos em que n é um primo ímpar e também os casos em que n é uma potência cuja base é um primo ímpar. *Mas, com relação ao único primo par, o que acontece quando n é uma potência de base* 2*?* Note que o caso $n = 2$ não faz sentido, pois um polígono tem no mínimo 3 lados. Por sua vez, o caso $n = 2^k$, onde $k > 1$, é trivial. Isso porque a divisão de um ângulo em duas partes iguais é uma das primeiras construções feitas em sala de aula em qualquer sequência didática sobre construções geométricas com régua e compasso. Inclusive, fazer a bissecção do ângulo é a motivação ideal para inserir o problema da trissecção do ângulo. E para construir qualquer 2^k-ágono regular, basta efetuar sucessivas bissecções. Por exemplo, se $n = 4$, a construção de um quadrado com régua e compasso é possível se, e somente se, $\frac{360^\circ}{4}$ é um ângulo construtível; e para mostrar isso, basta fazer a bissecção do ângulo de 360°, obtendo

assim um ângulo de 180°, e então fazer a bissecção do ângulo de 180°, obtendo o ângulo de 90°. Para mostrar de modo rigoroso que o mesmo pode ser feito para 2^k, para todo inteiro $k \geq 2$, basta fazer um processo de indução finita. Depois de todas as demonstrações feitas aqui, pode ser um excelente exercício para o leitor usar o *Princípio de Indução Finita* para provar o teorema a seguir, que é apresentado trivialmente sem demonstração.

Teorema 25. Para todo número inteiro $k \geq 2$, é possível construir um polígono regular com 2^k lados usando somente régua e compasso.

Falta pouco para se chegar ao topo da montanha. Com os teoremas 23, 24 e 25 em mãos, ficam resolvidos todos os casos em que n é um primo ou uma potência de primo para a construção de um n-ágono regular com apenas régua e compasso. Por fim, com relação a um número inteiro $n \geq 3$ qualquer, como decidir se é possível ou não construir um n-ágono regular no caso geral? Para responder a essa pergunta, será necessário o lema a seguir, que constitui o último passo em direção ao resultado final, que é a *caracterização dos polígonos regulares construtíveis*.

Lema 13. Seja $n > 2$ um número inteiro tal que $n = pq$, onde $p > 1$ e $q > 1$ são inteiros e $mdc(p,q) = 1$. Então: o n-ágono regular é construtível se, e somente se, o p-ágono regular e o q-ágono regular são construtíveis.

Demonstração. Primeiro suponha que o n-ágono regular é construtível, ou seja, o ângulo abaixo é construtível:

$$\frac{360^\circ}{pq}.$$

Construindo-se com régua e compasso q ângulos com a medida acima, obtém-se que $\frac{360^\circ}{p}$ é um ângulo construtível, pois

$$\frac{360^\circ}{p} = q \cdot \frac{360^\circ}{pq}.$$

Ou seja, o p-ágono regular é construtível. De modo análogo, conclui-se que o q-ágono regular é construtível, como se queria mostrar.

Agora suponha que o p-ágono regular e o q-ágono regular são construtíveis, ou seja, os ângulos abaixo são construtíveis:

$$\frac{360^\circ}{p} \quad \text{e} \quad \frac{360^\circ}{q}.$$

Pelo *Teorema de Bézout*, como $mdc(p,q) = 1$, existem inteiros a e b tais que

$$ap + bq = 1.$$

Multiplicando ambos os membros da igualdade acima por $\frac{360^\circ}{pq}$ e cancelando os fatores iguais, obtém-se:

$$a \cdot \frac{360^\circ}{q} + b \cdot \frac{360^\circ}{p} = \frac{360^\circ}{pq}.$$

Como $\frac{360^\circ}{q}$ e $\frac{360^\circ}{p}$ são ângulos construtíveis, segue que $a \cdot \frac{360^\circ}{q}$ e $b \cdot \frac{360^\circ}{p}$ são ângulos construtíveis e, por sua vez, a soma dos dois últimos, que é igual a $\frac{360^\circ}{pq}$, também é um ângulo construtível, ou seja, o n-ágono regular é construtível, como se queria demonstrar. □

O leitor atento já terá observado que o lema acima é exatamente a cola que estava faltando para juntar todos os pedaços apresentados até aqui. Todos os teoremas enunciados neste capítulo, juntamente com o lema anterior, resolvem por completo o problema da construção de polígonos regulares com régua e compasso, fornecendo uma *caracterização dos polígonos regulares construtíveis*, que esclarece por completo exatamente quando um polígono regular pode ou não ser construído com apenas régua e compasso e é apresentada através do magnífico teorema a seguir, que é o último resultado deste trabalho.

Teorema 26 (Teorema de Gauss-Wantzel)**.** Um n-ágono regular é construtível se, e somente se, n é um produto de uma potência de 2 por primos de Fermat distintos.

Demonstração. Seja $n > 2$ um número inteiro qualquer. Então n pode ser fatorado assim:

$$n = 2^k \cdot p_1^{e_1} \cdot \ldots \cdot p_m^{e_m},$$

onde $k \geq 0$ é um inteiro, $p_i > 2$ é primo e $e_i \geq 0$ é inteiro, para todo $i \in \{1, \ldots, m\}$ e, além disso, $p_i \neq p_j$ se $i \neq j$.

Primeiro suponha que p_i é um primo de Fermat e $e_i = 1$, para todo $i \in \{1, \ldots, m\}$. Então, pelo lema 13, segue dos teoremas 23 e 25 que o n-ágono regular é construtível.

Agora suponha que o n-ágono regular é construtível. Então, pelo lema 13, o $p_i^{e_i}$-ágono é construtível, para todo $i \in \{1, \ldots, m\}$. Segue do teorema 24 que $e_i = 1$ e segue do teorema 23 que p_i é um primo de Fermat, para todo $i \in \{1, \ldots, m\}$. □

O leitor há de concordar que há muito pouco a se dizer depois de tão grandioso resultado. Mesmo que não tenhamos feito todas as demonstrações ao longo do processo, fizemos uma enorme parte do trabalho, e isso nos permite admirar com muito prazer e alegria este resultado final. Além do fato de o teorema acima ser uma solução completa do problema da construção de polígonos regulares, que é algo que se buscou por muito tempo, existe a imensa beleza do fato de que essa caracterização se resume em um produto de uma potência de 2 e certos números primos. O engraçado é que potenciação e números primos são tópicos ensinados no 6º ano do Ensino Fundamental, ou seja, é possível responder de modo plenamente compreensível àquele aluno mais curioso *exatamente quais polígonos regulares podem ser construídos com apenas régua e compasso*, mesmo que seja um aluno do 6º ano! É claro que não é possível demonstrar de modo rigoroso o resultado completo, mas é possível apresentar exemplos de alguns argumentos ao longo do processo em diferentes níveis do ensino, como já foi falado aqui em alguns momentos e como, com sorte, se conseguirá descrever melhor no próximo e último capítulo desta dissertação.

7.4 Quadratura do círculo

Considere um círculo de raio 1. A área desse círculo, pela fórmula $A = \pi r^2$, é igual a π. Então, construir com apenas régua e compasso um quadrado de área igual a π implicaria em construir um segmento de reta cuja medida fosse $\sqrt{\pi}$. Por sua vez, se $\sqrt{\pi}$ fosse um número construtível, então π seria um número construtível. Deste modo, o segredo da solução do problema da quadratura do círculo reside em mostrar que isso é um absurdo, ou seja, que π *não* é um número construtível, assim como foi feito com $\sqrt[3]{2}$ na duplicação do cubo, com $\cos 20^\circ$ na trissecção do ângulo e com $\text{tg}\,\frac{360^\circ}{p}$ na construção de polígonos regulares. Entretanto, esses números presentes nas soluções dos três problemas anteriores são todos *algébricos*, e isso foi a *base para toda a teoria desenvolvida neste trabalho*. Tudo o que foi feito pode ser aplicado apenas para números algébricos! E como já foi falado, o número π não é algébrico.

É possível (e um tanto difícil) provar que π é um *número transcendente*. Devido a isso, a estratégia usada aqui para os outros três problemas *não serve para resolver a quadratura do círculo!* E é esse o comentário que se buscava fazer sobre esse último problema. Agora fica claro que só seria possível explicar isso após toda a teoria vista aqui. Para resolver o problema da quadratura do círculo neste trabalho, seria necessário desenvolver uma outra teoria, o que claramente não é o objetivo desta dissertação. Depois de tudo o que foi feito até este capítulo, fica claro que o objetivo era desenvolver toda a teoria de números construtíveis e de números algébricos para juntar os dois conceitos em um belo e fascinante desfecho.

Foi comentado no capítulo anterior (mas não provado) que todos os números construtíveis são algébricos, o que faz todo o sentido e não é difícil de aceitar, como já mencionado, pois os números construtíveis são resultantes de um processo recursivo de sucessivas interseções de retas e circunferências que se traduzem em equações polinomiais com coeficientes construtíveis, sendo que os coeficientes iniciais dessa recorrência são números racionais. Logo, a estratégia parece simples: basta provar que π é um número transcendente, pois, pela contrapositiva, se π não é algébrico, então π não é construtível! (É claro que para isso também seria necessário provar a afirmação não demonstrada de que todos os números construtíveis são algébricos.)

De fato, se sabia desde muito tempo que a demonstração da transcendência de π significaria a solução do problema da quadratura do círculo. Porém, tal demonstração não é nada simples e levou muito tempo para ser concretizada. É por isso que, na história dos problemas de construção com régua e compasso, a quadratura do círculo foi o último dos três problemas clássicos a ser resolvido, assim como está sendo o último problema a ser mencionado neste trabalho. Foi somente em 1882 que Ferdinand Lindemann provou que π é um número transcendente, e é claro que isso foi muito maior e mais importante do que apenas resolver o problema da quadratura do círculo, pois teve inúmeras outras implicações e aplicações. Ou seja, π não é raiz de nenhum polinômio com coeficientes inteiros. A demonstração de Lindemann foi baseada na primeira

demonstração da transcendência do número de Euler e,

$$e = \sum_{n=0}^{\infty} \frac{1}{n!},$$

que foi feita pelo matemático francês Charles Hermite em 1873.

Desde então, várias demonstrações da transcendência de π foram publicadas. Uma referência para uma demonstração mais simples da transcendência de π é o livro *A transcendência de* π, de Ivan Niven.

CAPÍTULO

8

ALGUMAS APLICAÇÕES NO ENSINO BÁSICO

Lá atrás, quando da ideia inicial de fazer um trabalho sobre os problemas clássicos de construção com régua e compasso, um objetivo era claro: construir de modo simplificado toda a teoria necessária para resolver os problemas da duplicação do cubo, da trissecção do ângulo e da construção de polígonos regulares, de modo a fornecer um texto autocontido, completo e com uma linguagem que fosse o mais acessível possível a um professor do ensino básico e, quem sabe, até mesmo a algum aluno mais interessado. Ou seja, a grande meta era tentar elaborar um caminho mais simples e menos abstrato que o usual, onde fossem usados mais noções e símbolos do currículo do ensino básico e menos conceitos e notações de álgebra abstrata. Além disso, também se idealizava um caminho com maior foco nos exemplos concretos e menor ênfase na teoria abstrata, onde fossem apresentados e provados todos os resultados necessários para se resolver os problemas de construção, porém que fossem acompanhados de exemplos que ilustrassem as ideias de modo concreto. Portanto, dessa perspectiva inicial, a grande *aplicação no ensino básico* seria a entrega de um material completo e acessível para que o professor pudesse estudar e entender as soluções dos problemas de construção com régua e compasso.

Acredita-se que esta aplicação foi entregue ao longo deste trabalho, porém uma observação importante se faz necessária. A primeira parte deste trabalho, que vai do capítulo 1 até o capítulo 4, e se caracteriza pela *caracterização dos números construtíveis* e pelas soluções dos problemas da *duplicação do cubo* e da *trissecção do ângulo*, constitui a parte mais acessível deste trabalho. Apesar de acreditar-se que muitos professores possam estudar esta primeira parte com plena compreensão (e muito esforço e dedicação), o conteúdo completo desta parte seria mais adequado para uma formação de professores, e não diretamente para todos os professores do ensino básico. Porém, ao se ignorar as demonstrações e se concentrar nos exemplos, nos resultados e nas conclusões, o material pode ser utilizado e compreendido de maneira ampla e direta por todos os professores interessados do ensino básico. Assim, a primeira parte fornece

um material completo para um minicurso de licenciatura ou para uma formação específica de professores já atuantes no ensino básico de matemática. Por outro lado, a segunda parte, que vai do capítulo 5 ao capítulo 7, e se caracteriza pelo *critério de construtibilidade* e pela solução do problema da *construção de polígonos regulares*, é realmente mais avançada e muito específica, direcionada a professores do ensino médio que estejam interessados de verdade no assunto e tenham maior nível de estudo e determinação para compreeender os tópicos mais abstratos que a constituem. Ainda assim, olhando apenas os exemplos e as conclusões, é possível que este público-alvo seja ampliado.

Não se pensava exatamente em sequências didáticas ou em um passo a passo específico para o professor seguir com seus alunos em sala de aula. Não, nunca foi esse o sentido de "aplicações no ensino básico" que se buscou neste trabalho. Até mesmo porque a realidade de cada sala de aula e de cada professor é única. Uma vez que o professor compreende os problemas e suas soluções de modo claro e completo, ele pode aplicar em suas salas de aula como achar melhor e, neste momento, a criatividade não tem limites e as aplicações podem variar desde fatos históricos e exemplos simples das ideias presentes nas soluções até mesmo resultados mais elaborados e demonstrações. Deste modo, neste capítulo, busca-se fornecer algumas ideias gerais e sugestões de possíveis aplicações no ensino básico, que de repente possam orientar o professor a elaborar sequências didáticas detalhadas de acordo com a realidade de sua turma, ideias essas que o professor pode modificar parcial ou completamente. Com esperança, essas sugestões, assim como o texto de todos os capítulos até aqui, inspirarão várias outras ideias, de modo a enriquecer o ensino de matemática e contribuir na disseminação das soluções dos problemas clássicos de construção com régua e compasso e da álgebra requintada que faz parte das mesmas, que é o grande propósito deste trabalho.

8.1 História, lendas e mitos

Os alunos sempre fazem perguntas curiosas, principalmente as crianças. Às vezes, na sala de aula, nós professores nos deparamos com algumas perguntas inusitadas e outras vezes com perguntas simples que nos fazem refletir sobre o porquê de não termos pensado naquilo antes. Ao enunciar os problemas de construção com régua e compasso em sala de aula, podem surgir perguntas como "Onde surgiram esses problemas?", "Por que podemos usar apenas régua e compasso?" ou ainda "Para que servem essas construções?", perguntas essas que são simples de se formular e difíceis de se responder, assim como os próprios problemas de construção que estudamos neste trabalho. É interessante que o professor saiba responder a essas questões, não apenas pela possibilidade de elas surgirem em sala de aula, mas porque as respostas a esses questionamentos podem ser uma oportunidade de introduzir o contexto e a história dos problemas de construção com régua e compasso, e assim envolver os alunos e melhorar sua compreensão, tornando o assunto mais interessante e enriquecedor. Na introdução deste trabalho, buscamos

contar um pouco sobre a origem dos problemas e sobre a restrição ao uso de régua e compasso. São questões difíceis de responder porque a história não fornece teoremas a seu respeito, e sim hipóteses. É interessante que o professor tenha isso em mente de modo claro, para não passar informações erradas aos alunos e diferenciar mitos e lendas dos fatos comprovados. Por isso, vale a pena ressaltar dois pontos principais sobre a história dos problemas de construção com régua e compasso.

- *A origem dos problemas é incerta*: São problemas muito antigos, que estão envoltos em lendas e mitos, o que dificulta determinar com certeza como e onde surgiram, mas sabe-se que sua fama cresceu muito com o estudo desses problemas realizado pelos gregos antigos.
- *O motivo da restrição ao uso da régua e do compasso também é incerto*: Não era uma regra presente em toda a geometria dos gregos antigos e na introdução deste trabalho foram apresentadas algumas hipóteses mais prováveis sobre o uso desses instrumentos em *Os Elementos*, de Euclides. Porém é interessante que o professor não promova como fato o mito de que a razão está ligada a Platão, como já se acreditou no passado. O professor pode até contar como sendo um mito e dizer que por um tempo se acreditou erroneamente na ideia platônica, pois apesar dos pesares é uma ideia bonita e que pode provocar a curiosidade dos alunos através de um mistério que se conecta à filosofia e a outras áreas do conhecimento. Mas é importante que o professor reforce que se trata apenas de um mito e destaque as hipóteses mais prováveis sobre o uso de régua e compasso. Inclusive, pode ser um bom momento para o professor falar aos alunos da obra *Os Elementos* e explicar os métodos utilizados no livro, indicando as prováveis motivações de Euclides ao utilizar somente retas e círculos nas construções ali apresentadas.

Ainda pensando nas perguntas “Onde surgiram esses problemas?” e “Para que servem essas construções?”, o professor pode se valer ainda de outros mitos e lendas para envolver ainda mais os alunos e aguçar a sua curiosidade, mas é interessante que sempre se faça a distinção do que é fato histórico e do que é lenda. Um exemplo notável é contar que o problema da duplicação do cubo também é conhecido como *problema deliano*, como Roque (2012, p. 155) explica:

> (...) Com relação à duplicação do cubo, existe uma lenda segundo a qual em 427 a.E.C. Péricles teria morrido de peste juntamente com um quarto da população de Atenas. Consternados, os atenienses consultaram o oráculo de Apolo, em Delos, para saber como enfrentar a doença. A resposta foi que o altar de Apolo, que possuía o formato de um cubo, deveria ser duplicado. Prontamente, as dimensões do altar foram multiplicadas por 2, mas isso não afastou a peste. O volume havia sido multiplicado por 8, e não por 2. A partir dessa lenda, o problema que consiste em, dada a aresta de um cubo, construir só com régua e compasso a aresta de um segundo cubo tendo o dobro do volume do primeiro, ficou conhecido como *problema deliano*.

8.2 Ideias para trabalhar alguns aspectos em sala de aula

Há vários grandes teoremas que os alunos aprendem desde cedo, sem demonstração e sem nem mesmo o rigor matemático da apresentação desses resultados. Por exemplo, é ensinado no 6º ano do Ensino Fundamental que todo número pode ser decomposto de modo único em um produto de fatores primos, embora não se faça a demonstração do Teorema Fundamental da Aritmética. De modo análogo, é possível apresentar alguns resultados deste trabalho em diferentes etapas do ensino básico, sem a necessidade de demonstrá-los, e até mesmo sem o rigor e a pompa com que eles foram apresentados aqui. Por exemplo, pode-se apresentar exemplos concretos e apresentar versões simplificadas que podem levar o aluno a entender a ideia mais geral, mas sem essa necessidade. Assim, o professor não precisa apresentar os detalhes algébricos para seus alunos para que a impossibilidade das construções com régua e compasso esteja presente no processo de ensino-aprendizagem. O interessante é que o professor entenda ele próprio os pormenores das soluções dos problemas de construção. Quanto maior for a compreensão do professor, melhor ele poderá selecionar e apresentar o que for mais adequado ao seu público, seja ele formado por alunos do Ensino Fundamental ou do Ensino Médio. A seguir serão apresentadas algumas ideias e sugestões na forma de exemplos.

Exemplo 13 (Apresentação dos problemas)**.** Um dos modos mais divertidos de introduzir os problemas de construção com régua e compasso é, sem dúvidas, a construção de um triângulo equilátero com régua e compasso, que é simples e elegante. O professor pode propor à turma o seguinte problema, sem especificar as ferramentas de construção: "Vocês conseguem desenhar um triângulo equilátero?" Uma boa ideia para propor este problema é dividir os alunos em grupos e usar a metodologia de ensino-aprendizagem de matemática através da resolução de problemas. Surgirão os mais diversos processos, desde uso da régua para medir os lados e fazer aproximações até mesmo uso de materiais escolares, como lápis e canetas, para auxiliar na construção. Neste momento, o professor pode permitir o uso de quaisquer instrumentos para a construção. Os alunos podem então apresentar suas soluções na lousa e o professor pode promover uma discussão, com o objetivo de se chegar a um consenso entre as diversas ideias dos alunos. Após a obtenção desse consenso, o professor pode dizer que *usando apenas uma régua sem marcações e um compasso*, os gregos antigos conseguiam construir um triângulo equilátero perfeito e também faziam várias outras construções geométricas, sem a tecnologia que temos hoje em dia. E então o professor pode apresentar a construção de um triângulo equilátero com régua e compasso, que é uma construção fácil de entender e ao mesmo tempo tem um resultado visual elegante, constituindo assim uma excelente porta de entrada ao universo das construções geométricas com régua e compasso em todas as idades. Esta etapa onde o professor apresenta a construção de um triângulo equilátero com régua e compasso constituirá uma etapa de formalização do conteúdo, onde o professor explicará as "regras do jogo", ou seja, o que se pode fazer com uma régua sem marcações (*retas*) e o que se pode fazer com um compasso (*círculos*). Neste momento, o professor também exemplifica através da construção do triângulo

equilátero porque o triângulo obtido possui todos os lados de mesma medida. Após esta etapa de formalização do conteúdo, o professor pode promover novos problemas, como por exemplo a construção de um quadrado ou de um hexágono regular, a depender, é claro, do público-alvo em questão. Fato é que, em algum momento após a construção do triângulo equilátero, o professor pode apresentar o *problema mais geral da construção de um polígono regular qualquer*. É possível explicar aos alunos que por muito tempo os matemáticos tentaram obter um modo de construir um n-ágono regular qualquer usando somente régua e compasso, e a partir disso contar a história narrada neste trabalho, do modo como for mais adequado ao seu público-alvo, mesmo que seja apenas contando o lado histórico e o resultado final. Ou seja, pode ser contado como Gauss apresentou uma condição suficiente para a construção de um n-ágono regular e como Wantzel provou que essa condição é também necessária, e então pode ser apresentado o *Teorema de Gauss-Wantzel* sem demonstração. Para se apresentar este teorema, também pode ser um bom momento para introduzir o que é um *número primo de Fermat*, que é um conceito simples e fácil de entender e visualizar com exemplos.

Uma vez explicadas as regras do uso de régua e compasso e uma vez que os alunos têm pelo menos um exemplo de construção com estes instrumentos, para apresentar o *problema da trissecção do ângulo*, o professor pode propor o seguinte problema: "Se eu lhe der um ângulo qualquer, você consegue dividir esse ângulo em duas partes iguais usando apenas régua e compasso?" A introdução deste problema em sala de aula também pode ser conduzida através da metodologia de ensino-aprendizagem de matemática através da resolução de problemas. Mas independentemente da metodologia utilizada, após o professor apresentar a bissecção de um ângulo qualquer com apenas régua e compasso e formalizar o conteúdo, pode introduzir o problema da trissecção do ângulo, e então contar a história e o desfecho do mesmo, nomeando como um dos *três problemas clássicos de construção*. De modo análogo, para apresentar o *problema da duplicação do cubo*, o professor pode propor o seguinte problema: "Se eu lhe der um quadrado qualquer, você consegue construir um novo quadrado cuja área seja o dobro da área do quadrado inicial?" E assim apresentar a "duplicação do quadrado" usando somente régua e compasso. Isso pode ser um bom ponto de partida para apresentar o problema da duplicação do cubo ou problema deliano. Este problema é bem interessante e pode provocar a curiosidade dos alunos devido à sua história envolta em lendas e mitos, e também é um dos três problemas clássicos de construção.

Para os três problemas citados anteriormente, é razoável imaginar aplicações para a construção de um triângulo equilátero, para a bissecção de um ângulo e para a duplicação de um quadrado, e por isso estes constituem bons exemplos iniciais para se introduzir os problemas da construção de polígonos regulares, da trissecção do ângulo e da duplicação do cubo, respectivamente. Porém, não é igualmente razoável entender a utilidade de se construir um quadrado que tenha a mesma área que outra figura geométrica. De fato, um dos modos de entender a importância deste problema é conhecer como os gregos antigos mediam áreas de

figuras planas. Por exemplo, imagine que os gregos quisessem calcular a área de um pentágono. Para isso, eles não associavam um número ao pentágono como fazemos hoje em dia e sim tentavam obter uma figura plana que fosse mais simples e que tivesse a mesma área que o pentágono inicial. E essa figura mais simples era o *quadrado*. Ou seja, para obter a área de uma figura plana qualquer, os gregos antigos tentavam encontrar um quadrado que tivesse a mesma área que a figura inicial, e esse era o problema de encontrar a *quadratura* da figura dada. Uma vez explicado este contexto, fica fácil entender o porquê da importância do *problema da quadratura do círculo*, que é o terceiro dos três problemas clássicos de construção. Deste modo, essa explicação pode ser um bom modo de introduzir o problema da quadratura do círculo usando somente régua e compasso. Neste contexto de "áreas equivalentes", pode ser feito um paralelo com a importância do *Teorema de Pitágoras*, que pode ser visto como uma ferramenta para o cálculo de áreas. Roque (2012) apresenta uma demonstração do Teorema de Pitágoras que usa a ideia de "áreas equivalentes" e pode ser trabalhada com um público-alvo mais avançado para mostrar a importância do problema da quadratura de uma figura geométrica.

Exemplo 14 (Problemas impossíveis)**.** No momento de explicar sobre as soluções dos problemas de construção com régua e compasso, surgirá a necessidade de explicar que esses problemas foram resolvidos e que suas soluções mostram que é impossível fazer essas construções, o que pode ser feito através de uma analogia com um exemplo mais simples, como por exemplo o problema proposto na introdução deste trabalho: *Obter um quadrado de lado inteiro cuja área seja igual a um número natural dado*. Neste caso, a explicação pode ser feita como no primeiro capítulo desta dissertação. Como mencionado naquele capítulo, uma interessante versão alternativa deste problema seria a seguinte: *Obter um quadrado de lado racional cuja área seja igual a um número dado*. O enunciado desta versão é mais simples porque não apresenta restrição no número dado e sim apenas a restrição do quadrado que se deseja construir. Porém, o ponto de interesse nessa versão é que ela permite trabalhar a irracionalidade de $\sqrt{2}$. Então seria interessante trabalhar essa versão em uma etapa onde os alunos já conhecessem a diferença entre números racionais e irracionais, e soubessem que $\sqrt{2}$ não é racional. Seria muito enriquecedor, pois constituiria uma aplicação do fato de que a raiz quadrada de 2 é um número irracional.

Exemplo 15 (Números construtíveis)**.** Ao falar de construções com régua e compasso, o professor pode dar uma ideia do que são pontos construtíveis como os pontos que são obtidos através de interseções de retas e círculos construídos a partir de pontos previamente construídos com régua e compasso. A partir daí, fica fácil definir número construtível como sendo a coordenada de algum ponto construtível. É uma ótima ideia dar alguns exemplos de números construtíveis, fazendo a construção dos mesmos. Inclusive, este é o modo mais concreto de introduzir o conceito, e já permite fazer o seguinte questionamento na sequência: *Quais números são construtíveis?* E então o professor pode fazer a sequência de construções apresentada no exemplo 3 do capítulo 3, que induzirá o aluno a concluir de modo intuitivo que *número construtível* é sinônimo de *expressão com radicais de índice 2*. E este fato é suficiente para o entendimento do aluno. É

claro que não se falará em extensões quadráticas iteradas de $\mathbb{Q}$. Basta que o aluno saiba que todas as expressões com radicais de índice 2 são números construtíveis e que todos os números construtíveis são expressões com radicais de índice 2.

Exemplo 16 (Soluções dos problemas)**.** Com certeza, o problema que tem a solução mais simples de exemplificar é a duplicação do cubo. Para duplicar o cubo unitário, é necessário construir um segmento de reta cuja medida elevada ao cubo seja igual a dois, ou seja, o número $\sqrt[3]{2}$ deve ser um número construtível. E então pode ser explicado de modo informal aos alunos que é possível provar que esse número não é construtível, pois não pode ser escrito através de uma expressão com radicais de índice 2. Através do exemplo 3 do capítulo 3, talvez seja uma tarefa fácil convencer o aluno de que não será possível aparecer uma raiz cúbica onde, após várias construções, apareceram apenas raízes quadradas. Deste modo, o aluno perceberá de modo informal, porém concreto, que não é possível construir um segmento de reta cuja medida seja igual a $\sqrt[3]{2}$, e portanto é impossível duplicar o cubo unitário. De maneira análoga, é possível dar uma ideia da impossibilidade da trissecção do ângulo, embora neste caso o convencimento será um pouco mais difícil, pois o número que aparece é $\cos 20^\circ$, que dá um pouco mais de trabalho argumentar, mesmo que informalmente, que não é construtível, e é menos intuitivo do que a raiz cúbica de 2.

Exemplo 17 (Equações cúbicas)**.** Seguindo na linha do exemplo anterior, é possível aproveitar a deixa da trissecção do ângulo para falar da aplicação de equações cúbicas na resolução dos problemas de construção com régua e compasso. É comum os alunos perguntarem sobre equações de grau maior após estudarem equações do 1º e do 2º grau na escola. Então pode ser um bom momento para falar do surgimento de equações cúbicas, ou seja, equações do 3º grau, na resolução da duplicação do cubo e da trissecção do ângulo. Podem ser apresentados aos alunos os mesmos desenvolvimentos feitos no capítulo 4 para se obter a *equação da duplicação* e a *equação da trissecção*, embora a da trissecção possa ser feita apenas para alunos do Ensino Médio, enquanto que a equação da duplicação é mais acessível. Além de servir como exemplos de equações do 3º grau, as equações da duplicação e da trissecção constituem um ótimo exemplo de aplicação das equações. É interessante contar que os matemáticos tentavam resolver os problemas da duplicação do cubo e da trissecção do ângulo desde o século V a.C. aproximadamente, mais de dois mil anos atrás, e naquela época não se tinha as equações como se tem hoje, e só após muito tempo, com o desenvolvimento do estudo de equações, os matemáticos conseguiram resolver esses problemas de construção, provando que não é possível fazer essas construções geométricas, conforme explicamos neste trabalho. Pode ser um bom momento também para mostrar aos alunos como geometria e álgebra se misturam, e não são duas coisas separadas como as apostilas da escola apresentam. É tudo uma coisa só, é tudo matemática! Para finalizar, para concluir a apresentação informal da solução da trissecção do ângulo, pode ser explicado aos alunos que os matemáticos provaram que a equação da trissecção não possui nenhuma raiz construtível e que daí se deduz que $\cos 20^\circ$ *não* é um número construtível e que, portanto, é impossível fazer a

trissecção do ângulo de 60°.

Com todos os exemplos apresentados neste capítulo, já é possível montar uma narrativa boa e bem ilustrativa, que pode fazer o aluno compreender e aplicar os conhecimentos matemáticos que são ensinados na escola e muitas vezes soam muito abstratos. As soluções dos problemas de construção com régua e compasso representam aplicações importantes dos conceitos ensinados na escola, que podem ajudar a dar sentido e significado para o aluno. Destas ideias podem surgir várias outras ideias. Uma vez que a gente entende e aprecia, consegue passar ao aluno muita coisa legal, que pode provocar a curiosidade e fazer o mesmo se interessar mais por matemática. Além de os problemas de construção com régua e compasso servirem como motivação para o estudo de matemática, ao introduzi-los em sala de aula, o professor estará contribuindo para a disseminação das soluções destes problemas, que é algo valioso por si só, visto que as mesmas ilustram bem o avanço da matemática ao longo dos séculos.

8.3 Considerações finais

O grande objetivo deste trabalho foi cumprido (e comprido!): construir de modo simplificado toda a teoria necessária para resolver os problemas da duplicação do cubo, da trissecção do ângulo e da construção de polígonos regulares, de modo a fornecer um texto autocontido, completo e com uma linguagem que fosse o mais acessível possível a um professor do ensino básico e, quem sabe, até mesmo a algum aluno mais interessado. Com mais tempo, eu teria preenchido mais o texto com algumas demonstrações, como por exemplo da parte de polinômios, e quem sabe até mesmo alguma coisa sobre a parte de Gauss no Teorema de Gauss-Wantzel. E poderia ter detalhado mais as ideias de aplições no ensino básico. Porém este tempo tenderia ao infinito, assim como o comprimento deste trabalho!

A grande *aplicação no ensino básico* é a entrega de um material completo e acessível para que o professor possa estudar e entender as soluções dos problemas de construção com régua e compasso. Espera-se que as ideias gerais de aplicações no ensino básico possam orientar o professor a elaborar sequências didáticas detalhadas de acordo com a realidade de sua turma. Com esperança, essas sugestões, assim como o texto de todos os capítulos até aqui, inspirarão várias outras ideias, de modo a enriquecer o ensino de matemática e *contribuir na disseminação das soluções dos problemas clássicos de construção com régua e compasso e da álgebra requintada que faz parte das mesmas, que é o grande propósito deste trabalho.*

Na graduação, esses problemas foram estudados superficialmente como uma aplicação de alguns conceitos de álgebra abstrata. Ao fazer o estudo de modo detalhado e com a visão de professor do ensino básico, a experiência foi completamente diferente e me fez perceber *nuances* que eu não havia notado antes. Eu tive a sensação que finalmente entendi as soluções destes problemas. Compreendi quais são os pontos principais das mesmas, diferenciando-os do que é formalização de ideias, e pude ver o que é passível de simplificação.

Com a conclusão do trabalho, eu posso levar muitos tópicos legais de *álgebra abstrata* para a sala de aula, de diversas maneiras e em todos os níveis, como por exemplo o Teorema de Gauss-Wantzel, que é um resultado ao mesmo tempo magnífico e simples de ser enunciado. Sendo assim, o PROFMAT contribuiu imensamente para a minha formação. Através do mestrado, veio uma mudança profunda: a geometria, que muitas vezes é deixada de lado por alguns professores (ocupando assim um espaço mínimo no currículo), é a nossa melhor aliada para tornar a matemática mais concreta e assim ensinar tópicos de álgebra de maneira mais efetiva. A geometria pode ser a motivação e inspiração que faltavam para que os alunos aprendam letras e equações de maneira totalmente descontraída e até mesmo divertida. O professor Alan conclui esta dissertação com uma visão muito ampliada do que pode ser a matemática em sala de aula e o que pode ser feito para que os alunos se envolvam mais com essa disciplina, que soa muitas vezes abstrata e distante da realidade dos alunos. É possível que mostremos que é justamente o contrário: a matemática pode ser muito concreta e está presente em tudo ao nosso redor.

REFERÊNCIAS

BOLD, B. **Famous problems of geometry and how to solve them**. New York: Dover Publications, Inc., 1982. Citado na página 30.

KAZARINOFF, N. D. **Ruler and the Round: Classic Problems in Geometric Constructions**. New York: Dover Publications, Inc., 2003. Citado nas páginas 24, 28 e 33.

ROQUE, T. **História da Matemática: uma visão crítica, desfazendo mitos e lendas**. Rio de Janeiro: Jorge Zahar Editor Ltda., 2012. Citado na página 24.


ICMC
USP
SÃO CARLOS