Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Álgebra motivada pela Geometria

Denis Fermino

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática Universitária como requisito parcial para a obtenção do grau de Mestre

Orientador
Prof. Dr. Vanderlei Marcos do Nascimento

2013

TERMO DE APROVAÇÃO

Denis Fermino

Álgebra motivada pela Geometria

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Prof. Dr. Vanderlei Marcos do Nascimento
Orientador

Prof. Dr. Thiago de Melo
Departamento Matemática - UNESP/Rio Claro

Profª. Drª. Rita de Cássia Pavani Lamas
Departamento de Matemática - UNESP/São José do Rio Preto

Rio Claro, 09 de Dezembro de 2013

Dedico aos meu pais,
Sebastião Fermino e Sueli Pedroso Fermino.

Agradecimentos

Agradeço a Deus por ter me dado suporte para concluir este trabalho. Aos meus pais que sempre estiveram me apoiando em todas as circunstâncias. Aos amigos que estiveram por perto vivenciando minhas angustias e alegrias em todo este processo e aos que não tão próximos literalmente, mas estiveram intercedendo por mim. De modo especial, ao Prof. Vanderley Marcos do Nascimento por ter acreditado em mim e me dado esta oportunidade. Ao Prof. Dr. Thiago de Melo e a Prof^{a}. Dr^{a}. Rita de Cássia Pavani Lamas pelos auxílios e opiniões. Mais uma vez a Deus por ter colocado grandes pessoas no meu caminho para que eu pudesse crescer mais.

A mente que se abre para um nova ideia jamais voltará ao seu tamanho original.

Albert Einstein

Resumo

Este trabalho se inicia em busca de uma resposta para a construtibilidade de números reais baseado nas construções fundamentais no plano com compasso e uma régua não graduada. Com a tal resposta apresentamos uma solução para os três problemas Gregos. Para dar uma solução para um outro problema Grego famoso, o problema de construir polígonos regulares, reunimos conceitos e resultados da Algebra que são fundamentais na formulação algébrica da construtibilidade geométrica. Com estes resultados, apresentamos uma condição necessária para o n-ágono regular ser construtível.

Palavras-chave: Construtibilidade, Polinômio, Extensão.

Abstract

This work begins in search of an answer to the constructability of real numbers based on the fundamental constructions in the plane using compass and no graduated ruler. With this response we present a solution to the three Greek problems. To give a solution to another famous Greek problem, the construction of regular polygons, we 've used some Algebra concepts and results that are fundamental in algebraic formulation of geometric constructability. With these results, we shows a necessary condition to the regular polygons being constructible.

Keywords: Constructibility, Polynomials, Extension.

Lista de Figuras

Sumário

Introdução

Problemas de construções geométricas sempre foram um assunto predileto da Geometria. Com a utilização apenas da régua e do compasso, uma grande diversidade de construções pode ser executada. Contudo, provas da impossibilidade de construções são, em geral, difíceis de serem obtidas via argumentos geométricos. Os três problemas gregos clássicos e a questão de construtibilidade de polígonos regulares desempenharam papel fundamental no desenvolvimento de grande parte da Matemática. A simplicidade com que esses problemas podem ser enunciados é uma forte aliada para motivação no ensino da Matemática. Contudo, o tratamento que a maioria dos textos dá para o assunto apresenta-o como um subproduto da Teoria de Galois, a qual, em geral, não é apresentada nos cursos de Licenciatura. Assim, torna-se interessante disponibilizar um texto que apresenta um tratamento alternativo. Isso é feito de forma bastante interessante na referência básica para este trabalho que é [1]. De nossa parte, a maioria das vezes, nos propusemos a explicitar mais detalhes técnicos; noutras vezes explicitamos passos conceituais que acreditamos colocar mais luz sobre o assunto.

No Capítulo 1 apresentamos a tradução algébrica da construtibilidade geométrica e, segundo ela, abordamos os problemas gregos clássicos. Ainda que essa abordagem possa ser considerada motivadora para os próximos capítulos, a intensidade dessa motivação é de difícil quantificação já que em casos particulares podemos utilizar argumentos específicos. Perceber que esses argumentos são, de fato, particularidades é que faz grandiosa a teoria que os contemplam como tais. Apenas no Capítulo 3 é que poderemos apreciar essa grandiosidade; todo o Capítulo 2 é dedicado a apresentar os conceitos da Álgebra que serão ferramentas para isso. No Capítulo 3, além de considerar os problemas gregos clássicos sob um novo olhar, também abordaremos a questão de construtibilidade dos polígonos regulares sob esse novo olhar.

1 Os Três Problemas Gregos

1.1 Comprimentos Construtíveis

Um passo importante para abordar os problemas gregos clássicos de construções geométricas será dado nesta seção, na qual devemos responder a seguinte questão: **Dado um segmento de reta de comprimento 1 no plano, para quais $a \in \mathbb{R}$ podemos construir um segmento de comprimento a?**

Como usual na Geometria, devemos considerar comprimentos sendo não-negativos. Naturalmente, precisamos pôr um olhar muito cuidadoso para as regras que regem às construções. Construção será entendida como sendo uma sequência finita de passos com um compasso ou com uma régua não graduada.

Os passos que podem ser feitos com estes instrumentos são chamadas de *construções fundamentais*. São eles:

1. Dados 2 pontos, podemos desenhar um segmento de reta unindo eles.
2. Dados 2 pontos, o segmento da reta que os une pode ser estendido ao longo dessa reta tanto quanto desejado.
3. Dados um ponto e um segmento de reta, podemos desenhar um círculo centrado nesse ponto e de raio igual ao comprimento do segmento tomado.

Seguirá facilmente do Lema 1.1 que dado um segmento de comprimento unitário, todo segmento de comprimento racional é construtível. Vejamos:

Lema 1.1. *Dados segmentos de comprimento* 1, a *e* b, *é possível construir segmentos de comprimento* $a+b$, $a-b$ *(quando* $a>b$*),* ab, *e* a/b *(quando* $b \neq 0$*).*

Demonstração. Considere uma reta s. Sobre ela, marque o segmento AB de comprimento a e o segmento BC de comprimento b. Construa uma circunferência com centro em B e raio BC. Logo, a circunferência intercepta s nos pontos C e D tais que B está entre A e C, e D está entre A e B. Como BD tem o mesmo comprimento que BC, o segmento AD tem comprimento $a-b$ e AC tem comprimento $a+b$.

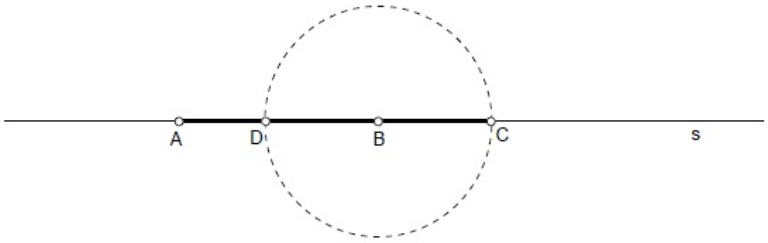

Figura 1.1: Segmento AD de comprimento $a - b$ e AC de comprimento $a + b$.

Para obtermos ab, primeiro construímos duas semirretas não colineares de mesma origem P. Sobre uma destas semi-retas marquemos o segmento PA de comprimento a e na outra, o segmento PB de comprimento 1. Conectemos as extremidades dos segmentos, formando o triângulo ΔPBA. Sobre a semirreta na qual o comprimento 1 foi marcado, marquemos o segmento BC de comprimento b.

Se uma semirreta é construída através do ponto C paralela ao lado AB do ΔAPB, ela intercepta a semirreta que passa por PA em um ponto D criando um segmento AD. Pelo teorema de Tales, $\frac{a}{1} = \frac{AD}{b}$. Logo, $ab = AD$.

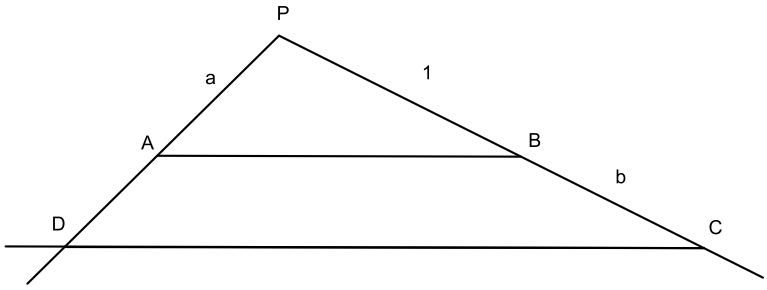

Figura 1.2: Segmento AD de comprimento ab.

Para obtermos a/b, analogamente construímos duas semirretas não colineares de origem P. Sobre uma dessas semirretas marquemos o segmento PA de comprimento a e na outra, o segmento PB de comprimento b. Conectemos as extremidades dos segmentos, formando o triângulo ΔPBA. Sobre a semirreta no qual o comprimento b foi marcado, marquemos o segmento BC de comprimento 1.

Se uma semirreta é construída através do ponto C paralela ao lado AB do ΔAPB, ela intercepta a semirreta que passa por PA em um ponto D criando um segmento AD. Pelo teorema de Tales, $\frac{a}{b} = \frac{AD}{1}$. Logo, $a/b = AD$.

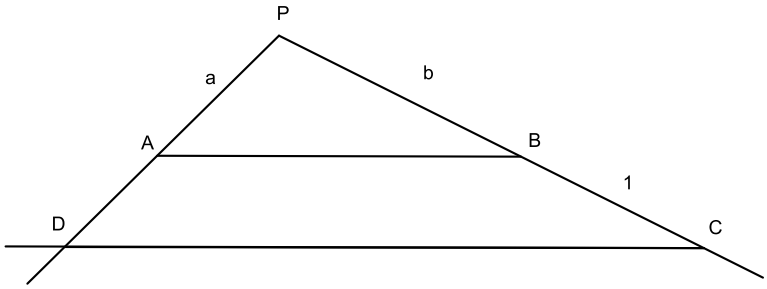

Figura 1.3: Segmento AD de comprimento a/b.

□

Chamamos um número real a de construtível *se $a = 0$ ou se, dado um segmento de comprimento 1, é possível construir um segmento de comprimento $|a|$.*

Pelo Lema 1.1, se $x, y \in \mathbb{R}$ são números construtíveis, podemos concluir que $x + y$, $x - y$, xy e x/y com $y \neq 0$ também são construtíveis.

Disto, segue que todos os números racionais são construtíveis, pois qualquer número inteiro pode ser construído por adição ou subtração de um número apropriado de 1's e assim, qualquer quociente de inteiros pode ser obtido (números racionais).

Seja F um subconjunto dos números reais. Dizemos que F é um corpo se ele satisfaz duas condições:

(1) F é fechado sob as "operações racionais"(adição, subtração, multiplicação e divisão), isto é, sempre que estas operações são aplicadas a pares de elementos de F, o resultado é um elemento de F.

(2) O número 1 é um elemento de F. (Tal condição exclui os casos: $F = \emptyset$ e $F = \{0\}$).

Vale observar que sendo as operações em F aquelas de $\mathbb{R}$, as propriedades distributiva e associativa valem para os elementos de F.

É claro que o conjunto dos números racionais $\mathbb{Q}$ e dos números reais $\mathbb{R}$ são corpos, e pelo Lema 1.1 o conjuntos dos números construtíveis também é um corpo.

Em nossa busca de uma descrição para números construtíveis, é importante notar que é possível, utilizando-se apenas elementos do corpo F construir um elemento que não pertence ao corpo F. Este é o caso em que F não é fechado sob a operação de extrair a raiz quadrada de um número positivo:

Lema 1.2. *Dados segmentos de comprimentos 1 e a, um segmento de comprimento $\sqrt{a}$ pode ser construído.*

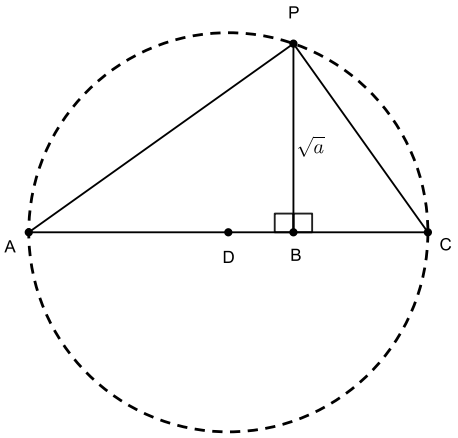

Figura 1.4: Construção da raiz quadrada de um comprimento a.

Demonstração. Considere uma reta s. Sobre ela marque o segmento AB de comprimento a e o segmento BC de comprimento 1 com $A-B-C$. Marque o ponto D sobre s como sendo o ponto médio do segmento AC. Trace a circunferência de centro em D e raio AD. Trace a reta perpendicular a s passando por B de modo a interceptar a circunferência em um ponto P. Assim, o segmento BP terá comprimento $\sqrt{a}$ pela semelhança entre os triângulos $\triangle ABP$ e $\triangle PBC$. □

Pelos lemas 1.1 e 1.2, se todos os números de um corpo F são construtíveis, então todos os números da forma $a+b\sqrt{k}$ também são, onde a, b e k pertencem a F e $k>0$.

É claro, se $\sqrt{k}$ está em F, esse conjunto é simplesmente o próprio F. Mas se $\sqrt{k}$ não está em F, este novo conjunto contém F como um subconjunto próprio. Neste caso $F(\sqrt{k})$ é chamado de uma *extensão quadrática de* F.

Lema 1.3. *Se F é um corpo e se $k \in F$, $k>0$, então $F(\sqrt{k})$ também é um corpo.*

Demonstração. Como $1 \in F$, $1 \in F(\sqrt{k})$. Tudo que precisamos mostrar agora é que a soma e o produto de elementos de $F(\sqrt{k})$ estão em $F(\sqrt{k})$ (ou seja, $F(\sqrt{k})$ é fechado sob as operações racionais).

Sejam a, b, c e d pertencentes F.

(1) soma: $(a+b\sqrt{k}) + (c+d\sqrt{k}) = (a+c) + (b+d)\sqrt{k}$,

(2) produto: $(a+b\sqrt{k})\,(c+d\sqrt{k}) = (ac+bdk) + (ad+bc)\sqrt{k}$. □

Sabemos agora que todo número racional é construtível e que todo número que pode ser calculado a partir de racionais por uma sequência finita de operações racionais ou de extração de raiz quadrada também é construtível. Por exemplo, o número $\sqrt[4]{13} + \frac{4}{3}\sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}}$ é construtível. Podemos construí-lo com a seguinte sequência de operações:

$$7, \sqrt{7}, \sqrt{7}+\sqrt{7} = 2\sqrt{7}, 1, 1+2\sqrt{7}, \sqrt{1+2\sqrt{7}},$$
$$6, \sqrt{6}, \sqrt{6}+\sqrt{1+2\sqrt{7}}, \sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}}, \frac{4}{3},$$
$$\frac{4}{3}\sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}}, 13, \sqrt{13}, \sqrt{\sqrt{13}} = \sqrt[4]{13},$$
$$\sqrt[4]{13} + \frac{4}{3}\sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}}.$$

Estas operações podem ser convenientemente reescritas em termos de corpos:

Lema 1.4. *Seja $a \in F$. Se existe uma sequência finita de corpos $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n$, com $a \in F_n$, tal que para cada j, $0 \leqslant j \leqslant n-1$, F_{j+1} é uma extensão quadrática de F_j, então a é construtível.*

Demonstração. Por indução sobre n. Temos que se $n = 0$, a é racional e portanto construtível. Supondo agora que o teorema é válido para $n = r$, mostremos que ele é válido para $n = r+1$. Seja $a \in F_{r+1}$. Logo, a é da forma $a = a_r + b_r\sqrt{k_r}$. Pela construção de F_{r+1}, a_r, b_r e k_r pertencem a F_r. Por hipótese de indução, F_r é construtível e portanto todos seus elementos são construtíveis. Pelos Lemas 1.1 e 1.2, segue que $a = a_r + b_r\sqrt{k_r}$ é construtível. □

Como exemplo, uma tal sequência de corpos para o número $\sqrt[4]{13}+\frac{4}{3}\sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}}$, temos a seguinte:

$$F_0 = \mathbb{Q}, F_1 = F_0(\sqrt{7}), F_2 = F_1(\sqrt{1+2\sqrt{7}}),$$
$$F_3 = F_2(\sqrt{6}), F_4 = F_3(\sqrt{\sqrt{6}+\sqrt{1+2\sqrt{7}}}),$$
$$F_5 = F_4(\sqrt{13}), F_6 = F_5(\sqrt{\sqrt{13}}).$$

O lema 1.4 dá uma condição suficiente para um número ser construtível. Seria também, esta condição necessária? A resposta é sim. A fim de ver isso, vamos fazer uso de um pouco de geometria analítica elementar.

Se F é um corpo, o conjunto de todos os pontos (x, y) no plano Cartesiano tais que x e y estão em F será denominado como *plano de* F e denotado por F^2. A idéia é que, quando os elementos de F são construtíveis, também são os elementos de F^2 os quais fornecem pontos para novas construções, conforme as definições 1.1 e 1.2.

Um subconjunto $S \subset \mathbb{R}^2$ é dito ser uma reta em $\mathbb{R}^2$, se S é o conjunto solução de uma equação da forma

$$ax + by + c = 0,$$

com a, b e c constantes, sendo $a \neq 0$ ou $b \neq 0$, e x, y incógnitas.

(Nesse caso, dizemos que $ax + by + c = 0$ é uma equação de S).

Definição 1.1. *Uma reta S em $\mathbb{R}^2$ é dita ser uma $F-$reta se existem $(x_1, y_1) \neq (x_2, y_2) \in F^2$ tais que $(x_1, y_1) \in S$ e $(x_2, y_2) \in S$.*

Um subconjunto $S \subset \mathbb{R}^2$ é dito ser uma circunferência em $\mathbb{R}^2$, se S é o conjunto solução de uma equação da forma

$$x^2 + y^2 + ax + by + c = 0,$$

com a, b, c constantes sendo, $\dfrac{a^2}{4} + \dfrac{b^2}{4} - c > 0$ e x, y incógnitas.

Proposição 1.1. *Um subconjunto $S \subset \mathbb{R}^2$ é uma circunferência se, e somente se, existem $(x_1, y_1) \neq (x_2, y_2) \in \mathbb{R}^2$ tais que S é o conjunto solução de uma equação da forma*

$$(x - x_1)^2 + (y - y_1)^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2.$$

Demonstração. ($\Rightarrow$) Seja $S \subset \mathbb{R}^2$. Suponha que existam $(x_1, y_1) \neq (x_2, y_2) \in \mathbb{R}^2$ tais que S é o conjunto solução de

$$(x - x_1)^2 + (y - y_1)^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2.$$

Temos,

$$x^2 - 2xx_1 + x_1^2 + y^2 - 2yy_1 + y_1^2 = x_2^2 - 2x_2x_1 + x_1^2 + y_2^2 - 2y_2y_1 + y_1^2,$$

$$x^2 + y^2 - 2x_1x - 2y_1y - x_2^2 - y_2^2 + 2x_2x_1 + 2y_2y_1 = 0.$$

Logo, S é uma equação da circunferência com $a = -2x_1$, $b = -2y_1$ e $c = -x_2^2 - y_2^2 + 2x_2x_1 + 2y_2y_1$

($\Leftarrow$) Agora, suponha que S tenha uma equação da forma $x^2+y^2+ax+by+c = 0$ com os coeficientes a, b, c constantes, sendo $\dfrac{a^2}{4} + \dfrac{b^2}{4} - c > 0$ e x, y incógnitas. Completando quadrados temos $(x+\dfrac{a}{2})^2+(y+\dfrac{b}{2})^2-\dfrac{a^2}{4}-\dfrac{b^2}{4}+c = 0$. Tomando $(x_1, y_1) = (\dfrac{-a}{2}; \dfrac{-b}{2})$ e $(x_2, y_2) = (\dfrac{-a}{2}+\sqrt{\dfrac{a^2}{4}+\dfrac{b^2}{4}-c}; \dfrac{-b}{2})$ vemos que $(x_1, y_1) \in S$ e que $(x+\dfrac{a}{2})^2+(y+\dfrac{b}{2})^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$. □

Definição 1.2. *Uma circunferência S em $\mathbb{R}^2$ é dita ser uma $F-circunferência$ se existem $(x_1, y_1) \neq (x_2, y_2) \in F^2$ tais que $(x_2, y_2) \in S$ e que*

$$(x - x_1)^2 + (y - y_1)^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2.$$

A importância dessas noções está no fato de que qualquer construção fundamental usando somente pontos do plano de um corpo F envolve construções de (ou porções de) uma $F - reta$ ou uma $F - circunferência$.

As duas primeiras construções fundamentais seguem da definição de $F-reta$, para quaisquer dois pontos dela.Para a terceira construção fundamental, a de um círculo com centro dado e raio igual ao comprimento do segmento que conecta dois pontos dados, suponha que o centro seja (x_1, y_1) e o raio seja dado pelo segmento conectando (a, b) e (c, d), onde todas as coordenadas estão em F. Está, o círculo definido por esses elementos no plano de F e é um $F-$*círculo*, pois seu centro está no plano de F e ele passa pelo ponto $(x_2, y_2) = (x_1 + (c - a), y_1 + (d - b))$.

Lema 1.5. *Um subconjunto S de $\mathbb{R}^2$ é uma $F - reta$ se, e somente se, S tem uma equação da forma $ax + by + c = 0$ com os coeficientes a, b e $c \in F$.*

Demonstração. ($\Rightarrow$) Seja $S \subset \mathbb{R}^2$ uma $F - reta$; por definição existem $(x_1, y_1) \neq (x_2, y_2) \in F^2$ tais que, $(x_1, y_1) \in S$ e $(x_2, y_2) \in S$. Por ser uma reta, temos que S é o conjunto solução de uma equação da forma $ax + by + c = 0$, com $a \neq 0$ ou $b \neq 0$.

Consideremos os casos para os possíveis a, b, c e para os possíveis (x_1, y_1) e (x_2, y_2).

Se $c = 0$, a equação é $ax + by = 0$. Caso $b = 0$ e $a \neq 0$, a equação é $ax = 0$ que (dividindo por a) é equivalente a $1x = 0$. Assim, basta tomar $a = 1$. Caso $a = 0$ e $b \neq 0$, é análogo. Portanto, nestes casos temos a, b e $c \in F$.

Se $c = 0, a \neq 0$ e $b \neq 0$ a equação $ax + by = 0$ é equivalente a

$$\frac{a}{b}x + 1y = 0.$$

Como (x_1, y_1) e $(x_2, y_2) \in S$ temos,

$$\frac{a}{b}x_1 + 1y_1 = 0 \text{ e } \frac{a}{b}x_2 + 1y_2 = 0.$$

Caso $x_1 = 0$ e $x_2 = 0$ teremos que $y_1 = y_2$, o que é impossível (pois, $(x_1, y_1) \neq (x_2, y_2)$ por hipótese).

Vejamos então o caso em que $x_1 \neq 0$ ou $x_2 \neq 0$. Suponha $x_1 \neq 0$. Da primeira equação temos,

$$\frac{a}{b} = \frac{-y_1}{x_1} \in F.$$

Assim, $\frac{-y_1}{x_1}x + 1y = 0$ é uma equação da reta com coeficientes em F.

Supondo agora $x_2 \neq 0$, de modo análogo conseguiremos uma equação com coeficientes em F.

Se $c \neq 0$, a equação $ax + by + c = 0$ é equivalente a

$$\frac{a}{c}x + \frac{b}{c}y + 1 = 0.$$

Como (x_1, y_1) e $(x_2, y_2) \in S$ temos,

$$\frac{a}{c}x_1 + \frac{b}{c}y_1 + 1 = 0 \; e \; \frac{a}{c}x_2 + \frac{b}{c}y_2 + 1 = 0.$$

A fim de facilitar a escrita consideremos $a' = \dfrac{a}{c}$ e $b' = \dfrac{b}{c}$. Então as equações acima ficam,

$$a'x_1 + b'y_1 + 1 = 0 \; e \; a'x_2 + b'y_2 + 1 = 0.$$

Caso $x_1 \neq 0$, isolando a' na primeira equação, temos

$$a' = \frac{-b'y_1 - 1}{x_1}.$$

Substituindo a' na segunda equação,

$$\begin{aligned} \frac{(-b'y_1 - 1)}{x_1}x_2 + b'y_2 + 1 &= 0, \\ \frac{-b'y_1x_2 - x_2 + b'y_2x_1 + x_1}{x_1} &= 0, \\ b'(y_2x_1 - y_1x_2) - x_2 + x_1 &= 0. \end{aligned}$$

Se $y_2x_1 - y_1x_2 \neq 0$, temos

$$b' = \frac{x_2 - x_1}{y_2x_1 - y_1x_2} \in F.$$

Substituindo b' em $a' = \frac{-b'y_1-1}{x_1}$ obtemos $a' = \frac{x_1-x_2}{y_2x_1-y_1x_2} \cdot \frac{y_1'-1}{x_1} \in F$. Assim,

$$\frac{x_1 - x_2}{y_2x_1 - y_1x_2} \cdot \frac{y_1' - 1}{x_1}x + \frac{x_2 - x_1}{y_2x_1 - y_1x_2}y + 1 = 0,$$

é uma equação da reta com coeficientes em F.

Caso $y_2x_1 - y_1x_2 = 0$, segue que $x_1 = x_2$ e portanto temos

$$a'x_1 + b'y_1 + 1 = 0 \; e \; a'x_1 + b'y_2 + 1 = 0.$$

Subtraindo uma equação da outra, obtemos

$$b'(y_1 - y_2) = 0.$$

Como $x_1 = x_2$, necessariamente $y_1 \neq y_2$. Logo $y_1 - y_2 \neq 0$ e $b' = 0$. Portanto, nesse caso temos

$$a' = \frac{-1}{x_1} \in F.$$

Assim,

$$\frac{-1}{x_1}x + 0y + 1 = 0$$

é uma equação da reta com coeficientes em F.

Se $y_1 \neq 0$ ou $x_2 \neq 0$ ou $y_2 \neq 0$, de modo análogo conseguiremos uma equação com coeficientes em F.

O caso em que $x_1 = 0$ e $x_2 = 0$ é impossível de ocorrer, pois

$$a'0 + b'0 + 1 = 0 \Rightarrow 1 = 0,$$

o que é um absurdo.

Já para o caso $x_1 = 0$ e $y_1 \neq 0$, temos

$$b'y_1 + 1 = 0 \; e \; a'x_2 + b'y_2 + 1 = 0.$$

Isolando b' na primeira equação temos $b' = \frac{-1}{y_1} \in F$. Substituindo na segunda obtemos,

$$a'x_2 + \frac{-1}{y_1} + 1 = 0 \Rightarrow a'x_2 = \frac{1}{y_1} - 1.$$

Se $x_2 = 0$, teríamos subtraindo as equações deste caso uma da outra que $b'(y_1 - y_2) = 0$, o que implica $b' = 0$ (pois, $y_1 - y_2 \neq 0$). Mas isso é impossível pois temos $b' = \frac{-1}{y_1}$ da primeira equação.

Logo $x_2 \neq 0$, e portanto $a' = \dfrac{\frac{1}{y_1} - 1}{x_2} \in F$. Assim,

$$\frac{\frac{1}{y_1} - 1}{x_2}x + \frac{-1}{y_1}y + 1 = 0,$$

é uma equação da reta com coeficientes em F.

Agora, caso $x_1 \neq 0$ e $y_1 = 0$, de modo análogo conseguiremos uma equação com coeficientes em F.

Portanto, em todos os casos conseguiremos uma equação da forma

$$ax + by + c = 0,$$

com coeficientes em F.

($\Leftarrow$) Seja $S \subset \mathbb{R}^2$ uma reta com equação $ax + by + c = 0$ com $a, b, c \in F$ e $a \neq 0$ ou $b \neq 0$. Suponha, sem perda de generalidade, que $a \neq 0$. Então considere os pontos $(-b - c/a, a)$, $(\frac{-b^2-c}{a}, b) \in F^2$; facilmente se nota que estes pontos pertencem a reta S o que conclui a demonstração. □

Lema 1.6. *Se um subconjunto S de $\mathbb{R}^2$ é uma $F-circunferência$, então S tem uma equação da forma $x^2+y^2+ax+by+c=0$ com os coeficientes a, b e $c \in F$.*

Demonstração. Seja $S \subset \mathbb{R}^2$ uma $F-circunferência$. Então existem $(x_1, y_1) \neq (x_2, y_2) \in F^2$ tais que $(x_2, y_2) \in S$ e que $(x-x_1)^2+(y-y_1)^2=(x_2-x_1)^2+(y_2-y_1)^2$. Temos,

$$x^2-2xx_1+x_1^2+y^2-2yy_1+y_1^2=x_2^2-2x_2x_1+x_1^2+y_2^2-2y_2y_1+y_1^2,$$

$$x^2+y^2-2x_1x-2y_1y-x_2^2-y_2^2+2x_2x_1+2y_2y_1=0.$$

Logo, S tem uma equação da forma esperada com $a=-2x_1$, $b=-2y_1$ e $c=-x_2^2-y_2^2+2x_2x_1+2y_2y_1 \in F$. □

Como o único caminho para construir um segmento é pela construção de seus pontos extremos, e como os únicos caminhos para construir um ponto são pela intersecção de duas retas; ou pela intersecção de uma reta e uma circunferência, ou pela intersecção de duas circunferências, é importante determinar a natureza dessas intersecções.

Lema 1.7. *O ponto de intersecção de duas $F-retas$ está em F^2. Os pontos de intersecções de uma $F-reta$ e uma $F-circunferência$, assim como os pontos de intersecções de duas $F-circunferências$, ou estão no plano de F ou no plano de alguma extensão quadrática de F.*

Demonstração. No caso da intersecção de duas $F-$ retas, ela é a solução simultânea de duas equações

$$a_1x+b_1y+c_1=0,$$

$$a_2x+b_2y+c_2=0,$$

em que os coeficientes estão, pelo Lema 1.5, todos em F. Como a solução simultânea das duas equações envolve operações racionais com seus coeficientes que estão em F, segue que as soluções x e y estão em F, o que significa que (x, y) está no plano de F.

No caso de uma $F-reta$ e uma $F-$circunferência, também é a solução simultânea de duas equações

$$\begin{aligned} a_1x+b_1y+c_1 &= 0, \\ x^2+y^2+a_2x+b_2y+c_2 &= 0, \end{aligned}$$

nos quais os coeficientes estão todos em F. Como a_1 e b_1 não podem ser ambos 0, digamos que $b_1 \neq 0$ e suponhamos (x, y) uma solução. Então, da primeira equação,

$$y=\frac{-c_1}{b_1}-\frac{a_1}{b_1}x.$$

Quando substituímos este y na segunda equação, vemos que x satisfaz uma equação quadrática com coeficientes em F. Portanto x é da forma $A \pm B\sqrt{k}$, com A, B e k em

F, sendo $k \geqslant 0$ (caso contrário, se $k < 0$, não haveria solução). Substituindo tal x na expressão para y também encontraremos uma expressão da forma $A' \pm B'\sqrt{k}$. Assim os pontos resultantes disto ou estão no plano de F, quando $\sqrt{k} \in F$, ou ambos estão no plano de $F(\sqrt{k})$, quando $\sqrt{k} \notin F$. (Quando $k = 0$, temos somente um ponto de intercessão e ele está no plano de F.)

No caso de duas $F-$ circunferências, suponha (x, y) uma solução de

$$x^2 + y^2 + a_1x + b_1y + c = 0 \text{ e } x^2 + y^2 + a_2x + b_2y + c = 0,$$

e subtraindo a primeira igualdade da segunda teremos que x e y satisfazem uma equação linear com coeficientes em F. Isto reduz a discussão à situação do caso anterior de reta e circunferência. □

Finalmente chegamos ao ponto em que é possível estabelecer e provar o resultado principal relativo a construtibilidade, e assim responder a pergunta feita na primeira parte desse capítulo.

Teorema 1.1. *As afirmações a seguir são equivalentes:*

(i) *O número a é construtível.*

(ii) *Existe uma sequência finita de corpos $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n$, com $a \in F_n$, tal que para cada j, $0 \leqslant j \leqslant n-1$, F_{j+1} é uma extensão quadrática de F_j.*

Demonstração. $(ii) \Rightarrow (i)$ É justamente o Lema 1.4.

$(i) \Rightarrow (ii)$ Se nos são dados os pontos $(0, 0)$ e $(1, 0)$ no plano cartesiano, por hipótese um segmento de comprimento $|a|$ pode ser construído. Podemos usar o ponto $(0, 0)$ e uma reta através de $(0, 0)$ e $(1, 0)$, para construir o ponto $(a, 0)$, o qual chamaremos de P. É suficiente mostrar que P está em F_n^2 para um corpo F_n do tipo descrito em (ii), isto é, um corpo cujos elementos podem ser obtidos de $\mathbb{Q}$ por uma sequência de extensões quadráticas.

A construção de P envolve um número finito de construções fundamentais, cada uma dos quais resulta em um número finito de novos pontos como intersecções de vários tipos. Listamos todas essas na ordem de construção, onde os pontos resultantes no mesmo passo podem ser listados em qualquer ordem. O ponto P está nesta lista, digamos na $M-$*ésima* posição. Omitindo a lista depois de P (que incluiria apenas pontos construídos no mesmo passo que P), temos: $P_1, P_2, \cdots, P_{M-1}, P_M$. O teorema estará provado quando estabelecermos a seguinte afirmação:

Existe um corpo F, obtido de $\mathbb{Q}$ por uma sequência de extensões quadráticas, tal que $P_1, P_2, \cdots, P_{M-1}, P_M$ estão todos F^2.

Como P_1 e P_2 devem ser os dois pontos indicados $(0, 0)$ e $(1, 0)$, os quais estão no plano de $\mathbb{Q}$, a afirmação está provada para $M = 1$ e $M = 2$.

Mostremos que é válido para qualquer M. Lembremos que a construção de P_M envolve apenas figuras construídas usando os pontos de P_1 até P_{M-1}, e pela hipótese

de indução, figuras no plano de algum corpo $\tilde{F}$ obtido de $\mathbb{Q}$ por uma sequência de extensões quadráticas.

Mas então, pelo Lema 1.7, ou P_M está no plano de $\tilde{F}$ ou no plano de $\tilde{F}(\sqrt{k})$, para algum $k \in \tilde{F}$ com $\sqrt{k} \notin \tilde{F}$. Em ambos os casos, tanto P_M quanto os outros $P_i's$ estão todos no plano de um corpo do tipo requerido. □

Vale observar que esse teorema estabelece uma equivalência entre duas propriedades, uma geométrica e uma algébrica. Através deste teorema, temos a reformulação dos problemas geométricos para problemas algébricos.

1.2 Duplicação do Cubo

Iniciaremos lembrando o problema clássico da "duplicação do cubo": **Dado um segmento de reta representando a aresta de um cubo, é possível construir outro segmento de reta representando a aresta de um cubo com o dobro do volume do primeiro?** Se tomarmos nossa unidade de comprimento para ser o comprimento do segmento dado, então o desejado segmento deverá ter comprimento $\sqrt[3]{2}$.

Então o problema é simplesmente verificar se $\sqrt[3]{2}$ é construtível ou não. Pelo Teorema 1.1, se $\sqrt[3]{2}$ fosse construtível, deveria existir uma sequência de extensões quadráticas de corpos associados a ele. Que isto é impossível, seguirá facilmente do lema a seguir.

Lema 1.8. *Seja $F(\sqrt{k})$ uma extensão quadrática de um corpo F. Se $\sqrt[3]{2}$ está em $F(\sqrt{k})$, então $\sqrt[3]{2}$ deve estar em F.*

Demonstração. Nos é dado que $\sqrt[3]{2}$ pode ser escrito da forma $a+b\sqrt{k}$, com $a, b, k \in F$, $\sqrt{k} \notin F$. Temos que mostrar que b dever ser 0. O cálculo

$$\begin{aligned} \sqrt[3]{2} &= (a + b\sqrt{k}) \\ 2 &= (a + b\sqrt{k})^3 \\ 2 &= a^3 + 3a^2b\sqrt{k} + 3ab^2k + b^3k\sqrt{k} \\ 2 &= [a^3 + 3ab^2k] + [3a^2b + b^3k]\sqrt{k} \end{aligned}$$

implica que $3a^2b + b^3k = 0$, pois caso contrário $\sqrt{k}$ teria que ser um elemento de F.

Mas, então,

$$(a - b\sqrt{k})^3 = [a^3 + 3ab^2k] - [3a^2b + b^3k]\sqrt{k} = 2$$

o que nos dá $a - b\sqrt{k}$ como raíz cúbica de 2.

Por outro lado, como a função $y = x^3$ é estritamente crescente, deve haver no máximo uma raíz cúbica para 2. Logo b deve ser 0 como queríamos. □

E agora segue o resultado principal:

Teorema 1.2. *É impossível "duplicar um cubo".*

Demonstração. Como observado na introdução dessa seção, duplicar o cubo é equivalente a construir $\sqrt[3]{2}$. Se $\sqrt[3]{2}$ fosse construtível, pelo Teorema 1.1 existiria um sequência de corpos $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n$, sendo que cada um é extensão quadrática do corpo anterior, de tal forma que $\sqrt[3]{2} \in F_n$. A aplicação repetida do Lema 1.8 implicaria em $\sqrt[3]{2} \in \mathbb{Q}$, mas é simples mostrar que $\sqrt[3]{2} \notin \mathbb{Q}$. □

A ideia básica desta seção será ligeiramente generalizada na próxima seção, na qual será fornecida uma solução para o problema da trissecção do ângulo.

1.3 Trissecção do Ângulo

Outro problema clássico levantado pelos gregos é se todo ângulo pode ser trissectado. A resposta é não como veremos em seguida.

Como o ângulo de 60° pode ser construído, se ele pudesse ser trissectado, então o ângulo de 20° poderia se construído. Mas então, como ilustrado na figura 1.5, o valor de $\cos 20°$ poderia ser construído. Será mostrado, porém, que o número $\cos 20°$ é raiz de uma equação cúbica a qual não tem raiz construtível.

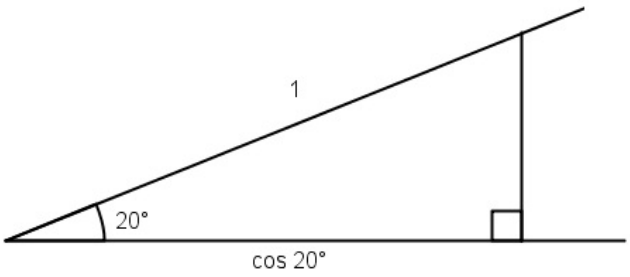

Figura 1.5: Um arco de 20°.

Das fórmulas elementares de trigonometria temos,

$$\begin{aligned}
\cos 3\theta &= \cos(2\theta + \theta) \\
&= \cos 2\theta \cos\theta - \operatorname{sen} 2\theta \operatorname{sen}\theta \\
&= (\cos^2\theta - \operatorname{sen}^2\theta)\cos\theta - (2\operatorname{sen}\theta\cos\theta)\operatorname{sen}\theta \\
&= \cos^3\theta - 3\operatorname{sen}^2\theta\cos\theta \\
&= \cos^3\theta - 3(1-\cos^2\theta)\cos\theta \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

Quando $\theta = 20°$, $\cos 3\theta = \dfrac{1}{2}$, então o número $\cos 20°$ deveria ser uma raiz da equação cúbica:

$$8u^3 - 6u - 1 = 0.$$

Fazendo nesta equação uma simples mudança de variável $x = 2u$ temos,

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

Se $\cos 20^\circ$ fosse construtível, então deveria ser possível construir uma raiz dessa equação. Como primeiro passo para a demonstração de que isto é impossível, faremos uma observação muito similar ao Lema 1.8.

Lema 1.9. *Seja $F(\sqrt{k})$ uma extensão quadrática de um corpo F. Se a equação $x^3 - 3x - 1 = 0$ tem uma raiz em $F(\sqrt{k})$, então ela tem uma raiz em F.*

Demonstração. Se a equação tem uma raiz em $F(\sqrt{k})$, podemos denota-la por $a + b\sqrt{k}$, em que a, b e k estão em F. Se $b = 0$, não temos nada a fazer, pois $a \in F$ e então a é a raiz desejada. Se $b \neq 0$, mostraremos que $-2a$ é uma raiz e que ela está em F.

Substituindo a raiz dada na equação temos,

$$\begin{aligned} (a + b\sqrt{k})^3 - 3(a + b\sqrt{k}) - 1 &= 0 \\ a^3 + 3a^2b\sqrt{k} + 3ab^2k + b^3k\sqrt{k} - 3a - 3b\sqrt{k} - 1 &= 0 \\ (a^3 + 3ab^2k - 3a - 1) + (3a^2b + b^3k - 3b)\sqrt{k} &= 0. \end{aligned}$$

Como $\sqrt{k} \notin F$ seque que $(3a^2b + b^3k - 3b) = 0$, pois caso contrário resolvendo a equação para $\sqrt{k}$ teremos $\sqrt{k} \in F$. Logo, $a^3 + 3ab^2k - 3a - 1 = 0$. Dividindo a primeira igualdade por b (o qual não é zero), temos

$$\begin{aligned} 3a^2 + b^2k - 3 &= 0 \\ a^3 + 3ab^2k - 3a - 1 &= 0. \end{aligned}$$

Isolando b^2k na primeira equação e substituindo o resultado na segunda temos

$$\begin{aligned} a^3 + 3a(3 - 3a^2) - 3a - 1 &= 0 \\ -8a^3 + 6a - 1 &= 0 \\ (-2a)^3 - 3(-2a) - 1 &= 0 \end{aligned}$$

da qual podemos ver que $-2a$, que está em F, é uma solução da equação original. □

Agora o resultado principal torna-se mais acessível.

Teorema 1.3. *Nem todo ângulo pode ser trisectado.*

Demonstração. Se fosse possível trissectar todo ângulo, deveria ser possível trissectar o ângulo de 60° que é construtível. Mas, como observado anteriormente, isso deve implicar a construtibilidade de $\cos 20^\circ$ e consequentemente a construtibilidade de uma raiz para a equação cúbica $x^3 - 3x - 1 = 0$. Pelo Teorema 1.1, tal raiz deve pertencer a um corpo F_n situado numa sequência $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n$ em que cada corpo é uma extensão quadrática do corpo anterior. Pela repetida aplicação do Lema

1.9 deve existir uma raiz *racional* para a equação $x^3 - 3x - 1 = 0$. Mostremos que isso é impossível.

Se um número racional M/N, na forma irredutível, fosse uma raiz da equação, teríamos

$$\frac{M^3}{N^3} - \frac{3M}{N} - 1 = 0$$

e, então,

$$M^3 - 3MN^2 - N^3 = 0.$$

Assim poderíamos reescrever

$$M^3 = N[3MN + N^2] \tag{1.1}$$

e

$$N^3 = M[M^2 - 3N^2]. \tag{1.2}$$

De (1.1) concluímos que se N tem um fator primo p, então p deve dividir M^3 e, portanto divide M. De (1.2) concluímos que se M tem um fator primo q, então q deve dividir N^3 e, portanto divide N. Como M e N foram supostos não terem um fator em comum, os únicos valores possíveis para M e N são ± 1, e então as únicas raízes racionais possíveis são ± 1. Contudo nenhuma dessas raízes satisfaz a equação. Logo, a equação não tem raiz racional. Com isso podemos concluir que é impossível trissectar todo ângulo. □

1.4 Quadratura do Círculo

O terceiro problema clássico de construção, que é a quadratura do círculo, apresenta uma dificuldade muito superior às apresentadas nos problemas anteriores. A questão é: **Dado um círculo, é possível construir um quadrado com a mesma área do círculo?** Se tomarmos como unidade de comprimento o raio de um círculo, sua área é π, então a construção de um quadrado de mesma área implica na construção de um segmento de comprimento $\sqrt{\pi}$ ao qual necessita da construtibilidade de π. Mostrando que π não é construtível, concluímos que é impossível quadrar o círculo. A prova que π não é construtível consiste de duas partes principais: primeira, todo número construtível é raiz de uma equação polinomial com coeficientes racionais; segunda, que π não pode ser uma raiz de equação polinomial com coeficientes racionais. Não incluiremos tal demonstração, mas o leitor interessado pode encontrá-la em todo detalhe na referência [1].

2 Polinômios: conceitos fundamentais

2.1 Aritmética dos Polinômios

Um polinômio p sobre um corpo F na indeterminada λ é uma soma formal

$$p(\lambda) := \sum_{i=0}^{\infty} a_i \lambda^i,$$

em que $a_i \in F$ para todo $i \in \mathbb{N}$ e existe n tal que $a_i = 0$ para todo $i > n$.

Se $a_i = 0$ para todo $i \geqslant 1$ dizemos que o polinômio é *constante*. Se além disso, $a_0 = 0$ dizemos que o polinômio é *nulo*, e reciprocamente.

Se $p(\lambda)$ é um polinômio tal que $a_i = 0,\ \forall i > n$, às vezes escreveremos

$$p(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n.$$

Reciprocamente se escrevemos $p(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$ fica entendido que $a_i = 0,\ \forall i > n$. Vale observar que nessa convenção não estamos supondo que n é o menor natural com a propriedade $a_i = 0,\ \forall i > n$.

Dado um polinômio $p(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$, se $a_k \neq 0$ para algum $0 \leqslant k \leqslant n$ e $a_i = 0$ para todo $i > k$, dizemos que k é o *grau do polinômio* $p(\lambda)$ e escrevemos $\deg(p(\lambda)) = k$. Destacamos que não está definido grau para o polinômio nulo.

Dado um corpo F, denotamos por $F[\lambda]$ o conjunto de todos os polinômios sobre um corpo F na indeterminada λ.

Definição 2.1. *Sejam $p(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$ e $q(\lambda) = b_0 + b_1\lambda + \cdots + b_m\lambda^m$ em $F[\lambda]$. Definimos*

$$p(\lambda) + q(\lambda) = c_0 + c_1\lambda + \cdots + c_i\lambda^i,$$

onde $c_i = (a_i + b_i)$ e

$$p(\lambda) \cdot q(\lambda) = d_0 + d_1\lambda + \cdots + d_k\lambda^k,$$

onde

$$d_j = \sum_{i=0}^{j} a_i b_{j-i},\ \ j = 0, 1, \ldots, k,$$

sendo $k = \deg(p(\lambda)) + \deg(q(\lambda))$.

A fim de facilitar a escrita no texto, denotaremos um polinômio $p(\lambda)$ simplesmente por p e deg $(p(\lambda))$ por deg (p).

É importante observar que $(F[\lambda],+,\cdot)$ é um domínio de integridade, em que o polinômio nulo é o elemento neutro de $F[\lambda]$ e o polinômio constante 1 é identificado como a unidade de $F[\lambda]$.

Em se tratando do conjunto $F[\lambda]$, observa-se nele várias propriedades muito similares às do conjunto $\mathbb{Z}$. Em $F[\lambda]$ nem todo elemento tem inverso multiplicativo. Similarmente à "divisão com resto" em $\mathbb{Z}$, temos o **algoritmo da divisão para polinômios**, explicitado no Teorema 2.1 que segue:

Teorema 2.1. *Sejam f e g polinômios em $F[\lambda]$, $g \neq 0$. Então existem únicos polinômios q e $r \in F[\lambda]$, tais que*

$$f = g \cdot q + r,$$

com r ou sendo identicamente nulo ou com grau menor que o de g (q é chamado quociente de f dividido pelo g, e r é chamado de resto da divisão).

Demonstração. (Existência) Escrevamos:

$$f(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n,$$
$$g(\lambda) = b_0 + b_1\lambda + \cdots + b_m\lambda^m,$$

com $m \geqslant 0$ e $b_m \neq 0$.

Mostremos tal resultado considerando os casos:

(i) Caso $f = 0$ (polinômio nulo), basta tomar $q = r = 0$;

(ii) Caso $f \neq 0$ e deg $(f) <$ deg (g). Basta tomar $q = 0$ e $r = f$, assim temos $f = 0 \cdot g + f$;

(iii) Caso $f \neq 0$ e deg $(f) \geqslant$ deg (g). Mostremos este caso por indução sobre o grau de f.

Para o primeiro passo no argumento da indução, se deg $(f) = 0$ teremos que deg $(g) = 0$ (pois, caso contrário, deg $(g) >$ deg (f), e portanto recairíamos no caso anterior). Assim, $f = a_0$ e $g = b_0$, com $a_0,\ b_0 \neq 0 \in F$. Como $a_0 = \dfrac{a_0}{b_0}b_0 + 0$, basta tomar $q = \dfrac{a_0}{b_0}$ e $r = 0$.

Suponhamos agora que deg $(f) = n > 0$ e que o teorema seja válido para todo polinômio de grau k, com $0 \leqslant k < n$. Consideremos o polinômio h definido por,

$$h = f - \frac{a_n}{b_m}\lambda^{n-m}g$$

e escrevamos

$$f = \frac{a_n}{b_m}\lambda^{n-m}g + h.$$

Se deg $(h) = 0$ ou deg $(h) < b_m\lambda^{n-m}$ e $r = h$.

Caso contrário, tem-se $0 <$ deg $(h) < b_m\lambda^{n-m}g$. Logo, pela hipótese de indução, existem polinômios q' e r' tais que

$$h = q'g + r', \text{ com } r' = 0 \text{ ou deg } (r') < \text{deg } (g).$$

Assim, temos

$$\begin{aligned} f - \frac{a_n}{b_m}\lambda^{n-m}g &= q'g + r', \\ f &= \frac{a_n}{b_m}\lambda^{n-m}g + q'g + r', \\ f &= (\frac{a_n}{b_m}\lambda^{n-m} + q')g + r', \end{aligned}$$

em que $r' = 0$ ou deg $(r') <$ deg (g).

Portanto, basta tomar $q = \frac{a_n}{b_m}\lambda^{n-m} + q'$ e $r = r'$. Isto prova a existência.

(Unicidade) Suponha que se tenha

$$f = q_1g + r_1 \text{ e } f = q_2g + r_2,$$

com

$$r_i = 0 \text{ ou deg } (r_i) < \text{deg } (g), \text{ para } i = 1, 2.$$

Subtraindo uma expressão para f da outra, obtemos

$$r_1 - r_2 = (q_2 - q_1)g.$$

Se $r_1 - r_2 \neq 0$, temos que $q_2 - q_1 \neq 0$ pois $g \neq 0$ e $F[\lambda]$ é um domínio de integridade. Assim, como

$$\text{deg } (r_1 - r_2) < \text{deg } (g) \text{ e deg } (r_1 - r_2) = \text{deg } ((q_1 - q_2)g) > \text{ deg } (g)$$

temos uma contradição.

Devemos então ter, necessariamente $r_1 - r_2 = 0$. Assim, $(q_2 - q_1)g = 0$ o que implica $q_2 - q_1 = 0$ e que garante a unicidade. □

Observamos que, no contexto do Teorema 2.1, se $\tilde{F} \subset F$ é um subcorpo contendo todos os coeficientes de f e g, então a demonstração acima implica que ambos q e r, na realidade, pertencem a $\tilde{F}[\lambda]$, um subanel de $F[\lambda]$.

Dizemos que um polinômio $g \neq 0$ *divide* um polinômio f, denotando por $g|f$, se o resto da divisão de f por g é o polinômio nulo.

Neste caso, dizemos que g é um *divisor* de f. A expressão f/g é usada para o quociente de f dividido por g. Se $f \neq 0$ e g é um divisor de f com deg $g <$ deg f, dizemos que g é um divisor próprio de f.

Observe que se deg $(f) = 0$, f não admite divisor próprio. Dizemos ainda que g é um *divisor não-trivial* se seu grau é maior que 0. Com estes conceitos de divisibilidade, podemos introduzir em $F[\lambda]$ o conceito análogo a números primos em $\mathbb{Z}$.

Definição 2.2. *Um polinômio não constante $f \in F[\lambda]$ é chamado irredutível em $F[\lambda]$ ou irredutível sobre F se ele não tem um divisor próprio não-trivial em $F[\lambda]$.*

Em outras palavras f é irredutível se não pode ser escrito como um produto de dois polinômios em $F[\lambda]$ de graus menores. Como exemplo, $\lambda^2 + 1$ é irredutível sobre $\mathbb{Q}$. Mas irredutibilidade depende do corpo em questão. O mesmo polinômio $\lambda^2 + 1$ é também irredutível sobre $\mathbb{R}$, mas sobre $\mathbb{C}$ é redutível, ou seja, $\lambda^2 + 1$ pode ser escrito pelo produto $(\lambda - i)(\lambda + i)$. De fato, sobre $\mathbb{C}$ todo polinômio é completamente redutível, isto é, pode ser escrito como um produto de fatores de grau um. Dado um polinômio sobre um corpo F, em geral, é bastante difícil determinar se ele é irredutível ou não. Para o corpo $\mathbb{Q}$, um critério útil será dado pelo Teorema 2.2. Felizmente, este é o caso que detém a maior importância para o que faremos. Para a demonstração deste Teorema, devemos fazer uso do **Lema de Gauss.**

Lema 2.1 (Gauss)**.** *Se um polinômio com coeficientes inteiros pode ser escrito como um produto de dois polinômios de graus menores com coeficientes racionais, então ele pode ser escrito como um produto de dois polinômios de graus menores com coeficientes inteiros.*

Demonstração. Suponha que $f = gh$, onde f tem coeficientes inteiros e g e h têm coeficientes racionais. (Aqui e em outros lugares, justaposição será entendido como significando multiplicação de polinômios). Sem perda de generalidade, podemos assumir que os coeficientes de f são relativamente primos (i.e., o maior divisor comum dele é 1). Escrevamos

$$g(\lambda) = \frac{a_n}{b_n}\lambda^n + \frac{a_{n-1}}{b_{n-1}}\lambda^{n-1} + \cdots + \frac{a_0}{b_0},$$

$$h(\lambda) = \frac{c_m}{d_m}\lambda^m + \frac{c_{m-1}}{d_{m-1}}\lambda^{m-1} + \cdots + \frac{c_0}{d_0},$$

onde os $a_i, b_i, c_j, d_j \in \mathbb{Z}$, $\forall i = 1, \ldots, n$ e $\forall j = 1, \ldots, m$.

Multiplicando o polinômio g pelo produto $B = b_n b_{n-1} \cdots b_0$ temos como resultado um polinômio com coeficientes inteiros. Agora, dividindo Bg por A, sendo A o maior divisor comum dos coeficientes inteiros de Bg, temos

$$(B/A)g(\lambda) = A_n\lambda^n + A_{n-1}\lambda^{n-1} + \cdots + A_0,$$

um polinômio com coeficientes relativamente primos.

Analogamente, obtemos

$$(D/C)h(\lambda) = C_m\lambda^m + C_{m-1}\lambda^{m-1} + \cdots + C_0,$$

que também é um polinômio com coeficientes relativamente primos.

De $f = gh$, obtemos $BDf = (AC)[(B/A)g] \cdot [(D/C)h]$. Como o produto BD é o maior divisor comum dos coeficientes do polinômio BDf (pois os coeficientes de f são relativamente primos) no lado esquerdo da igualdade e o produto AC é um divisor comum dos coeficientes do polinômio do lado direto, então $AC|BD$.

Definindo $E = BD/AC$, um inteiro, temos

$$Ef(\lambda) = [A_n\lambda^n + A_{n-1}\lambda^{n-1} + \cdots + A_0] \times [C_m\lambda^m + C_{m-1}\lambda^{m-1} + \cdots + C_0].$$

Mostrando que $E = \pm 1$, teremos escrito f na forma desejada. Suponha $E \neq \pm 1$. Logo, E tem um fator primo p. Como p não pode dividir todos os $A_i^{'s}$, pois eles são relativamente primos, então existe um menor inteiro $i \geqslant 0$ tal que p não divide A_i. Similarmente, existe um menor inteiro $j \geqslant 0$ tal que p não divide C_j. Comparando o coeficiente de λ^{i+j} em ambos os lados da igualdade, temos no lado esquerdo, que este coeficiente é divisível por E (pois é o maior divisor comum dos coeficientes desse lado). Logo, este coeficiente também é divisível por p. Do lado direito, o coeficiente de λ^{i+j} é,

$$\sum_{k=0}^{i-1} A_k C_{i+j-k} + A_i C_j + \sum_{k=i+1}^{i+j} A_k C_{i+j-k}.$$

Uma vez que cada A_k na primeira soma é divisível por p, segue que a soma também é. Como cada C_{i+j-k} na segunda soma é divisível por p, a soma também é. Mas por definição de i e j, os termos A_iC_j não são divisíveis por p. Assim, toda a soma não pode ser divisível por p, o que é uma contradição (pois se p divide E, então deveria dividir toda a soma também). Então, $E = \pm 1$. □

Agora podemos apresentar uma condição suficiente para irredutibilidade sobre $\mathbb{Q}$ dos polinômios com coeficientes inteiros. É o chamado **critério de irredutibilidade de Eisenstein**.

Teorema 2.2. *Seja $f(\lambda) = a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1} + a_n\lambda^n$, com coeficientes inteiros. Se existe um primo p tal que: (i) p divide $a_0, a_1, \cdots, a_{n-1}$; (ii) p não divide a_n; e (iii) p^2 não divide a_0; então f é irredutível sobre $\mathbb{Q}$.*

Demonstração. Se f fosse redutível, ele poderia ser escrito como um produto de polinômios gh sobre $\mathbb{Q}$ cada um com grau $\geqslant 1$. Pelo Lema 2.1, podemos assumir que g e h têm coeficientes inteiros. Se escrevermos

$$g(\lambda) = b_k\lambda^k + b_{k-1}\lambda^{k-1} + \cdots + b_0,$$

$$h(\lambda) = c_m\lambda^m + c_{m-1}\lambda^{m-1} + \cdots + c_0,$$

então $a_n = b_kc_m$, de modo que p não divida b_k nem c_m. Como p divide $a_0 = b_0c_0$, p divide b_0 ou c_0. Mas como p^2 não divide a_0, segue que p não divide b_0 e c_0. Suponha

que p divida b_0. Como p não divide b_k, deve existir um menor índice $j \geqslant 1$ tal que p não divide b_j. Na igualdade polinômial $f = gh$ compararemos os coeficientes de λ^j em ambos os lados. No lado esquerdo temos o coeficiente a_j, o qual é divisível por p uma vez que $j \leqslant k < n$. No lado direito, o respectivo coeficiente é a soma $b_0c_j + b_1c_{j-1} + \cdots + b_jc_0$, a qual não é divisível por p, pois na soma existe um termo que não é divisível por p, o último. Isto dá uma contradição. Analogamente, temos o mesmo resultado se supormos que p divida c_0. Portanto, f não pode ser redutível. □

É importante observar que o teorema acima dá uma condição apenas suficiente para irredutibilidade sobre $\mathbb{Q}$. Por exemplo, ele nos permite concluir que $\lambda^5 - 2$ e $3\lambda^5 + 7\lambda^4 - 14\lambda^2 + 7\lambda + 56$ são irredutíveis em $\mathbb{Q}$ (tomando $p = 2$ e 7 respectivamente), mas não podemos dar uma informação imediata sobre $\lambda^3 - 3\lambda - 1$ ou $\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1$, ambos os quais são irredutíveis sobre $\mathbb{Q}$. Para analisar situações como essas, algumas vezes uma simples mudança de variável pode ser encontrada para colocar um polinômio na forma ao qual o teorema é aplicável. Por exemplo, fazendo a mudança de variável $\lambda = u + 1$ em $\lambda^3 - 3\lambda - 1$, obtemos $u^3 + 3u^2 - 3$, o qual agora vemos ser irredutível ($p = 3$). Mais a frente mostraremos que para $f \in \mathbb{Q}[\lambda]$ e $a \in \mathbb{Q}$, $f(\lambda)$ é irredutível sobre $\mathbb{Q}$ se, e somente se, $f(\lambda + a)$ também o é (Proposição 3.3).

Até agora, o único resultado que temos sobre irredutibilidade de polinômios é para o caso especial de polinômios em $\mathbb{Q}[\lambda]$. Notando que a definição de irredutibilidade de um polinômio é bastante similar à aquela de um número primo, vamos agora prosseguir para ver que essa analogia se estende muito mais. Um fato sobre números primos que temos usado é que se, um primo divide um produto, ele deve dividir um dos fatores. Uma afirmação semelhante aparecerá para polinômios irredutíveis (Teorema 2.4). Outro fato útil sobre primos é que, todo inteiro pode se escrito unicamente como um produto de primos. Uma afirmação análoga será vista para a fatoração de um polinômio em fatores irredutíveis (Teorema 2.5). De modo a desenvolver estes resultados introduziremos mais alguns conceitos.

Definição 2.3. *Dados dois polinômios f e g em $F[\lambda]$, um maior divisor comum de f e g, denotado por (f, g), é qualquer polinômio em $F[\lambda]$ de grau maximal dentre os que dividem f e g.*

Isto é, podem existir muitos polinômios (incluindo todos os polinômios constantes, exceto o nulo) que dividem ambos f e g, qualquer um de grau máximo é um maior divisor comum (m.d.c.) de f e g.

Na realidade, será visto que todos os m.d.c.'s são múltiplos constantes uns dos outros (Ver Corolário 2.1). Quando escrevermos (f, g), estaremos nos referindo a algum m.d.c., particular ou não cujo contexto deixará claro.

O Teorema a seguir, garante uma maneira de se obter um m.d.c. de quaisquer dois polinômios em $F[\lambda]$. É o chamado **Algoritmo Euclidiano para polinômios**.

Teorema 2.3. *Sejam f e $g \in F[\lambda]$. Existe (f, g) e existem s e $t \in F[\lambda]$ tais que*

$$(f, g) = sf + tg.$$

Demonstração. Começando pela divisão de f por g, temos

$$f = gq_1 + r_1, \text{ com } r_1 = 0 \text{ ou } \deg(r_1) < \deg(g).$$

Se $r_1 = 0$, então $g|f$. Logo, g é um máximo divisor comum de f e g (pois g é um polinômio de grau maximal que divide ele próprio e f). Como g pode ser escrito da forma,

$$g = 0f + 1g,$$

basta tomar $s = 0$ (polinômio nulo) e $t = 1$ (polinômio constante).

Caso $r_1 \neq 0$, dividamos o divisor g pelo resto r_1. Assim,

$$g = r_1q_2 + r_2, \text{ com } r_2 = 0 \text{ ou } \deg(r_2) < \deg(r_1).$$

Se $r_2 = 0$, então $r_1|g$. Logo, r_1 é um máximo divisor de g e r_1 (pois r_1 é um polinômio de grau maximal que divide ele próprio e g). Do passo anterior, temos que $r_1|(gq_1 + r_1) = f$, ou seja, r_1 é um polinômio de grau maximal que divide f. Logo, r_1 é um máximo divisor de f e g também. Assim, r_1 pode ser escrito da forma

$$r_1 = 1f - q_1g$$

e portanto, basta tomar $s = 1$ e $t = -q_1$.

Caso $r_2 \neq 0$, dividimos o divisor r_1 pelo resto r_2. Assim,

$$r_1 = r_2q_3 + r_3, \text{ com } r_3 = 0 \text{ ou } \deg(r_3) < \deg(r_2).$$

Repetindo o processo, necessariamente existirá um $n \in \mathbb{N}$ tal que $\deg(r_n) = 0$, pois o conjunto formado pelos graus dos restos é um conjunto limitado inferiormente, ou seja,

$$\deg(g) > \deg(r_1) > \deg(r_2) > \cdots \geqslant 0.$$

Assim, a divisão do polinômio r_{n-1} por r_n terá resto $r_{n+1} = 0$ (polinômio nulo, pois r_n é um polinômio constante).

Assim, teremos:

$$r_1 = r_2q_3 + r_3,$$

$$r_2 = r_3q_4 + r_4,$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n,$$

$$r_{n-1} = r_nq_{n+1} + 0.$$

Mostremos por indução sobre n que r_n pode ser escrito na forma desejada do teorema. Para $n = 1$, temos $r_1 = 1f + (-q_1)g$. Para $n = 2$, temos $r_2 = g - r_1q_2 = g - fq_2 + q_1q_2g = (-q_2)f + (1 + q_1q_2)g$. Observe que para $n = 3$, temos

$$\begin{aligned} r_3 &= r_1 + (-q_3)r_2 \\ &= [1f + (-q_1)g] + (-q_3)[(-q_2)f + (1 + q_1q_2)g \\ &= (1 + q_3q_2)f + (-q_1 - q_3 - q_3q_1q_2)g \end{aligned}$$

Assumindo ser verdade o passo acima para $n = i-1$, mostremos para $n = i$. Temos,

$$r_i = r_{i-2} - r_{i-1}q_i.$$

Como r_{i-1} e r_{i-2} podem ser escrito da forma desejada pelo teorema, segue que realizando manipulações algébricas convenientes conseguiremos escrever $r_i = sf + tg$, onde $s, t \in F[\lambda]$. Logo, r_n admite a forma desejada do teorema.

Agora, resta mostrar que r_n é verdadeiramente um m.d.c. Da representação $r_n = sf + tg$, vemos que qualquer maior divisor comum de f e g, digamos (f, g), divide r_n e portanto $\deg(f, g) \leqslant \deg(r_n)$. Pelo sucessivo algoritmo da divisão iniciando de f por g até r_n, observamos que r_n divide sucessivamente $r_{n-1}, r_{n-2}, \ldots, r_1, g$ e f. Assim, r_n é um divisor comum de f e g, de modo que $\deg(r_n) \leqslant \deg(f, g)$. Combinando isto com o resultado anterior, temos que $\deg(r_n) = \deg(f, g)$, e assim r_n é um *m.d.c.* de f e g. □

Corolário 2.1. *Se d_1 e d_2 são máximos divisores de f e g, então d_1 e d_2 são múltiplos constantes um do outro.*

Demonstração. Sendo d_1 um máximo divisor de f e g, segue do Teorema 2.3 que existem $s, t \in F[\lambda]$ tais que $d_1 = sf + tg$. Pelo fato de d_2 dividir f e g, d_2 divide d_1 (e analogamente d_1 divide d_2). Como $d_1 = cd_2$, para algum polinômio c, temos que $\deg(d_1) = \deg(c) + \deg(d_2)$. Sendo d_1 e d_2 de grau maximal dentre os divisores de f e g (por hipótese), concluímos que o grau de c é 0. Portanto é um polinômio constante. □

Seguindo a terminologia de $\mathbb{Z}$, dizemos que dois polinômios f e g são *relativamente primos* se eles não têm fatores não-constantes em comum. Nesse caso, escrevemos $(f, g) = 1$, em que o lado direito naturalmente se refere ao polinômio constante 1. Agora, finalmente, podemos mostrar os dois resultados básicos mencionados anteriormente.

Teorema 2.4. *Sejam f, g e $h \in F[\lambda]$ e seja f irredutível. Se $f|gh$, então $f|g$ ou $f|h$.*

Demonstração. Suponha que f não divide g. Como f é irredutível, temos que $(f, g) = 1$. Pelo Teorema 2.3, existem polinômios s e $t \in F[\lambda]$ tais que

$$1 = sf + tg,$$

de modo que,

$$h = sfh + tgh,$$

da qual, como $f|gh$, concluímos que $f|h$. □

Teorema 2.5. *Seja $f \in F[\lambda] - \{0\}$. Então f pode ser escrito como um produto de polinômios irredutíveis em $F[\lambda]$, e esta decomposição é única a menos de múltiplos constantes de cada fator não constante.*

Demonstração. Mostremos por indução sobre o grau de f. Quando deg $(f) = 1$, não há nada a fazer pois f é irredutível (ou seja, f não admite divisor próprio não-trivial). Suponha que deg $(f) = n > 1$ e que o teorema seja válido para polinômios de graus menores que n. Se f é irredutível, não há nada a fazer. Se f é redutível, então existem polinômios $g, h \in F[\lambda]$ tais que

$$f = gh,$$

com deg $(g) > 0$ e deg $(h) > 0$. Como deg $(f) =$ deg $(g) +$ deg (h) e deg $(f) = n$ temos que deg $(g) < n$ e deg $(h) < n$. Assim, pela hipótese de indução, g e h se escrevem como produto de polinômios irredutíveis. Logo, f pode ser escrito como produto de polinômios irredutíveis.

Para mostrar a unicidade, suponha que escrevemos simultaneamente $f = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, em que os $p's$ e $q's$ são polinômios não constantes irredutíveis em $F[\lambda]$. Suponha que $m > n$. Pelo Teorema 2.4, p_1 deve dividir algum q_i, digamos q_1. Pela irredutibilidade de q_1 segue que ele é um múltiplo constante de p_1, ou seja, $q_1 = k_1 p_1$, $k_1 \in F[\lambda]$. Quando ambos os lados da equação são divididos por p_1, temos

$$p_2 \cdots p_n = k_1 q_2 \cdots q_m,$$

Agora repetindo o processo para p_2, $p_3, \ldots, p_n$ teremos,

$$1 = k_1 k_2 \cdots k_n q_{n+1} \cdots q_m,$$

o que é um absurdo pois temos de um lado um polinômio de grau 0 e do outro um polinômio de grau maior que 0. O raciocínio é análogo para $n > m$. Portanto, segue que $n = m$. □

2.2 Raízes de Polinômios

Dizemos que uma função $f : F \to F$ é polinomial sobre F se existem $a_0, a_1, \cdots, a_n \in F$ tais que,

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \forall x \in F,$$

em que nesta expressão para $f(x)$ a notação é a usual para somas e produtos de elementos de um corpo F.

É simples verificar que a soma e o produto de funções polinomiais resultam em funções polinomiais. Na verdade, a aplicação

$$p(\lambda) = a_0 + a_1\lambda^1 + \cdots + a_n\lambda^n \mapsto \tilde{p}(x) = a_0 + a_1 x + \cdots + a_n x^n, \forall x \in F,$$

é um homomorfismo de anéis.

Uma raiz de um polinômio p é um valor da variável x para o qual a função polinomial $\tilde{p}$ anula-se.

Proposição 2.1. *Seja $p \in F[\lambda]$. Um número r é uma raiz de p se, e somente se, $(\lambda - r)$ divide p.*

Demonstração. ($\Rightarrow$) Seja p um polinômio tal que r é raiz de p. Mostremos que $(\lambda - r)$ divide p. Pelo algoritmo da divisão para polinômios existem $q, s \in F[\lambda]$ tais que,

$$p(\lambda) = (\lambda - r)q(\lambda) + s(\lambda), \text{ com } s(\lambda) = 0 \text{ ou } \deg\ s(\lambda) < \deg\ (\lambda - r).$$

Suponha que $s(\lambda)$ não seja o polinômio nulo. Como $\deg\ s(\lambda) < \deg\ (\lambda - r) = 1$, segue que $\deg\ s(\lambda) = 0$, ou seja, $s(\lambda)$ é um polinômio constante não nulo. Agora, como r é raiz de p

$$\begin{aligned} \tilde{p}(r) &= \widetilde{(r - r)}\tilde{q}(r) + \tilde{s}(r), \\ 0 &= 0\tilde{q}(r) + \tilde{s}(r), \end{aligned}$$

ou seja,

$$\tilde{s}(r) = 0.$$

Logo, r é raiz de $s(\lambda)$, o que contraria a hipótese de $s(\lambda)$ ser um polinômio constante não nulo.

Assim, $s(\lambda)$ é o polinômio nulo e portanto, $(\lambda - r)$ divide p.

($\Leftarrow$) Se $(\lambda - r)$ divide p temos,

$$p(\lambda) = (\lambda - r)g(\lambda).$$

Calculando $\tilde{p}(r)$, temos

$$\begin{aligned} \tilde{p}(r) &= \widetilde{(r - r)}\tilde{g}(r), \\ \tilde{p}(r) &= 0\tilde{g}(r), \\ \tilde{p}(r) &= 0, \end{aligned}$$

ou seja, r é raiz de $p \in F[\lambda]$ como queríamos. □

O teorema a seguir, que não será demonstrado, é chamado de **Teorema Fundamental da Álgebra**:

Teorema 2.6. *Todo polinômio sobre $\mathbb{C}$ de grau $\geqslant 1$ tem pelo menos uma raiz (em $\mathbb{C}$).*

A demonstração envolve técnicas que fogem um tanto do espírito deste trabalho e preferimos não incluí-las. Ver referência [2].

Se r é raiz de f, definimos a multiplicidade de r como o maior inteiro m tal que $(\lambda - r)^m$ divida f.

Teorema 2.7. *Todo polinômio sobre $\mathbb{C}$ de grau n tem exatamente n raízes, contadas suas multiplicidades.*

Demonstração. Por indução sobre n, temos que para $n = 0$ (grau zero), o polinômio é não nulo constante e portanto não tem raiz. Supondo verdade que todo polinômio de grau $n-1$ tem $n-1$ raízes, mostremos para polinômio de grau n.

Sendo f um polinômio de grau $n \geqslant 1$, então pelo Teorema 2.6 ele tem pelo menos uma raiz r. Assim, $(\lambda - r)$ divide f e podemos fatorar f da seguinte forma,

$$f(\lambda) = (\lambda - r)g(\lambda),$$

onde $g(\lambda)$ é um polinômio de grau $n-1$.

Por hipótese de indução, g tem $n-1$ raízes, o que implica que f têm n raízes, como queríamos. □

Uma consequência imediata do Teorema 2.7 e o seguinte corolário:

Corolário 2.2. *Se F é um subcorpo de $\mathbb{C}$, a correspondência*

$$p(\lambda) = a_0 + a_1\lambda^1 + \cdots + a_n\lambda^n \mapsto \tilde{p}(x) = a_0 + a_1x + \cdots + a_nx^n, \forall x \in F,$$

é uma bijeção entre $F[\lambda]$ e o conjunto das funções polinomiais.

Demonstração. A correspondência é sobrejetora pela definição de função polinomial. Agora, se correspondência não fosse injetiva, para alguma função polinomial existiriam dois polinômios de grau finitos dão origem a mesma função polinomial. Digamos, $g(\lambda) = \tilde{p}(x), \forall x \in F$ e $f(\lambda) = \tilde{p}(x), \forall x \in F$. Subtraindo uma expressão da outra obtemos $g(\lambda) - f(\lambda) = 0, \forall x \in F$. Isto implica que $g(\lambda) - f(\lambda)$ tem infinitas raízes, que é uma contradição pois tal polinômio deveria ter grau finito e pelo Teorema 2.7 teria um número finito de raízes. □

A partir de agora, neste trabalho o termo corpo estará se referindo a um subcorpo de $\mathbb{C}$.

Dizemos que um número r é *algébrico* sobre F se existe um polinômio (não nulo) sobre F, do qual r é uma raiz. Caso contrário, dizemos que r é *transcendente*.

Nos casos em que F não estiver identificado, entenderemos F como sendo $\mathbb{Q}$. Assim devemos dizer que 3, i e $\sqrt[3]{7}$ são algébricos, pois eles são raízes dos polinômios sobre $\mathbb{Q}$ $x - 3$, $x^2 + 1$ e $x^3 - 7$, respectivamente.

Teorema 2.8. *Se F é um corpo, então o conjunto de todos números algébricos sobre F também é um corpo.*

Demonstração. Suponha que os números r e s são algébricos sobre F e que satisfazem,

$$a_n r^n + a_{n-1} r^{n-1} + \cdots + a_0 = 0,$$

$$b_m s^m + b_{m-1} s^{m-1} + \cdots + b_0 = 0,$$

em que todos os coeficientes estão em F e a_n, $b_m \neq 0$.

Vemos que $-s$ é algébrico sobre F, pois ele satisfaz,

$$(-1)^m b_m (-s)^m + (-1)^{m-1} b_{m-1} (-s)^{m-1} + \cdots + b_0 = 0.$$

Se $s \neq 0$, $\dfrac{1}{s}$ é algébrico sobre F, pois é raiz da equação

$$b_m + b_{m-1} s + \cdots + b_0 s^m = 0.$$

Assim, é suficiente mostrar que $r + s$ e rs são algébricos sobre F.

Uma observação a mais: usando as equações originais, r^n e s^m podem ser expressos em potências menores de r e s, respectivamente. Por exemplo:

$$r^n = -(a_{n-1} r^{n-1} + \cdots + a_0)/a_n.$$

Considere a tabela com mn números:

$$\begin{array}{ccccc} 1 & r & r^2 & \cdots & r^{n-1} \\ s & sr & sr^2 & \cdots & sr^{n-1} \\ s^2 & s^2 r & s^2 r^2 & \cdots & s^2 r^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s^{m-1} & s^{m-1} r & s^{m-1} r^2 & \cdots & s^{m-1} r^{n-1} \end{array}$$

Listando eles em qualquer ordem, e chamando-os de $c_1,\ c_2, \cdots,\ c_R$, em que $R = mn$, notemos que para todo i, rc_i pode ser escrito com uma combinação linear de todos os c_i's:

$$rc_i = d_{i1} c_1 + d_{i2} c_2 + \cdots + d_{iR} c_R,$$

em que os coeficientes $d_{ij} \in F$. Na realidade, a maioria dos d_{ij}'s são 0. Por exemplo, se c_i não é uma entrada da última coluna da tabela, rc_i é apenas alguma entrada a sua direta. Agora, se c_i é uma entrada da última coluna, então rc_i tem a forma $r^n s^k$, na qual r^n é substituído pelo seu equivalente em termos de potências menores de r (ao qual todos os coeficientes estão em F). Em qualquer caso acima a representação é possível.

Denotando por C vetor coluna cuja as R entradas são os c_i's e por D a matriz $R \times R$ dos d_{ij}'s, podemos escrever a equação acima em forma de matriz,

$$rC = DC.$$

Analogamente, existe uma matriz E tal que

$$sC = EC.$$

Assim temos,

$$(r+s)C = (D+E)C,$$

pois vale a distributiva para matrizes.

Como $C \neq 0$ (matriz nula), isto implica que $r+s$ é um autovalor da matriz $D+E$. Mas então $r+s$ é raiz do polinômio característico, $\det(D+E-\lambda I)$, onde I é a matriz identidade. Como esse é um polinômio sobre o corpo F, concluímos que $r+s$ é algébrico sobre F.

Para o produto observe que,

$$(rs)C = r(sC) = r(EC) = E(rC) = E(DC) = (ED)C.$$

Assim, rs é um autovalor para ED. E pela mesma razão acima rs é algébrico. □

3 Extensão de Corpos

3.1 Extensões Simples, Múltiplas e Finitas

O conceito de extensões de corpos surgiu logo na Seção 1.1 deste trabalho, em que vimos como extensões quadráticas são fundamentais para teoria de construtibilidade. Nesta seção será generalizada a noção de extensões de corpos e apresentada uma teoria segundo a qual poderemos lançar novo olhar sobre alguns resultados anteriores.

Se F é um corpo e $a_1, a_2, \cdots, a_m$ são m números complexos, definimos a *extensão de F por $a_1, a_2, \cdots, a_m$*, denotando por $F(a_1, a_2, \cdots, a_m)$, como sendo o menor corpo contendo $a_1, a_2, \cdots, a_m$, como também todos os elementos de F. (Por "menor", queremos dizer ser o corpo que é a intersecção de todos os corpos contendo todos estes elementos). Em geral, ela é chamada de *extensão múltipla de F*. No caso de $m = 1$, é chamada de *extensão simples*. Além disso, se cada um dos a_i's é algébrico sobre F, ela é chamada de *extensão algébrica*; caso contrário, ela é chamada de *extensão transcendente*.

É natural perguntar "Como é $F(a)$?" Isto é, quando F é estendido por a, que outros elementos também são incluídos? Nas seções anteriores encontramos $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ que é um corpo. Neste caso, e entre outros, fomos capazes de expressar cada elemento da extensão como uma combinação linear de alguma coleção finita de elementos da extensão, onde os coeficientes na combinação linear pertencem ao corpo original. Isto é uma forte indicação de alguma estrutura de espaço vetorial, que é exatamente a chave para o estudo destas extensões.

Primeiro, para generalizar ainda mais o conceito de extensão de corpos, se E e F são corpos tais que $E \supset F$, então E é chamado *extensão* de F. Neste caso, E pode ser considerado como um espaço vetorial sobre F, onde a adição vetorial é simplesmente a adição usual do corpo e multiplicação por escalar é a multiplicação usual do corpo. A dimensão do espaço vetorial E sobre F é chamada de *grau* da extensão e é denotada por $[E : F]$. Se E é uma extensão de F e $[E : F]$ é finita, denominamos E como uma *extensão finita* de F.

Por exemplo, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, pois uma base para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ é dada pelo conjunto $\{1, \sqrt{2}\}$. Uma questão natural de se pensar é, **existe algum modo alternativo para determinar o grau de uma extensão?** A resposta é afirmativa a questão, em

certos casos importantes, dos quais faremos uso frequentemente. Ela será desenvolvida nos próximos parágrafos.

Vamos iniciar com o caso de uma *extensão algébrica simples* $F(a)$ de F. Como a é algébrico sobre F, existe um polinômio sobre F tendo a como uma raiz e, além disso, existe tal polinômio sendo de menor grau. Todo polinômio desta forma é chamado de *polinômio minimal* de a sobre F, e seu grau é chamado de *grau de a sobre F*, denotado por $\deg_F\ a$. Por exemplo, $\deg_{\mathbb{R}}\ i = 2$, pois $\lambda^2 + 1$ é um polinômio minimal de i sobre $\mathbb{R}$. Dado um número a, em geral é bastante difícil encontrar diretamente (ou mostrar que você encontrou) um polinômio minimal para a. A chave para esta questão está na equivalência entre o conceito de "polinômio minimal" e o conceito de "polinômio irredutível".

Teorema 3.1. *Seja $f \in F[\lambda]$ com $\tilde{f}(a) = 0$. Então, f é um polinômio minimal para a sobre F se, e somente se, f é irredutível sobre F.*

Demonstração. ($\Rightarrow$) Seja f um polinômio minimal de a sobre F. Suponha f não ser irredutível sobre F. Logo, f pode ser escrito como um produto gh, com $g, h \in F[\lambda]$, de graus menores. Como a é raiz de f, um desses polinômios dever ter a como uma raiz, o que contraria a hipótese de f ser minimal (pois g e h são de graus menores que o de f sobre F). Portanto, f tem que ser irredutível.

($\Leftarrow$) Seja f irredutível sobre F. Podemos aplicar o algoritmo da divisão para dividi-lo por um polinômio minimal de a sobre F, digamos g. Logo, existem $q, r \in F[\lambda]$ tais que $f = gq + r$, com $r = 0$ ou $\deg\,(r) < \deg\,(g)$ e não nulos. Pela minimalidade de g, a é raiz de g, e portanto $\tilde{f}(a) = \tilde{g}(a) = 0$. Isto implica, $\tilde{r}(a) = 0$. Como $\deg\,(r) < \deg\,(g)$ e g é um polinômio de grau mínimo, segue que r tem que ser o polinômio nulo. Agora, por f ser irredutível e $\deg\,(g) \geqslant 1$, devemos ter que $\deg\,(g) = \deg\,(f)$ e portanto podemos concluir que q é um polinômio constante. Assim, como f tem o mesmo grau de g, ele também é minimal. □

Visto que temos um critério de irredutibilidade para polinômios em $\mathbb{Q}[\lambda]$ com coeficientes inteiros (Teorema 2.2), algumas vezes seremos capazes de usar este teorema para encontrar o grau de algum número algébrico sobre $\mathbb{Q}$. Por exemplo, $\deg_{\mathbb{Q}}\ \sqrt[5]{2} = 5$, pois $\sqrt[5]{2}$ é uma raiz do polinômio irredutível $\lambda^5 - 2$. Já $\deg_{\mathbb{Q}}\ \cos 20^\circ = 3$, pois $\cos 20^\circ$ é uma raiz do polinômio irredutível $8\lambda^3 - 6\lambda - 1$ (Ver Seção 1.3).

Com essas idéias em mente, retornaremos ao problema de encontrar o grau de uma extensão algébrica simples.

Teorema 3.2. *Se a é algébrico sobre F, $[F(a) : F] = \deg_F\ a$.*

Demonstração. Para qualquer a, observemos que

$$F(a) = \{\tilde{g}(a)/\tilde{h}(a) | g, h \in F[\lambda], \tilde{h}(a) \neq 0\}.$$

Observamos que quando a é algébrico sobre F somos capazes de simplificar a representação dos elementos desse conjunto. Supondo $\deg_F\ a = n$, mostremos primeiro que os elementos $1, a, a^2, \cdots, a^{n-1}$ são um conjunto gerador para $F(a)$ sobre F; ou o que é equivalente, todo elemento $\tilde{g}(a)/\tilde{h}(a)$ é igual a algum $\tilde{r}(a)$, onde $r \in F[\lambda]$ de deg $(r) \leqslant n-1$ ou $r = 0$.

Seja f um polinômio minimal de a sobre F. Se deg $(h) \geqslant 1$, então $(f, h) = 1$, pois f é irredutível (pelo Teorema 3.1) e não pode dividir h (senão, existiria um $k \in F[\lambda]$ tal que $h = fq$ e como f é minimal $\tilde{h}(a) = \tilde{f}(a)\tilde{k}(a) = 0$). Pelo algoritmo Euclidiano, existem $s, t \in F[\lambda]$ tais que $1 = sf + th$. Como $\tilde{f}(a) = 0$, obtemos $\tilde{t}(a) = 1/\tilde{h}(a)$. Logo, $\tilde{g}(a)/\tilde{h}(a) = \tilde{g}(a)\tilde{t}(a)$. Aplicando o algoritmo da divisão para dividir o polinômio gt por f temos $gt = fq + r$, em que $r = 0$ ou deg $(r) \leqslant n-1$. Observando novamente que a é algébrico sobre F temos que $\tilde{g}(a)\tilde{t}(a) = \tilde{r}(a)$, como queríamos.

Resta garantir que os elementos $1, a, a^2, \cdots, a^{n-1}$ são linearmente independentes sobre F. Se não fossem, a deveria satisfazer um polinômio sobre F de grau $\leqslant n-1$, contrariando a minimalidade de n. Portanto, estes elementos formam uma base para a extensão, completando assim a demonstração de que quando a é algébrico,

$$[F(a) : F] = deg_F\ a.$$

□

Veremos que o caso de encontrar o grau de uma extensão finita ou algébrica múltipla de F é coberto pelo teorema anterior, pois mostraremos que estes casos de extensões são eles próprios extensões simples. Esse resultado é interessante em si próprio e importante para o trabalho mais a frente, mas não nos fornece uma maneira muito útil de investigar sobre o grau destas extensões. Em geral, isto é feito via Teorema 3.4.

Vejamos uma proposição que será utilizada na demonstração do resultado comentado anteriormente.

Proposição 3.1. *Se f é um polinômio irredutível sobre F, então f não tem raízes múltiplas.*

Demonstração. Suponha que α é uma raíz múltipla de $f \in F[\lambda]$ tal que $\alpha \in E$, onde E é um extensão de F. Pela irredutibilidade de f sobre F, segue que f é o polinômio minimal para α sobre F. Como α é raiz múltipla, podemos escrever em $E[\lambda]$

$$f(\lambda) = (\lambda - \alpha)^2 g(\lambda)$$

$$f'(\lambda) = 2(\lambda - \alpha)g(\lambda) + (\lambda - \alpha)^2 g'(\lambda),$$

ou seja, $f'(\alpha) = 0$. Isso contraria a minimalidade de f pois deg $(f') <$ deg (f) e $f' \in F[\lambda]$. Portanto, f não pode ter raízes múltiplas. □

Teorema 3.3. *As seguintes afirmações são equivalentes:*

(*i*) *E é extensão finita de F.*

(*ii*) *E é uma extensão algébrica múltipla de F.*

(*iii*) *E é uma extensão algébrica simples de F.*

Demonstração. ($i \Rightarrow ii$) Observemos primeiro que todo elemento de E é algébrico sobre F. Seja $a \in E$ e $n = [E : F]$. Assim, como os $n+1$ vetores $1, a, a^2, \ldots, a^n$ devem ser linearmente dependentes, existe uma combinação linear não-trivial deles igual a 0, com coeficientes em F, ou seja, a é uma raiz de algum polinômio sobre F. Como a é qualquer, concluímos que todo elemento de E é algébrico sobre F, ou seja, E é uma extensão algébrica de F.

Mostremos que E é uma extensão múltipla. Seja $\{a_1, a_2, \ldots, a_n\}$ uma base para E sobre F. Por um lado, como E é uma extensão finita de F, ele contém todos os elementos de F, bem como $a_1, a_2, \ldots, a_n$. Logo, E deve conter o menor corpo contendo esses elementos, o qual por definição é $F(a_1, a_2, \ldots, a_n)$. Portanto, $F(a_1, a_2, \ldots, a_n) \subset E$. Por outro lado, $F(a_1, a_2, \ldots, a_n)$ deve conter o conjunto de todas as combinações lineares dos a_i's, com coeficientes em F, a qual tal conjunto é precisamente E, ou seja, $E \subset F(a_1, a_2, \ldots, a_n)$. Por esta, e pela conclusão anterior temos que $E = F(a_1, a_2, \ldots, a_n)$, ou seja, E é uma extensão algébrica múltipla de F.

($ii \Rightarrow iii$) Primeiramente notemos que a extensão múltipla $F(a_1, a_2, \ldots, a_n)$ pode ser construída pela sequência de extensões simples:

$$\begin{aligned}
F_1 &= F(a_1), \\
F_2 &= F(a_1)(a_2) = F_1(a_2), \\
F_3 &= F(a_1)(a_2)(a_3) = F_1(a_2)(a_3) = F_2(a_3), \\
&\vdots \\
F_n &= F(a_1)(a_2)\cdots(a_{n-2})(a_{n-1})(a_n) = F_{n-1}(a_n).
\end{aligned}$$

Se pudermos mostrar que estas extensões podem ser combinadas duas a duas para formar extensões simples, podemos aplicar repetidamente este resultado para deduzir que $F(a_1, a_2, \ldots, a_n)$ é uma extensão simples F.

É suficiente considerar então o caso para $n = 2$, e alterando a notação, mostrar que para quaisquer dois elementos b e c que são algébricos sobre F, existe um elemento a tal que $F(b, c) = F(a)$. Encontraremos um a na forma de uma combinação linear de b e c, $a = b + kc$, onde o coeficiente k é um elemento convenientemente escolhido de F.

Como b é algébrico sobre F, ele é raiz de algum polinômio minimal f, e portanto irredutível sobre F cujo conjunto completo de suas raízes são $b = b_1, b_2, \ldots, b_q$. Estas raízes são todas distintas, um vez que um polinômio irredutível não pode ter múltiplas raízes (Proposição 3.1). Analogamente, c é raiz de algum polinômio irredutível g, cujas raízes são $c = c_1, c_2, \ldots, c_m$, onde estas são todas distintas também. Olhe para as $q(m-1)$ equações em λ: $b_i + xc_j = b_1 + xc_1$, para $1 \leqslant i \leqslant q$, $2 \leqslant j \leqslant m$. Como para

esses valores de j, $c_j \neq c_1$, cada uma dessas equações tem exatamente uma solução em $\mathbb{C}$ para λ, e portanto, no máximo uma solução em F para λ. Como F tem um número infinito de elementos, podemos escolher $k \in F$ que não é nenhuma destas soluções. Assim, $b_i + kc_j \neq b_1 + kc_1$ sempre que $1 \leqslant i \leqslant q$ e $2 \leqslant j \leqslant m$.

Definindo $a = b + kc$, mostraremos que $F(b, c) = F(a)$. Primeiro, como tal $a \in F(b, c)$, temos que $F(a) \subset F(b, c)$. Para mostrar que $F(b, c) \subset F(a)$, é suficiente mostrar que ambos b, $c \in F(a)$. Observe que basta mostrarmos simplesmente que $c \in F(a)$, pois como $F(a)$ é corpo temos que $b = a - kc \in F(a)$.

Provaremos que $c \in F(a)$ mostrando que c é raiz de um polinômio de grau 1 sobre $F(a)$. Olhe para os polinômios $g(\lambda)$ e $f(a - k\lambda)$, ambos certamente estão em $F(a)$. (De fato, $g \in F[\lambda] \subset F(a)[\lambda]$). O número c é uma raiz de cada um, ou seja, $\tilde{g}(c) = 0$ e $\tilde{f}(a - kc) = \tilde{f}(b) = 0$. Como existe um *m.d.c.* desses polinômios e como ele é divisível por $(\lambda - c) \in \mathbb{C}[\lambda]$, ele tem c como uma raiz; a multiplicidade de c como uma raiz do *m.d.c.* é exatamente 1, pois c é uma raiz de multiplicidade 1 para g. Porém, pela escolha de k, os polinômios $g(\lambda)$ e $f(a - k\lambda)$ não têm em comum outras raízes, pois as outras raízes de g são da forma c_j, $2 \leqslant j \leqslant m$, e $a - kc_j \neq b_i$ para qualquer i. Assim, o tal *m.d.c.* de $g(\lambda)$ e $f(a - k\lambda)$ tem grau 1, pois todas as suas raízes são comuns a destes polinômios. Mas este *m.d.c.* é um polinômio sobre $F(a)$, o corpo dos coeficientes de $g(\lambda)$ e $f(a - k\lambda)$. Assim c, uma raiz do tal *m.d.c.*, é uma raiz do polinômio de grau 1 sobre $F(a)$. Portanto, $c \in F(a)$.

$(iii \Rightarrow i)$ Isto é imediatamente do Teorema 3.2. □

Teorema 3.4 (Multiplicatividade dos Graus)**.** *Sejam $K \subset M \subset L$ corpos. Então $[L : K]$ é finita, se, e somente se, $[L : M]$ e $[M : K]$ são finitas. Neste caso,*

$$[L : K] = [L : M][M : K].$$

Demonstração. Sejam $[L : K] < \infty$ e B uma base de L sobre K. Claramente $[M : K]$ é finita, uma vez que M é subespaço de um espaço vetorial de dimensão finita. Para mostrar a finitude de $[L : M]$, basta observar que existe $B' \subset B$ que é linearmente independente sobre M.

Suponha que $[L : M] = m$, $[M : K] = n$ e sejam $\{v_1, \ldots, v_m\}$ uma base de L sobre M e $\{w_1, \ldots, w_n\}$ uma base de M sobre K. Mostraremos que

$$\tilde{B} := \{v_i w_j | 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$$

é uma base de L sobre K. De fato, se $\alpha \in L$, existem $\alpha_1, \ldots, \alpha_m \in M$ tais que $\alpha = \sum_{i=1}^{m} \alpha_i v_i$. Cada α_i, por sua vez, é uma combinação da forma $\alpha_i = \sum_{j=1}^{n} \beta_{ij} w_j$, onde $\beta_{ij} \in K$, $1 \leqslant j \leqslant n$.

Logo,

$$\alpha = \sum_{i=1}^{m} (\sum_{j=1}^{n} \beta_{ij} w_j) v_i \Rightarrow \alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} (v_i w_j).$$

Portanto $\tilde{B}$ gera L como K-espaço vetorial. Para mostrar a K-independência linear dos elementos de $\tilde{B}$, seja

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\beta_{ij}(v_i w_j) = 0 \Rightarrow \sum_{i=1}^{m}(\sum_{j=1}^{n}\beta_{ij}v_i)w_j = 0.$$

Como $w_1, \ldots, w_n$ são linearmente independentes, para cada j, $1 \leqslant j \leqslant n$,

$$\sum_{j=1}^{n}\beta_{ij}v_i = 0.$$

Pela independência linear de $v_1, \ldots, v_m$ concluímos $\beta_{ij} = 0, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n$. Portanto $\tilde{B}$ é uma base de L sobre K. Para finalizar, observamos que

$$|\tilde{B}| = [L : K] = mn = [L : M][M : K].$$

□

Este teorema relativamente simples será aplicado frequentemente no desenvolvimento dos resultados subsequentes. Observamos que a aplicação repetida do teorema anterior para uma sequência finita de corpos $F_N \supset F_{N-1} \supset \cdots \supset F_1 \supset F_0$, em que para cada $j = 0, 1, \ldots, n-1$, $[F_{j+1} : F_j]$ é uma extensão finita, podemos garantir que,

$$[F_N : F_0] = [F_N : F_{N-1}][F_{N-1} : F_{N-2}] \cdots [F_1 : F_0].$$

3.2 Revendo as Construções Geométricas

Relembremos que a duplicação do cubo envolve a construção de uma raiz para o polinômio $\lambda^3 - 2$, que é irredutível sobre $\mathbb{Q}$. Similarmente, a trissecção de um ângulo de $60°$ envolve a construção de uma raiz do polinômio $\lambda^3 - 3\lambda - 1$, que também é irredutível sobre $\mathbb{Q}$ (Seção 2.1). Em cada caso foi requerido construir um número cujo grau sobre $\mathbb{Q}$ era 3. Usando a teoria de extensão de corpos, é muito simples de mostrar que os únicos números que podem ser construídos devem ter alguma potência de 2 como seu grau sobre $\mathbb{Q}$. Isto é, temos:

Teorema 3.5. *Se a é construtível, então a é algébrico e $\deg_{\mathbb{Q}}$ a é uma potência de 2.*

Demonstração. Se a é construtível, pelo Teorema 1.1, existe uma sequência finita de corpos $\mathbb{Q} = F_0 \subset F_1 \cdots \subset F_n$ tais que $a \in F_n$ e para cada j, F_{j+1} é uma extensão quadrática de F_j. Assim, para cada j, $[F_{j+1} : F_j] = 2$. Pela aplicação repetida do Teorema 3.4, temos que $[F_n : \mathbb{Q}] = 2^n$. Logo $[F_n : \mathbb{Q}] = 2^n$ é uma extensão finita e portanto algébrica pelo Teorema 3.3. Como $a \in F_n$, a é algébrico sobre $\mathbb{Q}$.

Agora, observe que $\mathbb{Q}(a) \subset F_n$, pelo Teorema 3.4

$$[F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}].$$

Como o lado esquerdo é 2^n, nenhum fator do lado direito pode ter um fator primo ímpar. Portanto, $[\mathbb{Q}(a) : \mathbb{Q}]$ deve ser uma potência de 2, que pelo Teorema 3.2 equivale a $\deg_{\mathbb{Q}} a$. □

Temos ainda, como um corolário, a seguinte reformulação:

Corolário 3.1. *É impossível construir qualquer número que seja raiz de um polinômio irredutível sobre* $\mathbb{Q}$ *que tenha grau diferente de uma potência de* 2.

Demonstração. Seja a uma raiz de $p(\lambda)$, um polinômio irredutível sobre $\mathbb{Q}$ que tem grau diferente de uma potência de 2. Como p é irredutível sobre $\mathbb{Q}$, pelo Teorema 3.1 p é um polinômio minimal de a sobre $\mathbb{Q}$.

Assim, se a fosse um número construtível, a seria algébrico sobre $\mathbb{Q}$ e $\deg_{\mathbb{Q}} a$ seria um número diferente de uma potência de 2, contrariando o Teorema 3.5. □

Segue imediatamente deste resultado que é impossível duplicar o cubo, pois isto requer a construtibilidade da raiz de um polinômio irredutível sobre $\mathbb{Q}$ de grau 3. Analogamente, é impossível trissectar o ângulo 60°, o que mostra que não existe uma maneira de trissectar uma ângulo arbitrário. Embora as soluções originais para estes problemas sejam bem simples, percebe-se que o método atual é mais geral e poderoso.

Com estes métodos agora disponíveis, finalmente somos capazes de lidar com outro problema famoso: **Para quais valores de n é possível construir um polígono regular de n lados?** Tal polígono é chamado de *n-ágono regular*.

Primeiramente, observe que a construtibilidade de um *n-ágono regular* está equivalente a construtibilidade de um ângulo de $360°/n$. Pois, se $360°/n$ é construtível, podemos inscrever um *n-ágono regular* no círculo unitário marcando sucessivamente a abertura do ângulo central como na figura 3.1.

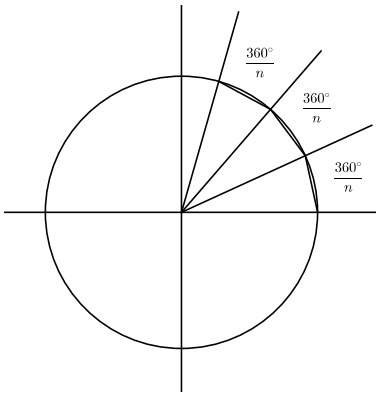

Figura 3.1: O n-ágono regular no círculo unitário.

Reciprocamente, se um *n-ágono regular* é construtível, cada um dos seus ângulos exteriores são construtíveis, e como a soma deles é 360°, cada um é $360°/n$ (Figura 3.2).

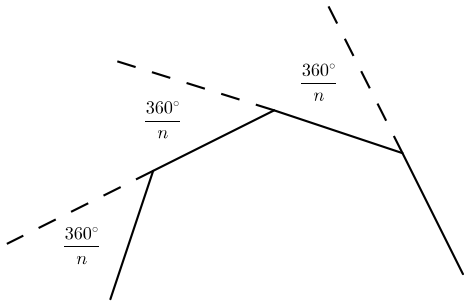

Figura 3.2: Ângulos externos do n-ágono regular.

Por outro lado, pode-se construir o centro do círculo em que o *n-ágono* está inscrito, tomando o ponto de intersecção das mediatrizes de quaisquer dois lados não paralelos. Assim, desenha-se o círculo. Os arcos entre quaisquer dois vértices sucessivos medem o valor do ângulo central de $360^\circ/n$.

Por tudo isso, fica claro que a construtibilidade de um ângulo de $360^\circ/n$ é, portanto, equivalente a construtibilidade de pontos da forma $(\cos(k360^\circ/n), \operatorname{sen}(k360^\circ/n))$ em $\mathbb{R}^2$. Na próxima sessão, devemos ver que esse pontos podem ser representados por números complexos. Além disso, veremos que toda a teoria da construtibilidade pode ser estendida simplesmente para os números complexos. Dentro deste quadro, seremos então capazes de resolver este problema.

3.3 Raízes de Números Complexos

Dizemos que o número x é uma *raiz n-ésima* de um dado número complexo a, se $x^n = a$. Todo número complexo $a \neq 0$ tem n raízes *n-ésimas* distintas. O polinômio $x^n - a$ tem exatamente n raízes (Teorema 2.7). As raízes *n-ésimas* do número 1 são chamadas de *raízes n-ésimas da unidade*, e são particularmente importantes para nosso trabalho.

Por exemplo, as raízes cúbicas da unidade são as raízes do polinômio $x^3 - 1$. Como 1 é uma raiz, podemos dividi-lo por $x - 1$ e obter $x^2 + x + 1$ cujas raízes $\dfrac{-1 \pm i\sqrt{3}}{2}$ são as outras raízes cúbicas da unidade. As raízes quarta da unidade são as raízes do polinômio $x^4 - 1$, que pode ser fatorado em $(x^2+1)(x^2-1)$, de onde obtemos os quatro valores, $+i, -i, +1, -1$.

Uma representação da raiz *n-ésima* da unidade é fornecida pela função exponencial complexa. Para isto, faremos alguns comentários sobre esta função. Se z é um número complexo, ele pode ser escrito na forma $z = x + iy$, onde x e y são números reais.

Os números x e y são chamados de parte *real* e parte *imaginária*, respectivamente. A expressão e^z é definida por ser o número complexo $e^x(\cos y + i \operatorname{sen} y)$, que envolve somente funções exponenciais e trigonométricas de variável real. Desta definição segue

que $e^{2\pi i} = e^0(\cos 2\pi + i \operatorname{sen} 2\pi) = 1$ e também que e^z satisfaz as propriedades usuais da exponencial, por exemplo $e^{z_1}e^{z_2} = e^{z_1+z_2}$.

Para todo $n \geqslant 2$, algumas das raízes *n-ésimas* da unidade podem ter a propriedade de que elas também são raízes *m-ésimas* da unidade para algum $0 < m < n$. Por exemplo, embora -1 seja uma raiz *quarta* da unidade ($n = 4$, ou seja, $(-1)^4 = 1$), -1 também é uma raiz *quadrada* da unidade ($n = 2$, $(-1)^2 = 1$). Aquelas raízes *n-ésimas* da unidade que não são raízes *m-ésimas* da unidade para qualquer que seja m com $0 < m < n$, são chamadas de *raízes n-ésimas primitivas da unidade.*

Proposição 3.2. *Se ω é uma raiz n-ésima primitiva da unidade, então os números $\omega, \omega^2, \cdots, \omega^n = 1$ formam a lista completa das raízes n-ésimas da unidade.*

Demonstração. Observe, primeiro, que todos esses números são raízes n-ésimas da unidade, ou seja, para qualquer que seja ω^j temos,

$$(\omega^j)^n = \omega^{jn} = (\omega^n)^j = (1)^j = 1,$$

com $1 \leqslant j \leqslant n$.

Além disso, eles são todos distintos, pois caso contrário se $\omega^j = \omega^k$ com $1 \leqslant k < j \leqslant n$, teríamos, dividindo a igualdade por ω^k, que $\omega^{j-k} = 1$. Isto contradiz a natureza primitiva de w, pois $1 \leqslant j - k \leqslant n - 1$. □

A *Função Euler* definida por $\phi(n) = \sharp\{k \in \mathbb{Z}^+ | \forall k \leqslant n,\ m.d.c\{k, n\} = 1\}$ (ou seja, o número de inteiros entre 1 e n inclusive, que são relativamente primos a n) fornece o número de raízes n-ésimas primitivas da unidade:

Teorema 3.6. *Se ω é uma raiz n-ésima primitiva da unidade, então ω^k é também uma raiz n-ésima primitiva da unidade se, e somente se, k e n são relativamente primos. O número de raízes n-ésimas primitivas da unidade é $\phi(n)$.*

Demonstração. A segunda sentença claramente seguirá imediatamente da primeira, pois todas as raízes da unidade são representadas pelos valores de k variando de 1 a n.

($\Leftarrow$) Suponha que k e n são relativamente primos. Queremos provar que não existe m, com $1 \leqslant m < n$ tal que $(\omega^k)^m = 1$. Se existisse algum m, $1 \leqslant m < n$, tal que $(\omega^k)^m = 1$, km deveria ser um inteiro múltiplo de n, ou seja, existiria um $q \in \mathbb{Z}$ tal que $km = nq$; de fato, caso contrário, pelo algoritmo da divisão em $\mathbb{Z}$, existiriam $q, r \in \mathbb{Z}$ tais que $km = nq + r$ com $1 \leqslant r < n$. Assim teríamos,

$$(\omega^k)^m = \omega^{kn} = \omega^{nq}\omega^r = (\omega^n)^q\omega^r = (1)^q\omega^r = 1\omega^r = \omega^r,$$

ou seja, $(\omega^k)^m = \omega^r$ Como, $(\omega^k)^m = 1$, teríamos $\omega^r = 1$ o que contraria a primitividade de ω, pois $1 \leqslant r < n$. Portanto, caso tal m exista, $km = nq,\ q \in \mathbb{Z}$. Disto segue que $n|km$ e portanto $n|k$ ou $n|m$ já que n e k são relativamente primos, por hipótese. Logo, $n|m$ o que é um absurdo pois $n > m$.

($\Rightarrow$) Seja ω^k uma raiz n-ésima primitiva da unidade. Mostremos que k e n são relativamente primos. Se k e n não fossem relativamente primos, eles teriam um fator inteiro primo p em comum. Assim, tomando $m = \dfrac{n}{p} < n$, temos

$$(\omega^k)^m = (\omega^k)^{\frac{n}{p}} = \omega^{\frac{kn}{p}} = (\omega^n)^{\frac{k}{p}} = 1^{\frac{k}{p}} = 1,$$

pois $\frac{k}{p}$ é um inteiro. Logo, ω^k seria uma raiz m-ésima da unidade contrariando a hipótese. Portanto k e n são relativamente primos. □

Observamos também que se r é uma raiz n-ésima qualquer do número complexo $a \neq 0$ e se ω é uma raiz n-ésima primitiva da unidade, então as n distintas raízes n-ésimas da unidade são dadas por $r\omega, r\omega^2, \cdots, r\omega^n = r$.

Existe uma interpretação geométrica dos números complexos bastante útil para nosso trabalho. Sendo $z = x + iy$, onde x e y são reais, representamos z no plano cartesiano pelo ponto (x, y). Em coordenadas polares podemos escrever,

$$\begin{aligned} z &= x + iy, \\ z &= \sqrt{x^2+y^2}.(\frac{x}{\sqrt{x^2+y^2}} + i\frac{y}{\sqrt{x^2+y^2}}), \\ z &= |z|[\cos\theta + i\,\mathrm{sen}\,\theta], \\ z &= |z|e^{i\theta}. \end{aligned}$$

O ângulo θ é chamado de argumento de z; o número $|z| = \sqrt{x^2+y^2}$ é chamado de módulo de z. É a situação descrita na figura 3.3.

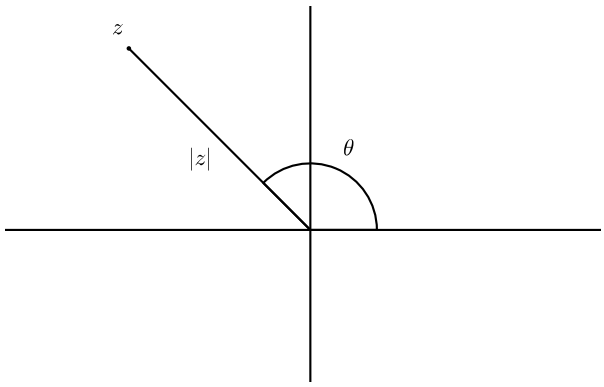

Figura 3.3: Representação geométrica de um número complexo.

A representação de um número complexo z na forma $z = |z|e^{i\theta}$ é chamada de representação polar. Ela dá um caminho muito conveniente para interpretar a multiplicação de números complexos. Escrevendo $z_1 = |z_1|e^{i\theta_1}$ e $z_2 = |z_2|e^{i\theta_2}$, as leis dos expoentes implicam que

$$z_1 z_2 = |z_1||z_2|e^{i(\theta_1+\theta_2)},$$

de modo que o módulo de um produto é o produto dos módulos e o argumento do produto é a soma dos argumentos.

Assim, uma raiz *n-ésima* de um número complexo z pode ser obtida tomando a raiz *n-ésima* real positiva de seu módulo e dividindo seu argumento por n. Isto é, uma raiz *n-ésima* de $z = |z|e^{i\theta}$ é dada por,

$$r = \sqrt[n]{|z|e^{i\theta}} = \sqrt[n]{|z|}\sqrt[n]{e^{i\theta}} = \sqrt[n]{|z|}(e^{i\theta})^{1/n},$$

$$r = \sqrt[n]{|z|}e^{\frac{i\theta}{n}}.$$

Logo,

$$r^n = (\sqrt[n]{|z|}e^{i\theta/n})^n = |z|e^{i\theta} = z.$$

Na representação gráfica de números complexos, observamos que as raízes *n-ésimas* da unidade são representadas pelos pontos,

$$(\cos(\frac{2\pi k}{n}),\ \text{sen}(\frac{2\pi k}{n})),\ 1 \leqslant k \leqslant n,$$

que são n pontos espaçados igualmente no círculo unitário, incluindo o ponto $(1, 0)$.

Se tomarmos $w = e^{\frac{2\pi i}{n}}$, estes pontos são marcados e rotulados como potências de w; observe a figura 3.4.

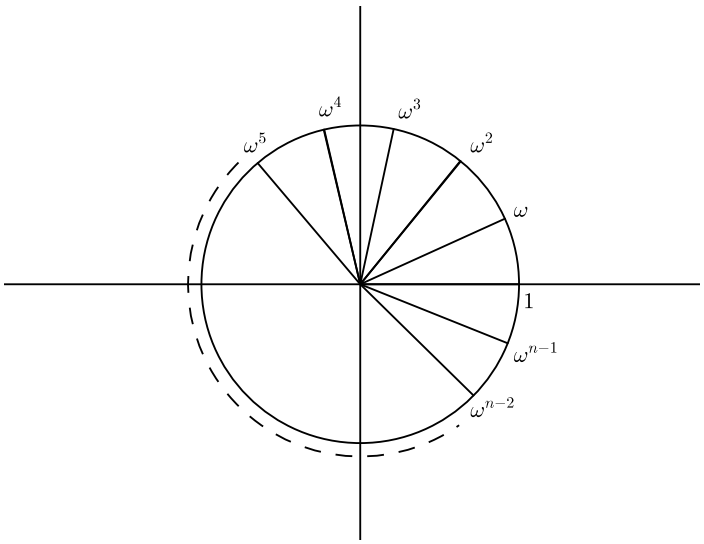

Figura 3.4: Raízes n-ésimas da unidade no círculo unitário.

Note que estes são precisamente os pontos que devem ser determinados para construir o *n-ágono* regular.

Com respeito as n raízes *n-ésimas* de um número complexo z qualquer, elas são simplesmente n pontos espaçados igualmente sobre um círculo de raio $\sqrt[n]{|z|}$.

3.4 Construtibilidade de Polígonos Regulares

Nessa seção será possível fazer um progresso substancial sobre a questão formulada na Seção 3.2. "Para quais valores de n é possível construir um *n-ágono regular*?"

Foi visto na Seção 3.3 que a construtibilidade de um *n-ágono* regular é equivalente a construir pontos no Plano Cartesiano correspondendo as raízes *n-ésimas* da unidade. Como estes números são complexos, será necessário estender a definição de construtibilidade diretamente para números complexos.

Para $a \in \mathbb{C}$, dizemos que a é construtível se sua parte real e imaginária são construtíveis. Isto é equivalente a construtibilidade do ponto "a" no plano cartesiano. A teoria de construtibilidade estende-se imediatamente para os números complexos, através dos Lemas 3.1 e 3.2 e dos Teoremas 3.7 e 3.8.

Lema 3.1. *Se a_1 e a_2 são construtíveis, então $a_1 + a_2$ e $a_1 a_2$ também são.*

Demonstração. Sejam b_i e c_i, respectivamente a parte real e a parte imaginária de cada a_i. Do cálculo abaixo, vemos que as partes real e imaginária que resultam do combinado de a_1 e a_2 são construtíveis, pelo Lema 1.1. Temos:

(i) $a_1 + a_2 = (b_1 + b_2) + i(c_1 + c_2)$

(ii) $a_1 a_2 = (b_1 + ic_1)(b_2 + ic_2) = (b_1 b_2 - c_1 c_2) + i(b_1 c_2 + b_2 c_1)$ □

Lema 3.2. *Se a é construtível e se $k^2 = a$, então k é construtível.*

Demonstração. Observe que um número complexo $z = |z|e^{i\theta}$ é construtível se, e somente se, o número real $|z|$ e o ângulo θ são construtíveis. Assim, sendo a construtível, o número $|a|$ e um ângulo θ, um argumento de a, são construtíveis. Pelo Lema 1.2, $\sqrt{|a|}$ é construtível e como um ângulo pode ser bissectado, o ângulo $\theta/2$ é construtível. Agora, como $k = \pm\sqrt{|a|}e^{\frac{i\theta}{2}}$, segue que k é construtível. □

Na afirmação do Lema 3.2, foi feito referência a um número k tal que $k^2 = a$; mas não escrevemos $\sqrt{a}$. A razão é esta: considerando "a" um número real positivo, $\sqrt{a}$ está bem definida como a única raíz quadrada positiva de a; quando "a" é complexo, não temos um caminho natural para considerar uma raiz quadrada particular de "a".

Com este cuidado em mente, devemos concordar em usar o símbolo $\sqrt{a}$ ou $\sqrt[n]{a}$ como uma abreviação para uma raiz quadrada ou *n-ésima* de a nos casos em que a afirmação feita for verdadeira para todas tais raízes.

Por uma extensão quadrática de um corpo arbitrário F queremos dizer uma extensão simples $F(\sqrt{a})$, onde $a \in F$ e $\sqrt{a} \notin F$; como as duas raízes quadráticas de a são o negativo uma da outra, a extensão por qualquer uma é o mesmo corpo. O Teorema 1.1 forneceu uma condição necessária e suficiente para construtibilidade de números reais, e ela estende-se facilmente para o caso complexo.

Teorema 3.7. *As afirmações seguintes são equivalentes:*

(i) *O número complexo a é construtível.*

(ii) *Existe uma sequência finita de corpos $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$, com $a \in F_n$ tal que para cada j, $0 \leqslant j \leqslant n-1$, F_{j+1} é uma extensão quadrática de F_j.*

Demonstração. $(i) \Rightarrow (ii)$ Suponha $a = b + ic$, com $b, c \in \mathbb{R}$. Pelo Teorema 1 e a construtibilidade de b e c, existem duas sequências de extensões quadráticas:

$$\mathbb{Q} = G_0 \subset G_1 \subset \cdots \subset G_l, \text{com } b \in G_l,$$

$$\mathbb{Q} = H_0 \subset H_1 \subset \cdots \subset H_m, \text{com } c \in H_m.$$

Para cada j, $H_{j+1} = H_j(\sqrt{k_j})$. Se estendermos G_l, um passo de cada vez, por

$$\sqrt{k_0}, \sqrt{k_1}, \cdots, \sqrt{k_{m-1}}, \text{e } i,$$

omitindo na sequência qualquer repetição, teremos a sequência de extensões quadráticas, com o último corpo contendo b, c e i e portanto a.

$(ii) \Rightarrow (i)$ Por indução sobre n. Se $n = 0$, a é racional e portanto construtível. Agora assumimos que o Teorema é verdadeiro para $n = r$ e provemos para $n = r + 1$.

Se $a \in F_{r+1}$, então $a = a_r + b_r\sqrt{k_r}$, onde a_r, b_r e k_r pertencem a F_r e portanto são construtíveis. Assim pelo Lema 3.1, seque que a é construtível. □

Por exatamente as mesmas razões de antes, usamos o Teorema 3.7 para obter o análogo para números complexos do Teorema 3.5 e seu Corolário.

Teorema 3.8. *Se $a \in \mathbb{C}$ é construtível, então a é algébrico e* $\deg_{\mathbb{Q}}$ *a é uma potência de* 2.

Corolário 3.2. *É impossível construir qualquer número complexo que seja a raiz de um polinômio irredutível sobre $\mathbb{Q}$ que tem grau diferente de uma potência de* 2.

Agora estamos prontos para lidar com a questão iniciada no começo desta seção. A construtibilidade do *n-ágono* regular é equivalente a construtibilidade das raízes n-ésimas da unidade, e portanto, em vista do Lema 3.1, a construtibilidade de qualquer raiz primitiva da unidade (pois qualquer raiz da unidade é um produto de uma raiz primitiva da unidade com ela mesma um número apropriado de vezes).

A maneira natural de procedermos é calcular o grau de uma raiz n-ésima primitiva da unidade sobre $\mathbb{Q}$. Depois excluir todos os valores de n para o qual este grau não é potência de 2. Acontece que as $\phi(n)$ raízes primitivas da unidade são precisamente o conjunto das raízes de um polinômio irredutível sobre $\mathbb{Q}$, com coeficientes inteiros, chamado de n-ésimo polinômio ciclotômico, e que tem grau $\phi(n)$. Mostrar esta afirmação não é simples, e ainda que a mostrássemos, teríamos a dificuldade de avaliar para quais valores de n, $\phi(n)$ é uma potência de 2. Simplificamos o problema trabalhando com divisores de n. Assim, teremos condições de garantir o Teorema 3.8 que diminui os

candidatos a valores de "n" para o qual o n-ágono regular pode ser construído. Vejamos alguns resultados:

Lema 3.3. *Se o n-ágono regular é construtível, então o m-ágono regular também é para todo $m \geqslant 3$ tal que $m|n$.*

Demonstração. Seja $m \geqslant 3$ tal que $m|n$. Logo, existe $k \in \mathbb{N}$ tal que $n = mk$. Como o *n-ágono* é construtível, seus n vértices são construtíveis. Assim, traçando segmentos a cada k a k vértices do n-ágono, construiremos o m-ágono regular. Sua construtibilidade é garantida pois usamos os vértices construtíveis do n-ágono. □

Proposição 3.3. *Seja $f \in \mathbb{Q}[\lambda]$ e $a \in \mathbb{Q}$. Então $f(\lambda)$ é irredutível se, e somente se, $f(\lambda + a)$ também é.*

Demonstração. ($\Rightarrow$) Suponha que $f(\lambda + a)$ é redutível. Logo existem $g, h \in \mathbb{Q}[\lambda]$ tais que

$$f(\lambda + a) = g(\lambda + a)h(\lambda + a).$$

Fazendo $\lambda = \lambda - a$,

$$f(\lambda) = g(\lambda)h(\lambda).$$

Assim, temos que f é redutível, o que contraria a hipótese.

($\Leftarrow$) Por outro lado, suponha que $f(\lambda)$ é redutível. Logo, existem $r, s \in \mathbb{Q}[\lambda]$ tais que

$$f(\lambda) = r(\lambda)s(\lambda).$$

Fazendo $\lambda = \lambda + a$, temos

$$f(\lambda + a) = r(\lambda + a)s(\lambda + a).$$

Um contradição, pois por hipótese $f(\lambda + a)$ é irredutível. □

Corolário 3.3. *Seja $f(\lambda) = \dfrac{\lambda^n - 1}{\lambda - 1} = \lambda^{n-1} + \lambda^{n-2} + \cdots + 1$ sobre $\mathbb{Q}$. Se $n = p$ é primo, então f é irredutível.*

Demonstração. Pela proposição anterior, basta mostrar que $f(\lambda+1)$ é irredutível sobre $\mathbb{Q}$. Temos,

$$f(\lambda + 1) = (\lambda + 1)^{p-1} + (\lambda + 1)^{p-2} + \cdots + (\lambda + 1) + 1,$$

e é fácil vermos que, para $1 \leqslant k \leqslant p - 2$, o coeficiente a_k de λ^k é

$$a_k = \binom{p-1}{k} + \binom{p-2}{k} + \binom{p-3}{k} + \cdots + \binom{k}{k} = \binom{p}{k+1},$$

que, portanto é múltiplo de p. Como,

$$f(\lambda + 1) = \lambda^{p-1} + a_{p-2}\lambda^{p-2} + \cdots + a_1\lambda + 1,$$

segue do critério de Eisenstein aplicado ao primo p que $f(\lambda + 1)$ é irredutível sobre $\mathbb{Q}$, e portanto $f(\lambda)$ também é. □

Proposição 3.4. *Se um n-ágono regular é construtível e se p é um primo ímpar que divide n, então p é da forma* $2^{2k}+1$.

Demonstração. Pela hipótese e pelo Lema 3.3, o *p-ágono* regular é construtível. Assim, as raízes *p-ésimas* da unidade são construtíveis.

Mas as $(p-1)$ raízes *p-ésimas* primitivas da unidade são raízes do polinômio

$$\frac{\lambda^p-1}{\lambda-1}=\lambda^{p-1}+\lambda^{p-2}+\cdots+1,$$

que pelo Corolário 3.3 é um polinômio irredutível.

Assim, pelo Teorema 3.8, $p-1$ dever ser uma potência de 2, ou seja,

$$p-1=2^m \Rightarrow p=2^m+1,$$

para algum inteiro m positivo.

Contudo, a única vez que um número dessa forma pode ser primo é quando $m=2^k$ para algum k. Para ver isto, note que para $m=1$ temos $k=0$ e portanto $p=3$. Já para $m>1$, m é da forma 2^k ou tem um fator ímpar q, tal que $m=qr$. Se m tivesse um tal fator ímpar q, então

$$p=2^m+1=2^{qr}+1=(2^r)^q+1^q=[2^r+1][(2^r)^{q-1}-(2^r)^{q-2}+(2^r)^{q-3}-\cdots-2^r+1],$$

ou seja, teríamos p como um produto de fatores onde nenhum deles é $\pm p$ e ± 1, contrariando a hipótese de p ser primo. Portanto, $m=2^k$. □

Primos da forma $2^{2^k}+1$ são chamados de Primos de Fermat. Os únicos conhecidos até o momento são $3, 5, 17, 257$ e 65537. Assim, se um n-ágono regular é construtível, todos os fatores primos ímpares de n devem ser primos de Fermat.

Além disso, nenhum primo ímpar pode dividir n mais de uma vez. Para garantirmos tal afirmação, precisamos dos seguintes resultados:

Lema 3.4. *Se p é primo e n um inteiro positivo, então* $\phi(p^n)=p^{n-1}(p-1)$.

Demonstração. Seja $\phi(p^n)=\#U$, onde $U=\{l\in\{1,2,\ldots,p^n\}|mdc(l,p^n)=1\}$,

$$l\in U \Leftrightarrow mdc(l,p^n)=1.$$

Logo, $p\nmid l$ (pois, se $p|l$, necessariamente $p|1$ pelo Teorema de Bezout, o que é um absurdo). Assim,

$$l\notin\{p.k|k=1,2,\ldots,p^{n-1}\},$$

conjunto que tem p^{n-1} elementos.

Portanto,

$$\phi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1).$$

□

Lema 3.5. *O grau sobre $\mathbb{Q}$ das raízes n-ésimas primitivas da unidade para $n = p$ e $n = p^2$, quando p é primo são $p-1$ e $p(p-1)$ respectivamente.*

Demonstração. Para $n = p$, as raízes *p-ésimas* primitivas da unidade são raízes do polinômio $\dfrac{\lambda^p - 1}{\lambda - 1} = \lambda^{p-1} + \lambda^{p-2} + \cdots + 1$, que pelo Corolário 3.3 é irredutível sobre Q. Portanto, o grau dessas raízes sobre $\mathbb{Q}$ é $(p-1)$.

Para $n = p^2$, as raízes p^2*-ésimas* primitivas da unidade são raízes do polinômio $\dfrac{\lambda^{p^2} - 1}{\lambda^p - 1} = \lambda^{p(p-1)} + \lambda^{p(p-2)} + \cdots + 1$. Este polinômio é irredutível sobre $\mathbb{Q}$, e isto pode ser visto fazendo a mudança de variável, $\lambda = u + 1$. Assim,

$$\begin{aligned} \textstyle\sum_{k=1}^{p}(u+1)^{p(p-k)} &= \textstyle\sum_{k=1}^{p}[(u+1)^p]^{(p-k)} \\ &= \textstyle\sum_{k=1}^{p}[u^p + 1 + pg(u)]^{(p-k)} \\ &= \textstyle\sum_{k=1}^{p}[(u^p+1)^{p-k} + ph_k(u)], \end{aligned}$$

onde cada $h_k(u)$ é um polinômio de grau $(p-1)(p-k)$ com coeficientes inteiros. Usando a fórmula da soma de uma progressão geométrica finita

$$\begin{aligned} \textstyle\sum_{k=1}^{p}(u+1)^{p(p-k)} &= \textstyle\sum_{k=1}^{p}(u^p+1)^{p-k} + pH(u) \\ &= \dfrac{(u^p+1)^p - 1}{u^p} + pH(u) \\ &= u^{p(p-1)} + pG(u), \end{aligned}$$

para algum polinômio G de grau $(p-1)^2$. Para aplicar o critério Eisenstein, precisamos ainda mostrar que o termo constante de toda a expressão não é divisível por p^2. Embora pudéssemos traçar esse valor através do cálculo, é mais fácil apenas ligar $u = 0$ a soma original, que dá termo constante igual a p. Agora, pelo critério de Eisenstein o polinômio em u, e portanto em x, é irredutível. Além disso, o grau sobre $\mathbb{Q}$ das raízes p^2*-ésimas* primitivas da unidade é $p(p-1)$. □

Proposição 3.5. *Se um n-ágono regular é construtível e se p é um primo ímpar que divide n, então p^2 não divide n.*

Demonstração. Do Lema 3.4, temos que $\phi(p^2) = p(p-1)$. Se $p^2|n$, pelo Lema 3.3 as $p(p-1)$ raízes p^2-ésimas primitivas da unidade deveriam ser construtíveis.

Mas cada uma dessas tem grau $p(p-1)$ sobre $\mathbb{Q}$, pelo Lema 3.5. Como seus graus tem o fator ímpar p, as raízes p^2-ésimas primitivas da unidade não podem ser construtíveis (Teorema 3.8). Portanto, p^2 não pode dividir n.

□

Com os resultados sobre n-ágono até aqui, obtemos a seguinte condição necessária sobre n para a construtibilidade de um n-ágono regular.

Teorema 3.9. *Para o n-ágono regular ser construtível, n dever ser da forma $2^k p_1 p_2 \cdots p_m$ onde os p_i's são primos de Fermat distintos (m pode ser igual a 0, caso em que n não tem fatores ímpares)*

Demonstração. Seja *n-ágono* regular um polígono construtível. Pelo Teorema Fundamental da Aritmética,

$$n = q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m},\ q_i's \text{ são primos distintos e com } r_i's \geqslant 1.$$

Se existe q_i como acima ímpar, pelo Lema 3.4, $q_i = 2^{2^k} + 1$ e pelo Lema 3.5 $r_i = 1$. Ainda pode acontecer que algum $q_i = 2$ e $r_i \geqslant 2$, então

$$n = 2^{r_i} \prod_{i=1}^{s} (2^{2k_i} + 1).$$

□

A recíproca deste Teorema também vale, isto é, para todo n da forma dada, é realmente possível construir o n-ágono regular. A prova disto pode ser vista em [1].

Podemos observar que o Teorema 3.9 implica que não é possível construir polígonos com $7, 11$ ou 90 lados. O problema de trissectar o ângulo de $60°$ exigiria a construtibilidade de um 18-ágono regular e como $18 = 2 \times 3^2$, isto é impossível.

Referências

[1] HADLOCK, C. *Field Theory and Its Classical Problems*. Reino Unido: The Mathematical Association of America (Cambridge University Press), 2000.

[2] SAMUEL, P. *Uma demostração Algébrica para o Teorema Fundamental da Álgebra*. Disponível em: <http://legauss.blogspot.com.br/2010/01/uma-demonstracao-algebrica-para-o.html>.

[3] COURANT, R.; ROBBINS, H. *O que é Matemática?* Rio de Janeiro: Editora Ciência Moderna Ltda, 2000.

[4] GONÇALVEZ, A. *Introdução a Álgebra*. 5. ed. Rio de Janeiro: Projeto Euclides, 2009.

[5] KAKUTA, N.; SALERYAN, P. *Introdução à Teoria de Galois*. São José do Rio Preto: Editora Unesp Ibilce, 2013.

[6] ÁVILA, G. *Variáveis complexas e aplicações*. 3. ed. Rio de Janeiro: LTC, 2011.

[7] HERSTEIN, I. N. *Tópicos de Álgebra*. São Paulo: Editora Polígno S. A., 1970.

[8] DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 4. ed. São Paulo: Atual Editora, 2003.