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

Um Estudo sobre as Raízes da Unidade e suas Aplicações em Matemática

Josiane de Carvalho Rezende

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

Orientadora
Profa. Dra. Carina Alves

2017

510 Rezende, Josiane de Carvalho
R467e Um estudo sobre as raízes da unidade e suas aplicações em matemática / Josiane de Carvalho Rezende. - Rio Claro, 2017
71 f. : il., figs.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas
Orientador: Carina Alves

1. Matemática. 2. Resolução de equações. 3. Teorema de Fermat. 4. Construção de reticulados. 5. Corpos ciclotômicos. 6. Teorema de Dirichlet. I. Título.

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Josiane de Carvalho Rezende

Um Estudo sobre as Raízes da Unidade e suas Aplicações em Matemática

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

Profa. Dra. Carina Alves
Orientadora

Profa. Dra. Marta Cilene Gadotti
Departamento de Matemática - UNESP (Rio Claro)

Prof. Dr. Cristiano Torezzan
Faculdade de Ciências Aplicadas - UNICAMP (Limeira)

Rio Claro, 03 de Fevereiro de 2017

Dedicada aos meus presentes e futuros alunos.

Agradecimentos

Houve grande espera para o meu ingresso ao programa de mestrado. Na elaboração dessa dissertação foram necessários meses de dedicação e estudo, e por isso quero agradecer primeiramente a Deus, que me deu forças para continuar diante de tantas dificuldades apresentadas.

Agradeço ao Prof. Dr. Edson Donizete de Carvalho, que além de ter sido, durante a graduação, um ótimo orientador em meu projeto de extensão, foi o principal motivador para o meu ingresso ao programa de mestrado na Unesp de Rio Claro.

Agradeço aos funcionários do Programa de Pós-Graduação da UNESP, que sempre foram muito atenciosos a todas as dúvidas.

Agradeço aos professores, pela partilha do conhecimento, pela paciência e pelos ensinamentos para a vida.

Aos meus amigos, pelas horas de risos, estudos e por todo o apoio.

Quero agradecer minha orientadora, Profa. Dra. Carina Alves, pela sua disponibilidade, atenção, amizade, por toda a sua ajuda e colaboração em todas as etapas da dissertação.

A minha família, que apesar das dificuldades que encontrei, sempre esteve ao meu lado me apoiando para que eu pudesse concluir essa importante etapa da minha vida.

Aos meus professores, colegas de trabalho e família meu agradecimento pela preocupação, incentivo e ajuda nos estudos. Enfim, agradeço a todas as pessoas que contribuíram para esta realização.

Resumo

A procura pela solução de alguns problemas relevantes, ou ainda, de equações, têm sido uma fonte de inspiração para ampliar os conjuntos numéricos. Quanto ao conjunto dos números complexos, um importante resultado é que todo polinômio de grau $n \geq 1$ e com coeficientes complexos tem n raízes complexas. De modo geral, o presente trabalho tem o objetivo de contextualizar algumas aplicações das raízes da unidade na matemática. Apresentamos sua aplicação em um caso particular do Teorema de Dirichlet, na construção de reticulados, cuja utilidade está ligada a problemas de transmissão de sinal, e na história da resolução do Último Teorema de Fermat.

Abstract

The search for the solution of some relevant problems, or even of equations, has been a source of inspiration to extend the numerical sets. As for the set of complex numbers, an important result is that every polynomial of degree $n \geq 1$ and with complex coefficients has n complex roots. In general, the present work aims to contextualize some applications of the roots of unit in mathematics. We present its application in a particular case of the Dirichlet Theorem, in the construction of lattices, whose utility is linked to signal transmission problems, and in the history of the resolution of the Fermat's Last Theorem.

Lista de Figuras

Sumário

1 Introdução

A História da Matemática nos mostra que a procura pela solução de alguns problemas relevantes, ou ainda, de equações, têm sido uma fonte de inspiração para ampliar os conjuntos numéricos. No conjunto dos números naturais $\mathbb{N}$ não podemos resolver a equação $x+3=0$, por exemplo. Ampliando esse conjunto para os números inteiros $\mathbb{Z}$, a equação anterior passa a ter solução, pois $-3 \in \mathbb{Z}$.

A inclusão de números negativos não resolve completamente as soluções de equações, pois, há equações sem solução em $\mathbb{Z}$, por exemplo, $5x+3=0$. Com isso, o conjunto dos inteiros foi ampliado para o conjunto dos números racionais $\mathbb{Q}$.

Com o objetivo de realizar a operação de radiciação, o conjunto dos números racionais precisou ser ampliado para o conjunto dos números reais $\mathbb{R}$. Desse modo, números tais como $\sqrt{2}, \sqrt{3}, \sqrt[3]{2}, \sqrt[3]{5}, \cdots$, chamados de irracionais, foram incluídos no sistema numérico, permitindo extrair raízes n-ésimas e resolver equações tais como $x^2-2=0, x^2-3=0, x^3-2=0, x^3-5=0, \cdots$, antes sem solução em $\mathbb{Q}$.

Com isso, foram obtidos os conjuntos numéricos $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Entretanto, equações tais como $x^2+1=0, x^2+2=0, x^2+x+1=0$ não possuem solução no conjunto dos números reais, pois não se pode extrair raízes quadradas de números reais negativos.

Isto serviu de motivação para ampliar o conjunto dos números reais à construção de um conjunto de números em que é possível extrair raízes quadradas de números reais negativos.

Segundo [14], em 1545 Gerônimo Cardano (Itália, 1501 - 1576), um dos mais destacados matemáticos do Renascimento, achou a resposta

$$\alpha = 5+\sqrt{-15} \quad \text{e} \quad \beta = 5-\sqrt{-15},$$

para o problema de determinar dois números cuja soma vale 10 e cujo produto vale 40, ou ainda, as raízes da equação do segundo grau $x^2-10x+40=0$. Na época as raízes quadradas de números negativos eram consideradas inexistentes, logo essas soluções eram tidas como absurdas.

O notável é que se operarmos formalmente com essas raízes, como se tivessem as propriedades aritméticas da adição e da multiplicação dos números reais e convencionarmos que

$$\left(\sqrt{-15}\right)^2 = -15,$$

podemos mostrar sem dificuldade que

$$\alpha + \beta = 10 \quad \text{e} \quad \alpha.\beta = 40.$$

O matemático indiano Rafael Bombelli (1526 - 1572) começou a estudar esses números por volta de 1550, estabelecendo regras operatórias, que muitos matemáticos da época desconfiavam admitindo-as como apenas artifício de cálculo, sem uma existência efetiva [14].

Ainda sem o termo específico de "*Álgebra*", o fato de encontrar a solução de problemas práticos por meio da determinação de um número incógnito foi de interesse geral para todos os povos há mais de 3500 anos. A Álgebra, durante o seu desenvolvimento, foi dividida como *retórica* e *sincopada*. No primeiro momento a Álgebra, com falta de simbologia, se utilizava de regras aritméticas estereotipadas. Durante o processo de transição até a Álgebra atual caracterizou-se a Álgebra sincopada que apresentava o uso de alguns símbolos específicos e abreviações.

O papiro de Moscou, que foi encontrado nessa mesma cidade (daí o nome), escrito por volta de 1850 a.C., apresenta uma coleção de vinte e cinco problemas práticos e o papiro Rhind, cujo nome remete numa homenagem ao antiquário escocês H. Rhind, escrito por volta de 1650 a.C., consta de oitenta e cinco problemas na maioria práticos e outros considerados recreativos. De forma geral, os egípcios não estabeleceram distinção entre problemas aritméticos, geométricos ou algébricos e praticamente desenvolveram a matemática em função da possibilidade em aplicações no cotidiano.

Na região da Mesopotâmia, que corresponde em sua maior parte no atual Iraque e Kuwait, os babilônios usavam plaquetas de argila para registrar suas informações. Quatrocentas, das quinhentas mil já encontradas, compõem-se de tabelas e listas de problemas envolvendo principalmente o que é chamado hoje de Aritmética, Geometria, Álgebra e Matemática Financeira. Elas pertencem, em geral, ao período em torno do ano de 2000 a.C. [8].

As civilizações, que se desenvolveram na China ao longo dos rios Amarelo e Yang - Tsé, têm um escasso registro favorecido pelo material de escrita ter sido de bambu e da ocorrência de queima de livros por ordem de um imperador. As duas principais fontes de informações acerca da matemática chinesa são: Zhoubi Suanjing e Jiuzhang Suanshu. O primeiro com a obra *A Aritmética Clássica do Gnômon e os Caminhos Circulares do Céu* e, o segundo com *As Nove Seções da Arte da Matemática* no qual compõe-se de duzentos e quarenta e seis problemas práticos sobre agrimensura, porcentagem e proporção, sociedade e regra de três, volumes, regra de falsa posição, sistemas de equações lineares envolvendo operações com o que hoje chamaríamos de matrizes e o teorema de Pitágoras. Conforme [8], depois que a matemática grega começou a entrar em declínio, a matemática chinesa continuou a florescer, creditando-se a ela várias contribuições que o ocidente só redescobriria séculos depois, como por exemplo o

Teorema do Binômio, o Método de Horner para a determinação numérica das raízes de uma equação algébrica e o Teorema Chinês dos Restos.

Euclides, em sua obra *Os Elementos*, datado de 300 a.C., e principalmente Diofanto de Alexandria (provavelmente século III d.C.) foram os personagens de destaque da matemática grega que desenvolveram trabalhos que se relacionam com as equações algébricas.

A matemática indiana se desenvolveu na região que corresponde ao atual Paquistão. Algumas das contribuições abrangem o atual sistema numérico indo-arábico e a introdução dos números negativos para indicar débitos, com destaque a obra do matemático e astrônomo Brahmagupta (aproximadamente do ano 628 d.C.). Brahmagupta levantou o questionamento da raiz quadrada de um número negativo, mas descartou a possibilidade de tal existência. As equações algébricas quadráticas também têm seu destaque na Índia através dos trabalhos dos matemáticos Ãryabhata (476 d.C.), Bhaskara I (século VI) e Bhaskara II (século XII). Segundo [8], os trabalhos imediatamente posteriores a Bhaskara I, sobre o desenvolvimento das equações quadráticas, estão relacionados à matemática árabe [8].

Na civilização árabe, inicialmente, reunia-se os intelectuais estrangeiros para trabalhar em seus centros culturais, ensinando, traduzindo obras clássicas para o árabe e contribuindo com sua própria produção científica. O influente algebrista al-Khwarizmi foi o primeiro matemático árabe a escrever a resolução de problemas no que hoje conhecemos por redução de termos semelhantes em membros opostos de uma mesma equação. A atual palavra *Álgebra* é uma variante de *al-jabr* que aparece no título da mais influente obra de al-Khwarizmi: *Hisab al-jabr w'al Muqabalah* (Ciência da Transposição e do Cancelamento, com base nas traduções usuais). Outro algebrista árabe foi Omar Khayyam que, em sua obra *Sobre as demonstrações de problemas de al-jabr e muqabala*, trata de equações de primeiro e segundo graus, aritmética e geometricamente da resolução das equações cúbicas [8].

A Europa, na Idade Média, tem o matemático mais talentoso Leonardo Pisa (1170 - 1250), também conhecido por Fibonacci, que em sua publicação *Liber abaci* (Livro do ábaco) desenvolve um tratamento sistemático das equações lineares e quadráticas e resolução de algumas equações cúbicas. Ele não acreditava numa solução algébrica geral e as raízes negativas e imaginárias eram desprezadas [8].

A Europa, no Renascimento, com o advento da imprensa (século XV), vivenciou a facilidade na disseminação do saber científico de um modo geral. Em relação às contribuições à matemática, a área que mais se destacou foi a da Álgebra cujo objetivo era basicamente o estudo das equações, ou ainda, a busca pura e simples da quantidade incógnita das equações. Neste período, os algebristas defrontaram com dois entraves: a falta de uma simbologia adequada e uniforme e a falta de qualquer fundamentação dos sistemas numéricos, até porque não havia sido esclarecida a natureza dos números negativos, irracionais e complexos. Lucas Pacioli, em sua obra *Summa de arithmetica,*

geometrica, proportioni et proportionalita (Suma de aritmética, geometria, proporções e proporcionalidade), em 1494, reuniu, de maneira bem feita, várias fontes mas, sem diferença relevante da obra *Liber abaci* de Fibonacci. Na seção que se refere a Álgebra, Pacioli trata da resolução de equações lineares e quadráticas por meio de regras verbais aplicadas a exemplos numéricos. Nessa época também aparecem Niccolo Fontana, apelidado de Tartaglia, e Gerônimo Cardano no desenvolvimento da Fórmula (3.1), que será apresentada no Capítulo 3, para a resolução de equações cúbicas da forma $x^3 + mx = n$ [8].

Nesse período a resolução das equações cúbicas e quárticas foi a mais importante contribuição à Álgebra desde o tempo dos babilônios, ainda mais por ter levantado questões como: Qual o papel das raízes quadradas de números negativos? E como lidar com elas? As equações de grau maior ou igual a cinco poderiam ser resolvidas com os mesmos processos até então conhecidos?

Nessa perspectiva, iniciamos nosso estudo apresentando, no Capítulo 2, uma breve revisão de conceitos importantes na compreensão do presente trabalho; no Capítulo 3 tem-se uma abordagem da motivação da construção do conjunto dos números complexos e introdução da raiz n-ésima da unidade; no Capítulo 4 a resolução das equações algébricas e sua contribuição no estudo da raiz n-ésima da unidade; no Capítulo 5 uma breve abordagem do Teorema de Dirichlet, cuja demonstração foi adaptada por nós, para contextualizar uma aplicação da raiz n-ésima da unidade; no Capítulo 6 apresentamos como reticulados podem ser construídos através de raízes n-ésimas da unidade e por fim, no Capítulo 7, apresentamos o levantamento de algumas contribuições já realizadas para a demonstração do Último Teorema de Fermat e uma consideração sobre a raiz n-ésima da unidade nesse estudo.

2 Preliminares

Neste capítulo destacamos alguns conceitos que consideramos básicos para o entendimento do trabalho. As principais referências utilizadas para o desenvolvimento deste capítulo foram [8], [12] e [23].

2.1 Congruência

Apresentamos propriedades elementares sobre divisibilidade no conjunto dos inteiros, o importantíssimo *Algoritmo da Divisão*, assim como o conceito de congruência. Estes possibilitarão o estudo de dois resultados importantes em nosso trabalho: o *Pequeno Teorema de Fermat* (Teorema (2.2)) e o *Lema de Gauss* (Teorema (2.5)).

Se a e b são inteiros dizemos que a divide b (denotando por $a|b$) se existir um único inteiro c tal que $b = ac$. A importância da unicidade de c se evidencia no exemplo a seguir.

Exemplo 2.1. Mostremos que 0 não divide um inteiro a qualquer. De fato, suponhamos por absurdo, $0|a$, então existe um único c tal que $a = 0 \cdot c$. Se $a = 0$, a igualdade anterior é verificada para qualquer inteiro c, e isto contraria a unicidade de c. Caso $a \neq 0$, a igualdade não é verificada, ou seja, não existe c, inteiro, satisfazendo $a = 0 \cdot c$.

Teorema 2.1 (Algoritmo da divisão)**.** *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r, \text{ com } 0 \leq r < b \ (r = 0 \Leftrightarrow b|a)$$

(q é chamado de quociente e r de resto da divisão de a por b).

Definição 2.1. *O **máximo divisor comum** de dois inteiros a e b (a ou b diferente de zero), denotado por $mdc(a, b)$, é o maior inteiro que divide a e b.*

Definição 2.2. *Um inteiro n ($n > 1$) possuindo somente dois divisores positivos, n e 1, é chamado **primo**. Se $n > 1$ não é primo dizemos que n é **composto**.*

Podemos ainda ter o caso de dois ou mais inteiros possuírem apenas o 1 como divisor comum, e nesse caso tais inteiros são **relativamente primos**, ou ainda, **primos entre si**.

O próximo exemplo será usado na demonstração do Teorema (2.2).

Exemplo 2.2. Mostremos que se p é primo vale $mdc((p-1)!, p) = 1$.

Consideremos os inteiros $n_i, n_j \in \{1, 2, \cdots, p-1\}$, $1 \leq i, j \leq p-1$. Logo, $n_i < p$ assim como, $n_j < p$. Pela hipótese segue $mdc(n_i, p) = 1$ e $mdc(n_j, p) = 1$, ou ainda, $p \nmid n_i$ e $p \nmid n_j$ o que implica $p \nmid n_i n_j$. Daí $mdc(n_i n_j, p) = 1$. Considerando outro n_k, $1 \leq n_k \leq p-1$, podemos pelos mesmos argumentos concluir que $mdc(n_i n_j n_k, p) = 1$. De maneira análoga, repetindo o raciocínio, concluímos que $mdc(1.2.\cdots.p-1, p) = 1$, ou seja, $mdc((p-1)!, p) = 1$.

Definição 2.3. *Se a e b são inteiros dizemos que a é **congruente** a b módulo m $(m > 0)$ se $m|(a-b)$. Denotamos isto por $a \equiv b(mod\ m)$. Se $m \nmid (a-b)$ dizemos que a é **incongruente** a b módulo m e denotamos $a \not\equiv b(mod\ m)$.*

Exemplo 2.3. $11 \equiv 3(mod\ 2)$, pois $2|(11-3)$. Como $5 \nmid 6$ e $6 = 17 - 11$, temos que $17 \not\equiv 11(mod\ 5)$.

Proposição 2.1 ([23], p.32)**.** *Se a e b são inteiros, temos que $a \equiv b(mod\ n)$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração. Se $a \equiv b(mod\ m)$, então $m|(a-b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial, pois da existência de um k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m|(a-b)$, isto é, $a \equiv b(mod\ m)$. □

Definição 2.4. *Se h e k são dois inteiros com $h \equiv k(mod\ m)$, dizemos que k é um **resíduo** de h módulo m.*

Definição 2.5. *O conjunto dos inteiros $r_1, r_2, \cdots, r_s$ é um **sistema completo de resíduos** módulo m se*

1. *$r_i \not\equiv r_j(mod\ m)$ para $i \neq j$,*
2. *para todo inteiro n existe um r_i tal que $n \equiv r_i(mod\ m)$.*

Exemplo 2.4. $\{0, 1, 2, \cdots, m-1\}$ é um sistema completo de resíduos módulo m.

Definição 2.6. *Para p um primo ímpar e a um inteiro não divisível por p, definimos o **Símbolo de Legendre** $\left(\frac{a}{p}\right)$ por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } x^2 \equiv a(mod\, p) \text{ possui solução} \\ -1, & \text{se } x^2 \equiv a(mod\, p) \text{ não possui solução.} \end{cases}$$

*Quando $x^2 \equiv a\,(mod\, p)$ possui solução, dizemos que a **é um resíduo quadrático de** p. Caso contrário, a **não é um resíduo quadrático de** p.*

Proposição 2.2 ([23], p.35). *Se a, b, k e m são inteiros com $k > 0$ e $a \equiv b(mod\ m)$, então $a^k \equiv b^k(mod\ m)$.*

Demonstração. O resultado segue, imediatamente, da identidade:

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + ... + ab^{k-2} + b^{k-1}).$$

□

Teorema 2.2 (Pequeno Teorema de Fermat, [23], p.41). *Seja p primo. Se $p \nmid a$ então $a^{p-1} \equiv 1(mod\ p)$.*

Demonstração. Sabemos, pela Definição 2.5, que o conjunto formado pelos p números $\{0, 1, 2, ..., p-1\}$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, ..., p-1\}$. Vamos agora, considerar os números $a, 2a, 3a, ..., (p-1)a$. Da hipótese $mdc(a, p) = 1$, e como nenhum destes números ia $(1 \leq i \leq p-1)$ é divisível por p, segue que nenhum destes números é congruente a zero módulo p.

Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak(modp)$ implica $j \equiv k(mod\ p)$ e, isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, ..., p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a)...(p-1)a \equiv 1 \cdot 2 \cdot 3...(p-1)(mod\ p)$$

ou seja, $a^{p-1}(p-1)! \equiv (p-1)!(mod\ p)$. Mas, como $mdc((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1(mod\ p),$$

o que conclui a demonstração. □

Teorema 2.3 (Wilson, [23], p.39). *Se p é primo, então $(p-1)! \equiv -1(mod\ p)$.*

Demonstração. O Teorema é verdadeiro para o caso $p = 2$, pois

$$(2-1)! = 1! = 1 \equiv -1(mod\ 2).$$

Vamos agora, supor $p \geq 3$. A congruência $ax \equiv 1(mod\ p)$ apresenta uma única solução para todo a no conjunto $\{1, 2, 3, \cdots, p-1\}$ (ver [23], p.37) e, como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, \cdots, p-2$ em $\frac{p-3}{2}$ pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos $2.3.4.\cdots.(p-2) \equiv 1(mod\ p)$. Multiplicando ambos os lados desta congruência por $p-1$, obtemos

$$2.3.4.\cdots.(p-2).(p-1) \equiv (p-1)(mod\ p).$$

Então, $(p-1)! \equiv -1(mod\ p)$ já que $p-1 \equiv -1(mod\ p)$. □

Teorema 2.4 (Critério de Euler, [23], p.98)**.** *Se p for um primo ímpar e a um inteiro não divisível por p, então:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p)\,.$$

Demonstração. Vamos supor, primeiramente, que $\left(\frac{a}{p}\right) = 1$, ou seja, que a congruência $x^2 \equiv a(mod\, p)$ tem solução. Seja y uma solução. Do fato de $mdc(a,p) = 1$ e $p|(y^2 - a)$ concluímos que $mdc(y,p) = 1$. Logo, pelo *Pequeno Teorema de Fermat*, $y^{p-1} \equiv 1(mod\, p)$ e, portanto,

$$a^{\frac{(p-1)}{2}} \equiv (y^2)^{\frac{(p-1)}{2}} = y^{p-1} \equiv 1(mod\, p)$$

o que prova o Teorema para o caso $\left(\frac{a}{p}\right) = 1$.

Consideremos, agora, o caso $\left(\frac{a}{p}\right) = -1$. Já vimos, na primeira parte, que se a for um resíduo quadrático logo $a^{\frac{(p-1)}{2}} \equiv 1(mod\, p)$. Pelo Teorema de Lagrange (ver em [23], p. 93) a congruência $f(x) = x^{\frac{(p-1)}{2}} - 1 \equiv 0(mod\, p)$ possui no máximo $\frac{(p-1)}{2}$ soluções incongruentes módulo p. Mas do fato de existirem $\frac{(p-1)}{2}$ resíduos quadráticos, e de termos $a^{\frac{(p-1)}{2}} \equiv 1(mod\, p)$ para todo resíduo quadrático, concluímos que todos eles são soluções de $f(x) \equiv 0(mod\, p)$. Isto nos garante que a congruência $f(x) \equiv 0(mod\, p)$ possui exatamente $\frac{(p-1)}{2}$ raízes e que, portanto, se a não for resíduo quadrático, isto é, $\left(\frac{a}{p}\right) = -1$, então $a^{\frac{(p-1)}{2}} \not\equiv 1(mod\, p)$. Mas, como

$$a^{p-1} - 1 = (a^{\frac{(p-1)}{2}} - 1)(a^{\frac{(p-1)}{2}} + 1)$$

e

$$a^{p-1} - 1 \equiv 0(mod\, p), \text{ para } mdc(p,a) = 1,$$

concluímos que $a^{\frac{(p-1)}{2}} \equiv \pm 1(mod\, p)$.

Logo, caso $\left(\frac{a}{p}\right) = -1$ deveremos ter $a^{\frac{(p-1)}{2}} \equiv -1(mod\, p)$, ou seja,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}}(mod\, p),$$

o que conclui a demonstração. □

Teorema 2.5 (Lema de Gauss, [23], p.103)**.** *Sejam p um primo ímpar e a um inteiro não divisível por p. Consideremos os menores resíduos positivos dos inteiros*

$$a, 2a, 3a, ..., \left(\frac{p-1}{2}\right) a. \tag{2.1}$$

Se r for o número destes resíduos que são maiores do que $\frac{p}{2}$, então,

$$\left(\frac{a}{p}\right) = (-1)^r.$$

Demonstração. Consideremos os menores resíduos positivos de $1a, 2a, 3a, \cdots, \left(\frac{p-1}{2}\right)a$ módulo p. É claro que estes resíduos são todos menores do que p. Sejam $a_1, a_2, \cdots, a_s$ os resíduos que são menores do que $\frac{p}{2}$ e $b_1, b_2, b_3, \cdots, b_r$ os que são maiores do que $\frac{p}{2}$. É claro que se multiplicarmos, membro a membro, todas as $\frac{p-1}{2}$ congruências de onde obtivemos os resíduos a_i e b_i acima teremos:

$$1a \cdot 2a \cdot 3a \cdot \cdots \cdot \tfrac{p-1}{2}a \equiv a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r (mod\ p)$$

ou seja,

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r (mod\ p). \tag{2.2}$$

Como os números $b_1, b_2, \cdots, b_r$ são maiores do que $\frac{p}{2}$ e menores do que p, os números $p - b_1, p - b_2, p - b_3, \cdots, p - b_r$ são todos menores do que $\frac{p}{2}$. Desejamos mostrar que os números $a_1, a_2, \cdots, a_s, p - b_1, p - b_2, p - b_3, \cdots, p - b_r$ são todos incongruentes módulo p. Isto será suficiente para mostrar que eles são, a menos da ordem, os números $1, 2, 3, \cdots, \frac{p-1}{2}$, uma vez que $r + s = \frac{p-1}{2}$. Se tivéssemos dois $a_i's$ ou dois $b_i's$ congruentes módulo p, teríamos dois elementos do conjunto $\{1a, 2a, \cdots, \frac{p-1}{2}a\}$ congruentes módulo p o que é impossível, pois $mdc(a, p) = 1$ e os números $1, 2, \cdots, \frac{p-1}{2}$ são todos menores que p. Nenhum a_i pode ser congruente com $p - b_j$, pois neste caso teríamos $a_i \equiv -b_j$ o que, após o cancelamento de a (a_i e b_i são, ambos, congruentes a múltiplos de a), em ambos os membros, nos daria uma congruência do tipo $n \equiv -m(mod\ p)$ com n e m elementos do conjunto $\{1, 2, \cdots, \frac{p-1}{2}\}$ o que é impossível. Com isto, concluímos que os números $a_1, a_2, \cdots, a_s, p - b_1, p - b_2, p - b_3, \cdots, p - b_r$ são, a menos de ordem, os números $1, 2, 3, \cdots, \frac{p-1}{2}$.

Portanto,

$$a_1 a_2 \cdots a_s (p - b_1)(p - b_2)(p - b_3) \cdots (p - b_r) \equiv 1 \cdot 2 \cdot 3 \cdots \tfrac{p-1}{2} (mod\ p)$$

ou seja,

$$a_1 a_2 \cdots a_s (-1)^r b_1 b_2 b_3 \cdots b_r \equiv \left(\tfrac{p-1}{2}\right)! (mod\ p)$$

isto é,

$$(-1)^r a_1 a_2 \cdots a_s b_1 b_2 b_3 \cdots b_r \equiv \left(\tfrac{p-1}{2}\right)! (mod\ p).$$

Utilizando-se a congruência 2.2 temos,

$$(-1)^r a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \equiv \left(\tfrac{p-1}{2}\right)! (mod\ p)$$

e, como, $mdc\left(\left(\frac{p-1}{2}\right), p\right) = 1$, obtemos,

$$(-1)^r a^{\frac{p-1}{2}} \equiv 1 (mod\ p).$$

Agora, se utilizarmos o Critério de Euler, após multiplicação de ambos os membros por $(-1)^r$ teremos,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^r (mod\ p) \text{ donde } \left(\frac{a}{p}\right) = (-1)^r.$$

□

2.1.1 Anéis e Corpos

Os conceitos básicos de *Anel* e *Corpo* é de grande relevância nos resultados de nosso trabalho. Para isso, destacamos os importantes resultados: anéis dos inteiros módulo n, anéis de polinômios e o corpo dos números complexos.

Definição 2.7. *Um* ***anel*** *ou* ***anel comutativo*** $(A, +, \cdot)$ *é um conjunto A com pelo menos dois elementos, munido de uma operação denotada por $+$ (chamada adição) e de uma operação denotada por $\cdot$ (chamada multiplicação) que satisfazem as propriedades associativa, comutativa, existência do elemento neutro aditivo (denotado por 0) e multiplicativo (denotado por 1), existência de elemento inverso com respeito a adição e a distributiva relativamente à multiplicação. (Para detalhes consultar [12], p. 34).*

Definição 2.8. *Um anel $(A, +, \cdot)$ é chamado* ***domínio de integridade*** *se ele não possui divisores de zero, isto é,*

$$\forall\ x, y \in A \setminus \{0\},\ x \cdot y \neq 0.$$

Definição 2.9. *Um domínio de integridade $(\mathbb{K}, +, \cdot)$ é chamado* ***corpo*** *se ele satisfaz a seguinte condição:*

$$\forall\ x \in \mathbb{K} \setminus \{0\},\ \exists\ y \in \mathbb{K} \text{ tal que } x \cdot y = 1.$$

Exemplo 2.5. $(\mathbb{Z}, +, \cdot)$ é um domínio e $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ são corpos, onde $+$ e $\cdot$ representam as operações usuais de adição e multiplicação, respectivamente.

Definição 2.10. *Seja A um anel. Suponhamos que, para algum $n > 0$ e para qualquer $a \in A$, verifica-se a igualdade $n.a = 0$ (zero do anel). Então existe um menor inteiro estritamente positivo r tal que $r.a = 0$, qualquer que seja $a \in A$. Esse inteiro r é chamado* ***característica*** *do anel A. Se, ao contrário, o anel A possui pelo menos um elemento tal que $n.a \neq 0$, qualquer que seja o inteiro estritamente positivo n, então se diz que a* ***característica*** *do anel é 0.*

Exemplo 2.6. Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm característica 0, pois se $m \neq 0$, então $m.1 = m$ e, portanto, $m.1 \neq 0$.

Exemplo 2.7 (Anel dos inteiros módulo n)**.** Seja n um inteiro positivo. Sobre $\mathbb{Z}$, definimos a relação $\equiv_n$ da maneira que segue: para $a, b \in \mathbb{Z}$,

$$a \equiv_n b \Leftrightarrow a - b \text{ é um múltiplo de } n.$$

Também podemos escrever $a \equiv_n b$ como $a \equiv b(mod\ n)$.
É imediato verificar:

- $a \equiv_n a$ (propriedade reflexiva);
- $a \equiv_n b \Rightarrow b \equiv_n a$ (propriedade simétrica),
- $a \equiv_n b$, $b \equiv_n c \Rightarrow a \equiv_n c$ (propriedade transitiva).

Se $a \in \mathbb{Z}$, então, por definição, sua classe de equivalência módulo o inteiro n, consiste no conjunto $\{b \in \mathbb{Z}; b \equiv_n a\}$, isto é, no subconjunto $\{a + kn; k \in \mathbb{Z}\}$; ela será denotada por $\bar{a}$ ou $a + n\mathbb{Z}$.

Considerando $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ o conjunto das classes de equivalência módulo n, definimos duas operações:

$$\begin{array}{ccc} \oplus : \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ (\bar{x}, \bar{y}) & \longmapsto & \overline{x+y} \end{array}$$

$$\begin{array}{ccc} \odot : \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ (\bar{x}, \bar{y}) & \longmapsto & \overline{x \cdot y} \end{array}$$

As operações $\oplus$ e $\odot$ estão bem definidas, isto é, os resultados não dependem da escolha das representações das classes de equivalência. De fato, se $\overline{a} = \overline{a'} \in \mathbb{Z}_n$ e $\overline{b} = \overline{b'} \in \mathbb{Z}_n$ então

$$a \equiv a'(mod\ n) \text{ e } b \equiv b'(mod\ n)$$

portanto, usando as propriedades de congruência:

$$a + b \equiv a' + b'(mod\ n) \text{ e } a.b \equiv a'.b'(mod\ n).$$

Consequentemente, $\overline{a+b} = \overline{a'+b'}$ e $\overline{a.b} = \overline{a'.b'}$. Além disso, como $\mathbb{Z}_n$, com as operações $\oplus$ e $\odot$, satisfaz as propriedades da Definição (2.7), segue que $(\mathbb{Z}_n, \oplus, \odot)$ é um anel denominado o *anel dos inteiros módulo n*.

Exemplo 2.8 (Anéis de polinômios)**.** Seja $(A, +, \cdot)$ um anel. Um *polinômio numa variável sobre A* é uma sequência $(a_0, a_1, ..., a_n, ...)$, onde $a_i \in A$ para todo índice e $a_i \neq 0$ somente para um número finito de índices.

Seja $\mathbf{A} = \{\text{polinômios numa variável sobre A}\}$. No conjunto $\mathbf{A}$, definimos as operações:

$$\begin{array}{ccc} \oplus : \mathbf{A} \times \mathbf{A} & \longrightarrow & \mathbf{A} \\ ((a_0, a_1, ...), (b_0, b_1, ...)) & \longmapsto & (a_0 + b_0, a_1 + b_1, ...) \end{array}$$

$$\begin{array}{ccc} \otimes : \mathbf{A} \times \mathbf{A} & \longrightarrow & \mathbf{A} \\ ((a_0, a_1, ...), (b_0, b_1, ...)) & \longmapsto & (c_0, c_1, ...) \end{array}$$

onde

$c_0 = a_0 b_0$
$c_1 = a_0 b_1 + a_1 b_0$
$\vdots$
$c_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + ... + a_{n-1} b_1 + a_n b_0$
$\vdots$

$\mathbf{A}$ com as operações $\oplus$ e $\otimes$ satisfaz as propriedades da Definição (2.7). Portanto, $(\mathbf{A}, \oplus, \otimes)$ é um anel.

Para facilitar usaremos o símbolo x para designar o elemento $(0, 1, 0, \cdots)$. Também no lugar de $(a_i, 0, 0, \cdots)$, vamos escrever a_i. Finalmente, no lugar de escrever $\oplus$ e $\otimes$, vamos escrever $+$ e $\cdot$. Com essas convenções, o elemento $(a_0, a_1, \cdots, a_n, 0, \cdots)$ é igual a soma $a_0 + a_1 x + ... + a_n x^n$, onde $a_i x^i$ designa $a_i \cdot x^i$. Logo,

$$\mathbf{A} = \left\{ \sum_{i=0}^{n} a_i x^i | n \in \mathbb{N} \text{ e } a_i \in A \right\}.$$

Portanto $(\mathbf{A}, \oplus, \otimes)$, que denotaremos por $A[x]$, é o *anel de polinômios numa variável* sobre A.

Se $p(x) = a_0 + a_1 x + ... + a_n x^n \in A[x]$, com $a_n \neq 0$, dizemos que n é o **grau do polinômio** $p(x)$, e nesse caso indicamos por $\partial p(x) = n$ e, se ainda $a_n = 1$, dizemos que $p(x)$ é um polinômio **mônico**.

Proposição 2.3 (Algoritmo da divisão, [12], p.66)**.** *Sejam $(A, +, \cdot)$ um anel comutativo e com unidade e $f(x), g(x) \in A[x]$, com $g(x) \neq 0$ e com coeficiente dominante inversível em A, então existem $q(x), r(x) \in A[x]$ tais que*

$$f(x) = g(x)q(x) + r(x),$$

com $\partial r(x) \leq \partial g(x)$ ou $r(x) = 0$.

Exemplo 2.9. Vejamos como o algoritmo da divisão se comporta num exemplo particular. Considere o problema de dividir $f(x) = x^4 - 2x^2 + 5x + 7$ por $g(x) = 3x^2 + 1$ em $\mathbb{Q}[x]$.

x^4	$-2x^2$	$+5x$	$+7$	$3x^2 + 1$
$-x^4$	$-\frac{1}{3}x^2$			$\frac{1}{3}x^2$
	$-\frac{7}{3}x^2$	$+5x$	$+7$	$\frac{1}{3}x^2 - \frac{7}{9}$
	$\frac{7}{3}x^2$		$+\frac{7}{9}$	
		$5x$	$+\frac{70}{9}$	

Portanto, $r(x) = 5x + \frac{70}{9}$ e $q(x) = \frac{1}{3}x^2 - \frac{7}{9}$.

Definição 2.11. *Seja A um domínio de integridade. Dizemos que o polinômio não constante $p(x)$ é irredutível em $A[x]$ (ou irredutível sobre A) se é impossível expressar $p(x)$ como um produto $a(x)b(x)$ em $A[x]$ cujos graus são ambos maiores ou iguais a 1.*

Exemplo 2.10. Veja que $p(x) = x^2 + 1$ é irredutível sobre $\mathbb{R}$, pois se fosse possível escrever $x^2+1 = (ax+b)(cx+d)$ com $ax+b$ e $cx+d$ de grau 1 e com coeficientes reais, então x^2+1 teria duas raízes, o que não é o caso, pois as raízes de $p(x)$ são $\pm i$ que não pertencem a $\mathbb{R}$. Por outro lado, x^2+1 não é irredutível em $\mathbb{C}$, pois $x^2+1 = (x+i)(x-i)$.

2.1.2 Módulos

Abordamos aqui as definições de módulos e submódulos que serão necessárias no contexto de reticulados, tema que será apresentado no Capítulo 6.

Definição 2.12. *Seja A um anel com unidade. Diz-se que um conjunto não vazio M é um* ***módulo*** *à esquerda sobre A (ou um A-***módulo** *à esquerda), se M é um grupo abeliano em relação a uma operação, que indicaremos por $+$, e está definida uma lei de composição externa que a cada par $(a, m) \in A \times M$ associa um elemento $am \in M$ e tal que, para todos $a, b \in A$ e todos $m_1, m_2 \in M$, verifica:*
i) $a(m_1 + m_2) = am_1 + am_2$;
ii) $(a + b)m_1 = am_1 + bm_1$;
iii) $(ab)m_1 = a(bm_1)$,
iv) $1m_1 = m_1$.

Exemplo 2.11. Exemplos:

1. Todo espaço vetorial sobre um corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo;
2. Todo grupo abeliano G pode ser considerado como um módulo sobre o anel $\mathbb{Z}$, dos números inteiros, definindo o produto de um inteiro n por um elemento $g \in G$ por:
   - $ng = g + \cdots + g$, (n vezes), se $n > 0$
   - $ng = (-g) + \cdots + (-g)$, ($|n|$ vezes), se $n < 0$
   - $0.g = 0$,
3. Todo anel pode ser considerado como um módulo sobre si mesmo.

Definição 2.13. *Seja M um A-módulo. Um subconjunto $N \subset M$ não vazio é um* A-**submódulo** *de M se, com as operações herdadas de M, também é um A-módulo.*

Exemplo 2.12. Seja V um espaço vetorial sobre um corpo $\mathbb{K}$. Um subconjunto $S \subset V$ é um submódulo, se e somente se, S é um subespaço de V.

Exemplo 2.13. Seja G um grupo abeliano. Os $\mathbb{Z}$-submódulos de G são precisamente os seus subgrupos.

Um A-módulo M é dito **finitamente gerado** se $M = \sum_{i=1}^{n} Am_i$, para $\{m_1, \cdots, m_n\} \subset M$. Um conjunto de elementos $m_1, \cdots, m_s \in M$ são linearmente independentes (sobre A) se a igualdade $\sum_{j=1}^{s} a_j m_j = 0$, com $a_j \in A$, implicar que $a_1 = \cdots = a_s = 0$. Mas, se além disso, $m_1, \cdots, m_s$ formarem um sistema de geradores de M, então eles formam uma base de M. Um A-módulo que possui uma base é chamado de um A-**módulo livre**, e o número de elementos da base é chamado de **posto** de M.

2.1.3 Extensão de Corpos

Apresentamos aqui uma breve abordagem sobre extensões de corpos com algumas definições e resultados que serão necessários para um melhor entendimento da próxima seção.

Definição 2.14. *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos. A dimensão do $\mathbb{K}$-espaço vetorial $\mathbb{L}$ é chamada de* ***grau*** *da extensão e denotada por $[\mathbb{L} : \mathbb{K}]$.*

Seja $\mathbb{F} \subset \mathbb{L}$ uma extensão de corpos. Seja $\mathbb{K}$ um corpo intermediário, $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$, neste caso dizemos que temos uma torre de extensões. Tanto $\mathbb{F}$ quanto $\mathbb{K}$ têm uma estrutura de $\mathbb{L}$-espaço vetorial, mas podemos também considerar $\mathbb{F}$ como um espaço vetorial tendo $\mathbb{K}$ como escalares. Há uma relação entre os graus de todas estas extensões.

Teorema 2.6 (Multiplicatividade dos Graus)**.** *Sejam $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$ corpos tais que $[\mathbb{L} : \mathbb{K}] < \infty$ então $[\mathbb{L} : \mathbb{M}] < \infty$, $[\mathbb{M} : \mathbb{K}] < \infty$ e $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}]$.*

Demonstração. Como $[\mathbb{L} : \mathbb{K}] < \infty$ então existe uma base B de $\mathbb{L}$ sobre $\mathbb{K}$. Extraindo um subconjunto B' de B tal que B' é linearmente independente sobre $\mathbb{M}$ temos que B' é uma base de $\mathbb{L}$ sobre $\mathbb{M}$, e portanto $[\mathbb{L} : \mathbb{M}] < \infty$. Sendo $\mathbb{M}$ um sub espaço de $\mathbb{L}$ sobre $\mathbb{K}$, temos que $[\mathbb{M} : \mathbb{K}] < [\mathbb{L} : \mathbb{M}] < \infty$. Suponha que $[\mathbb{L} : \mathbb{M}] = m$ e $[\mathbb{M} : \mathbb{K}] = n$ e sejam $\{v_i\}_{\{1 \leq i \leq m\}}$ uma base de $\mathbb{L}$ sobre $\mathbb{M}$ e $\{w_j\}_{\{1 \leq j \leq n\}}$ uma base de $\mathbb{M}$ sobre $\mathbb{K}$. Mostraremos que $\{v_i w_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$.

De fato, se $\alpha \in \mathbb{L}$, existem $\alpha_i \in \mathbb{K}, i = 1, \cdots, m$ tais que $\alpha = \sum_{i=1}^{m} \alpha_i v_i$. Por hipótese, para todo i existe $\beta_{ij} \in \mathbb{M}$ tal que $\alpha_i = \sum_{j=1}^{n} \beta_{ij} w_j$.

Logo,

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

Portanto, $\{v_i w_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ gera $\mathbb{L}$ como $\mathbb{K}$- espaço vetorial.
Vejamos, agora, que $\{v_i w_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ é linearmente independente.
De fato,

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

Como $\{w_j\}$ é linearmente independente, temos que para j, $1 \leq j \leq n$

$$\sum_{i=1}^{m} \beta_{ij} v_i = 0.$$

Como $\{v_i\}$ é linearmente independente, temos que

$$\beta_{ij} = 0, , \quad 1 \leq i \leq m, 1 \leq j \leq n.$$

Portanto, $\{v_i w_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$.

□

É sugestivo utilizar diagramas para representar extensões de corpos. Assim, na situação do enunciado do Teorema 2.6 temos o diagrama abaixo, onde o grau de $\mathbb{K} \subset \mathbb{L}$ é $m.n$.

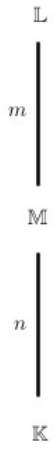


Figura 2.1: Diagrama.
Fonte: print screen do software Geogebra.

Definição 2.15. *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos. Um elemento $\alpha \in \mathbb{L}$ é chamado de* ***algébrico*** *sobre $\mathbb{K}$ se existe $f(x) \in K[x]\backslash\{0\}$ tal que $f(\alpha) = 0$. O polinômio mônico de menor grau $f(x)$ tal que $f(\alpha) = 0$ é chamado de* ***polinômio minimal*** *de α sobre $\mathbb{K}$ e o denotamos por $min_{\mathbb{K}}\alpha$. Se α não é algébrico sobre $\mathbb{K}$, então α é dito ser* ***transcendente*** *sobre $\mathbb{K}$.*

Exemplo 2.14. Considere $\alpha = i \in \mathbb{C}$ e $\mathbb{K} = \mathbb{R}$. Temos:

$$\alpha^2 = i^2 = -1 \Rightarrow \alpha^2 - 1 = 0.$$

Logo, $f(x) = x^2 - 1 \in \mathbb{R}[x]$ e $f(i) = 0$. Como $f(x)$ é irredutível sobre $\mathbb{R}$, segue que $f(x) = min_{\mathbb{R}}(i)$.

Definição 2.16. *Um* ***corpo de números*** $\mathbb{K}$ *é uma extensão finita de* $\mathbb{Q}$.

Denote por $\bar{N}$ o subcorpo de $\mathbb{C}$ consistindo de todos os números algébricos e por $\mathbb{A}$ o conjunto de todos os algébricos em $\bar{N}$. Um *corpo de números algébricos*, ou simplesmente, *corpo de números* é da forma

$$\mathbb{K} = \mathbb{Q}(\alpha_1, \cdots, \alpha_n) \subseteq \mathbb{C}, \text{ com } n \in \mathbb{N}, \alpha_j \in \bar{N}, 1 \leq i \leq n.$$

Definição 2.17. *Se* $\mathbb{K}$ *é um corpo de números algébricos, então* $\mathbb{K} \cap \mathbb{A}$ *é chamado o* ***anel dos inteiros algébricos*** *de* $\mathbb{K}$*, denotado por* $\mathcal{O}_{\mathbb{K}}$.

Temos que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{K} : \mathbb{Q}]$.

Definição 2.18. *Se* $\mathcal{O}_{\mathbb{K}}$ *é o anel dos inteiros de um corpo de números* $\mathbb{K}$*, uma base para* $\mathcal{O}_{\mathbb{K}}$ *sobre* $\mathbb{K}$*, ou simplesmente uma* $\mathbb{Z}$*-base para* $\mathcal{O}_{\mathbb{K}}$*, é chamada uma* ***base integral*** *para* $\mathcal{O}_{\mathbb{K}}$.

Exemplo 2.15. Se $\mathbb{K} = \mathbb{Q}(i)$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$ e $B = \{1, i\}$ é uma base integral para $\mathcal{O}_{\mathbb{K}}$.

Teorema 2.7. *[26] Se* $\mathbb{L} \supset \mathbb{K} \supset \mathbb{Q}$, $[\mathbb{L} : \mathbb{K}] < \infty$*, então existe* $\theta \in \mathbb{L}$ *tal que* $\mathbb{L} = \mathbb{K}(\theta)$*. O elemento* θ *é chamado* ***elemento primitivo****.*

Proposição 2.4. *[26] Seja* $\mathbb{K}$ *um corpo de números tal que* $\mathbb{L} = \mathbb{K}(\theta)$*, então* $[\mathbb{L} : \mathbb{K}] = \partial(min_{\mathbb{K}}\theta)$.

Exemplo 2.16. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{2} + \sqrt{5})$, então $[\mathbb{K} : \mathbb{Q}] = 4$, pois $min_{\mathbb{Q}}(\sqrt{2} + \sqrt{5}) = x^4 - 14x + 9$. De fato, se $\alpha = \sqrt{2} + \sqrt{5}$ então:

$$\begin{aligned} \alpha^2 &= 2 + 2\sqrt{2}\sqrt{5} + 5 \\ \alpha^2 &= 7 + 2\sqrt{2}\sqrt{5} \\ \alpha^2 - 7 &= 2\sqrt{2}\sqrt{5} \\ \alpha^4 - 14\alpha^2 + 49 &= 40 \\ 0 &= \alpha^4 - 14\alpha^2 + 9 \end{aligned}$$

Logo, $p(x) = x^4 - 14x + 9 = min_{\mathbb{Q}}(\alpha)$.

3 Os Números Complexos

Iniciamos o capítulo com um breve histórico sobre o surgimento da unidade imaginária i e posteriormente discutimos propriedades resultantes da definição do conjunto dos números complexos $\mathbb{C}$. As principais referências utilizadas para o desenvolvimento deste capítulo foram [2], [4], [11], [14] e [20].

3.1 Breve Histórico

Historicamente os números complexos foram introduzidos no estudo da solução geral de uma equação algébrica de grau dois com coeficientes reais [20]. Em meados do século XII, viveu na Índia um dos maiores matemáticos da época, conhecido como Bhaskara. Em seu tratado mais conhecido, chamado *Lilavati*, encontra-se uma série de estudos sobre equações lineares, quadráticas, progressões aritméticas e geométricas, entre outros assuntos matemáticos. A fórmula que permite a resolução de uma equação do segundo grau, $ax^2 + bx + c = 0$ ($a \neq 0$), foi batizada com o nome desse estudioso (na página 170 de [14] é citado o matemático hindu Shidhara, do século X, pelo mérito da fórmula resolvente da equação de segundo grau) e é dada por:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Obtemos, efetivamente, duas raízes quando o discriminante $b^2 - 4ac$ for positivo, e apenas uma raiz se ele for nulo. Quando o discriminante é negativo a fórmula acima não conduz a nenhuma raiz real.

Podemos resolver a equação do segundo grau, mesmo no caso em que $b^2 - 4ac < 0$, se operarmos com o símbolo $i = \sqrt{-1}$ como se fosse um número. Ele deve ter a propriedade de que $i^2 = -1$ e operar ao lado dos números reais com as mesmas propriedades destes números. Somos assim levados a introduzir os números complexos como sendo os números da forma $a + bi$.

Na verdade, a motivação maior para a aceitação dos números complexos ocorreu no século XVI quando os matemáticos descobriram a fórmula geral de resolução de equações do terceiro grau.

Resolver algebricamente uma equação de terceiro ou quarto grau pode ser considerado um dos feitos matemáticos mais extraordinários do século XVI. Existe uma polêmica em que Nicolo Fontana de Brescia (1499 - 1557), mais conhecido por Tartaglia, descobriu uma solução algébrica para a equação cúbica na forma $x^3 + px - q = 0$, na qual, mais tarde, Gerônimo Cardano (1501 - 1576) teria plagiado [11]. A solução é:

$$x = \sqrt[3]{\sqrt{(p/3)^3 + (q/2)^2} + q/2} - \sqrt[3]{\sqrt{(p/3)^3 + (q/2)^2} - q/2}. \tag{3.1}$$

Para exemplificar a dificuldade na época consideremos $x^3 = 15x + 4$. Quando aplicada em (3.1) tem-se o resultado:

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Cardano se referia às raízes quadradas de números negativos como "sofisticas" e que seu resultado era "tão sutil quanto inútil". Aparentemente, tratadas como uma anomalia, as raízes quadradas de números negativos foram denominadas pelos antigos algebristas por *casos irredutíveis* das equações cúbicas.

Deve-se a Leonhard Euler (1707 - 1783) a notação i para a unidade imaginária, $\sqrt{-1}$. Outra contribuição que é a de associar números complexos a pares ordenados de números reais foi registrada nos estudos de Caspar Wessel (1745 - 1818), Jean Robert Argand (1768 - 1822) e Carl Friedrich Gauss (1777 - 1855) [11].

Pelo *Teorema Fundamental da Álgebra* [18] segue um importante resultado envolvendo os *números complexos*: todo polinômio de grau $n \geq 1$ e com coeficientes complexos tem n raízes complexas. Assim, no presente trabalho iniciamos nosso estudo pelo conjunto dos números complexos a fim de calcularmos as raízes n-ésima da unidade.

3.2 Definições e Propriedades

Os números z da forma $a+bi$ são chamados de números complexos, onde $a, b \in \mathbb{R}$ e $i = \sqrt{-1}$, esta última denominada *unidade imaginária*. Denotaremos por $\mathbb{C}$ o conjunto dos números complexos. Dados os números complexos $z_1 = a_1 + b_1 i$ e $z_2 = a_2 + b_2 i$ definimos sua soma por

$$z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i \tag{3.2}$$

e seu produto por

$$z_1.z_2 = (a_1 + b_1 i).(a_2 + b_2 i) = (a_1.a_2 - b_1.b_2) + (a_1.b_2 + a_2.b_1)i \tag{3.3}$$

Exemplo 3.1. Consideremos os números complexos: $z_1 = 2 + 4i, z_2 = 5 - i, z_3 = 10$ e $z_4 = -\frac{1}{2}i$.

Pela definição de adição (3.2) e multiplicação (3.3) temos:

- $z_1 + z_2 = (2 + 4i) + (5 - i) = (2 + 5) + (4 + (-1))i = 7 + 3i$;

- $z_3 + z_4 = (10) + \left(-\frac{1}{2}i\right) = (10 + 0i) + \left(0 - \frac{1}{2}i\right) = (10 + 0) + \left(0 + \left(-\frac{1}{2}i\right)\right) = 10 - \frac{1}{2}i$;
- $z_1.z_2 = (2 + 4i).(5 - i) = (2.5 - 4.(-1)) + (2.(-1) + 4.5)i = 14 + 18i$,
- $z_2.z_4 = (5 - i).\left(-\frac{1}{2}i\right) = (5 - i).\left(0 - \frac{1}{2}i\right) = \left((5.0) - (-1).\left(-\frac{1}{2}\right)\right) + + \left(5.\left(-\frac{1}{2}\right) + (-1).0\right)i = -\frac{1}{2} - \frac{5}{2}i$.

As operações (3.2) e (3.3) gozam das seguintes propriedades:

(C. 1) Comutatividade: Se z_1 e $z_2 \in \mathbb{C}$ então $z_1 + z_2 = z_2 + z_1$ e $z_1.z_2 = z_2.z_1$;

(C. 2) Associatividade: Se z_1, z_2 e $z_3 \in \mathbb{C}$ então $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ e $(z_1.z_2).z_3 = z_1.(z_2.z_3)$;

(C. 3) Distributividade: Se z_1, z_2 e $z_3 \in \mathbb{C}$ então $z_1.(z_2 + z_3) = z_1.z_2 + z_1.z_3$;

(C. 4) Existência do zero: Existe um elemento $0 = 0 + 0i \in \mathbb{C}$ tal que $0 + z = z$ para todo $z \in \mathbb{C}$;

(C. 5) Existência da unidade: Existe um elemento $1 = 1 + 0i \in \mathbb{C}$ tal que $1.z = z$ para todo $z \in \mathbb{C}$;

(C. 6) Existência do inverso aditivo: Dado $z = a + bi \in \mathbb{C}$ existe um único $w = (-a) + (-b)i \in \mathbb{C}$ tal que $z + w = 0$. Notação: $w = -z$,

(C. 7) Existência do inverso multiplicativo: Dado $z = a+bi \in \mathbb{C}$, tal que $a \neq 0$ ou $b \neq 0$, existe $w = a\left(a^2 + b^2\right)^{-1} - b\left(a^2 + b^2\right)^{-1} i$ tal que $z.w = 1$. Notação: $w = z^{-1} = \frac{1}{z}$.

Dizemos então que $\mathbb{C}$ é um corpo com as operações (3.2) e (3.3). Um fato que devemos ter em mente é que o corpo dos reais está naturalmente mergulhado em $\mathbb{C}$ e para isto basta identificarmos um número real x com o complexo $x+0i$. Tendo em vista esta identificação, diremos que $\mathbb{R} \subset \mathbb{C}$. Observe que se $z = a+0i \in \mathbb{R}$ e $w = b+0i \in \mathbb{R}$ então $z + w$ e $z.w$ estão em $\mathbb{R}$. Portanto $\mathbb{R}$ é um subcorpo de $\mathbb{C}$, isto é, as operações (3.2) e (3.3) estendem as operações de soma e produto de números reais.

William Rowan Hamilton (1805 - 1865) durante o século XIX (um período de grandes contestações da álgebra conhecido como *a libertação da álgebra*) tratou os números complexos de forma elegante como um par ordenado de números reais. Podemos identificar o conjunto dos números complexos com o plano $\mathbb{R}^2 = \{(x, y)/x, y \in \mathbb{R}\}$ por meio do isomorfismo

$$\begin{array}{rcl} \varphi : \mathbb{R}^2 & \longrightarrow & \mathbb{C} \\ (x, y) & \longmapsto & x + yi \end{array}$$

Assim, podemos definir a soma e o produto de complexos $z_1 = (a_1, b_1)$ e $z_2 = (a_2, b_2)$, respectivamente:

$$z_1 + z_2 = (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \tag{3.4}$$

$$z_1.z_2 = (a_1, b_1).(a_2, b_2) = (a_1.a_2 - b_1.b_2, a_1.b_2 + a_2.b_1) \tag{3.5}$$

Podemos então representar geometricamente o conjunto dos números por um plano (Figura 3.1).

As conhecidas regras do paralelogramo para a soma e subtração de vetores se aplicam no caso de soma e subtração de números complexos (Figura 3.2).

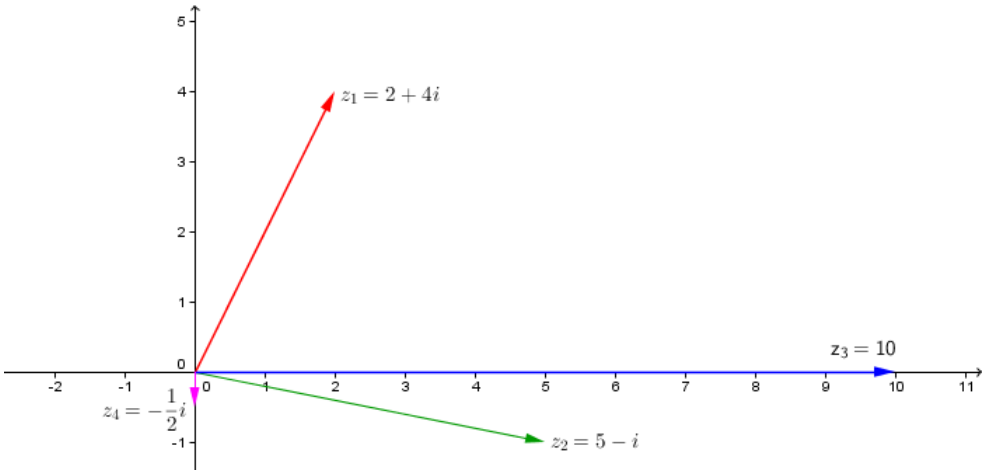


Figura 3.1: Representação geométrica dos números complexos z_1, z_2, z_3 e z_4.
Fonte: print screen do software Geogebra.

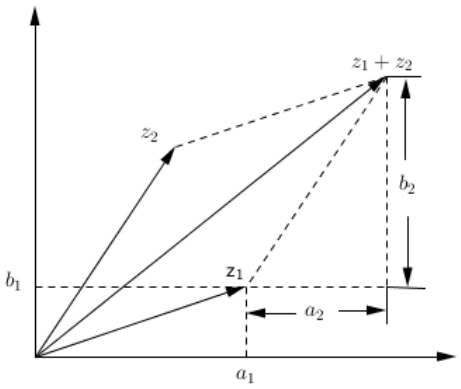


Figura 3.2: Representação geométrica da soma $z_1 + z_2$.
Fonte: print screen do software Geogebra.

Dado $z = x + yi \in \mathbb{C}$, definimos

$$Re(z) = x \text{ (parte real de } z)$$
$$Im(z) = y \text{ (parte imaginária de } z).$$

Assim, para todo $z \in \mathbb{C}$ temos $z = Re(z) + Im(z)i$.

Definimos o **módulo**, **valor absoluto** ou **norma** de um número complexo $z = x + yi$ como sendo o número não negativo $|z| = \sqrt{x^2 + y^2}$ (Figura 3.4). O **complexo conjugado** de $z = x + yi$ é definido como sendo $\overline{z} = x - yi$ (Figura 3.3).

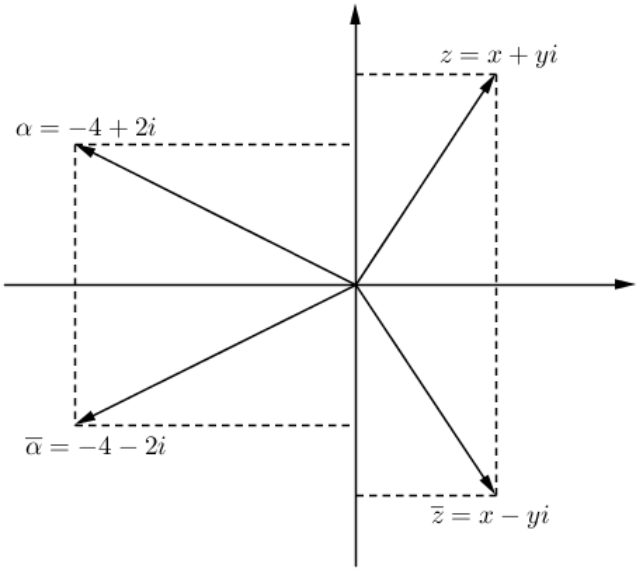


Figura 3.3: Conjugado de um número complexo.
Fonte: print screen do software Geogebra.

Em termos do módulo e do conjugado, temos:

$$z\overline{z} = (x + yi)(x - yi) = (x^2 + y^2) + (-xy + yx)i = x^2 + y^2$$

isto é, $z\overline{z} = |z|^2$.

O quociente $z = \frac{z_1}{z_2}$ de dois números complexos z_1 e z_2, $z_2 \neq 0$, é definido pela condição $z.z_2 = z_1$.

Para calcular o quociente basta multiplicar o numerador e o denominador pelo complexo conjugado do denominador.

Exemplo 3.2. Considere os números complexos $z_1 = -3+i$ e $z_2 = 1-2i$. Assim, $\frac{z_1}{z_2} = \frac{-3+i}{1-2i} = \frac{(-3+i).(1+2i)}{(1-2i).(1+2i)} = \frac{((-3).1 - 1.2) + ((-3).2 + 1.1)i}{(1.1 - (-2).2) + (1.2 + (-2).1)i} = \frac{-5-5i}{5} = -1 - i.$

Em geral, se $z_1 = x_1 + y_1 i$ e $z_2 = x_2 + y_2 i$,

$$\frac{z_1}{z_2} = \frac{z_1.\overline{z_2}}{z_2.\overline{z_2}} = \frac{x_1x_2 + y_1y_2 + (y_1x_2 - x_1y_2)i}{x_2^2 + y_2^2}.$$

Para $\forall z, w \in \mathbb{C}$, tem-se as seguintes propriedades:

1.) $|z| = |\overline{z}|$,

2.) $\overline{(z+w)} = \overline{z} + \overline{w}$,

3.) $\overline{z}.\overline{w} = \overline{zw}$,

4.) $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$, $w \neq 0$,

5.) $z^{-1} = \frac{\overline{z}}{|z|^2}$, $z \in \mathbb{C}$ - $\{0\}$,

6.) $Re(z) = \dfrac{z+\overline{z}}{2}$ e $Im(z) = \dfrac{z-\overline{z}}{2i}$,

7.) $|z+w|^2 = |z|^2 + |w|^2 + 2Re\,(z\overline{w})$.

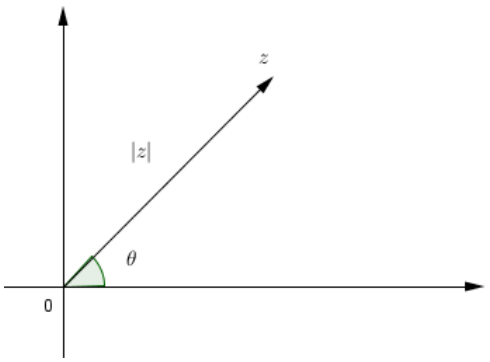


Figura 3.4: Representação geométrica da norma $|z|$.
Fonte: print screen do software Geogebra.

Consideremos agora um número complexo não nulo $z = x + iy$. Se $|z|$ é o comprimento do segmento de reta que liga 0 a z e θ é o ângulo que $|z|$ faz com o eixo dos x $(0 \leq \theta \leq 2\pi)$ (observe a figura (3.2)), podemos escrever

$$\cos\theta = \frac{x}{\sqrt{x^2+y^2}} = \frac{x}{|z|} \text{ e } \operatorname{sen}\theta = \frac{y}{\sqrt{x^2+y^2}} = \frac{y}{|z|}$$

e portanto

$$z = |z|\cos\theta + i|z|\operatorname{sen}\theta = |z|(\cos\theta + i\operatorname{sen}\theta). \tag{3.6}$$

A expressão (3.6) é chamada de **representação polar** do número complexo z. O número θ é chamado de **argumento** de z e denotaremos por $arg(z)$.

Podemos determinar θ de maneira única exigindo, por exemplo, que $0 \leq \theta < 2\pi$ ou que $-\pi < \theta \leq \pi$.

Exemplo 3.3. Seja $z_1 = 2 - 2i$, então $|z_1| = 2\sqrt{2}$ e $arg(z_1) = -\dfrac{\pi}{4} \pm 2n\pi$ $(n = 0, 1, 2, \cdots)$. Logo, uma forma polar desse número complexo é $z_1 = 2\sqrt{2}\left(\cos\left(-\dfrac{\pi}{4}\right) + i\operatorname{sen}\left(-\dfrac{\pi}{4}\right)\right)$.

Exemplo 3.4. Seja $z_2 = -i$, então $|z_2| = 1$ e $arg(z_2) = -\frac{\pi}{2} \pm 2n\pi$ $(n = 0, 1, 2, \cdots)$. Assim, uma forma polar desse complexo é $z_2 = \cos\left(-\frac{\pi}{2}\right) + i\,\mathrm{sen}\left(-\frac{\pi}{2}\right)$.

Também podemos considerar algum ponto z_0 que não seja a origem $(0, 0)$. A representação

$$z - z_0 = \rho(\cos\phi + i\,\mathrm{sen}\,\phi) \tag{3.7}$$

é a forma polar de $z - z_0$, onde $\rho = |z - z_0|$ e ϕ é o ângulo de inclinação do vetor $\overrightarrow{z - z_0}$.

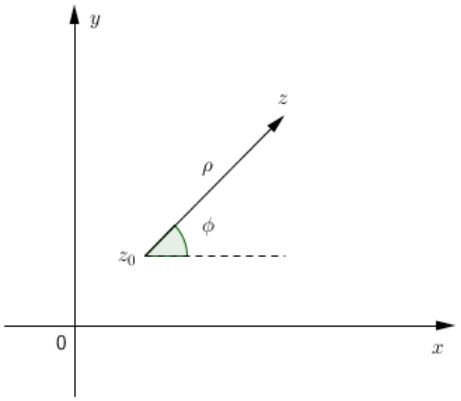


Figura 3.5: Representação geométrica de $z - z_0$.
Fonte: print screen do software Geogebra.

Para os números complexos

$$z_1 = r_1(\cos\theta_1 + i\,\mathrm{sen}\,\theta_1) \text{ e } z_2 = r_2(\cos\theta_2 + i\,\mathrm{sen}\,\theta_2)$$

segue a multiplicação e divisão, respectivamente:

$$z_1 z_2 = r_1 r_2[\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2)] \tag{3.8}$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i\,\mathrm{sen}(\theta_1 - \theta_2)] \tag{3.9}$$

Além disso, $z_1 = z_2 \Leftrightarrow r_1 = r_2$ e $\theta_1 \equiv \theta_2 (mod\, 2\pi)$.

As igualdades seguem imediatamente considerando as relações conhecidas:

- $\cos(\theta_1 + \theta_2) = \cos\theta_1 \cos\theta_2 - \mathrm{sen}\,\theta_1\,\mathrm{sen}\,\theta_2$
- $\mathrm{sen}(\theta_1 + \theta_2) = \mathrm{sen}\,\theta_1 \cos\theta_2 + \cos\theta_1\,\mathrm{sen}\,\theta_2$
- $\cos(\theta_1 - \theta_2) = \cos\theta_1 \cos\theta_2 + \mathrm{sen}\,\theta_1\,\mathrm{sen}\,\theta_2$
- $\mathrm{sen}(\theta_1 - \theta_2) = \mathrm{sen}\,\theta_1 \cos\theta_2 - \cos\theta_1\,\mathrm{sen}\,\theta_2$

A fórmula de multiplicação acima estende-se para um número qualquer de fatores. Sendo

$$z_j = r_j(\cos\theta_j + i\,\mathrm{sen}\,\theta_j),\ j = 1, 2, ..., n$$

teremos

$$z_1 z_2 ... z_n = r_1 r_2 ... r_n[\cos(\theta_1 + \theta_2 + ... + \theta_n) + i\,\mathrm{sen}(\theta_1 + \theta_2 + ... + \theta_n)].$$

A demonstração segue por indução. Em particular, quando todos os fatores são iguais e de módulo unitário, obtemos a chamada *Fórmula de De Moivre*:

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^n = \cos n\theta + i\,\mathrm{sen}\,n\theta. \tag{3.10}$$

Esta fórmula é válida também para expoentes negativos. De fato:

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^{-n} = \frac{1}{(\cos\theta + i\,\mathrm{sen}\,\theta)^n} = \frac{1}{\cos n\theta + i\,\mathrm{sen}\,n\theta} = \cos n\theta - i\,\mathrm{sen}\,n\theta,$$

isto é,

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^{-n} = \cos(-n\theta) + i\,\mathrm{sen}(-n\theta). \tag{3.11}$$

Exemplo 3.5. Vamos calcular o valor de $(1+i)^{200}$. Como $1+i = \sqrt{2}\left(\cos\frac{\pi}{4} + i\,\mathrm{sen}\,\frac{\pi}{4}\right)$ temos que $(1+i)^{200} = (\sqrt{2})^{200}\left(\cos\left(200\frac{\pi}{4}\right) + i\,\mathrm{sen}\left(200\frac{\pi}{4}\right)\right) = 2^{100}(\cos(50\pi) + i\,\mathrm{sen}(50\pi))$ $= 2^{100}$, pois 50π é múltiplo de 2π.

As seguintes propriedade se verificam de forma imediata:

1-) $|z| \geq 0$ e $|z| = 0$ se, e somente se, $z = 0$;

2-) $|Re(z)| \leq |z|$ e $|Im(z)| \leq |z|$,

3-) $|z| = |-z|$.

Desenvolvendo $|z_1 z_2|^2 = (z_1 z_2)(\overline{z_1 z_2}) = (z_1\bar{z_1})(z_2\bar{z_2}) = |z_1|^2|z_2|^2$ segue a propriedade 4:

4-) $|z_1 z_2| = |z_1||z_2|$.

Mostremos agora um resultado importante bem conhecido: a *desigualdade do triângulo*, ou ainda a propriedade 5:

5-) $|z_1 + z_2| \leq |z_1| + |z_2|$.

Sua representação geométrica é traduzida por:*a soma dos comprimentos de dois lados de um triângulo é maior ou igual ao comprimento do terceiro lado* (Figura 3.6).

Para a demonstração observemos que:

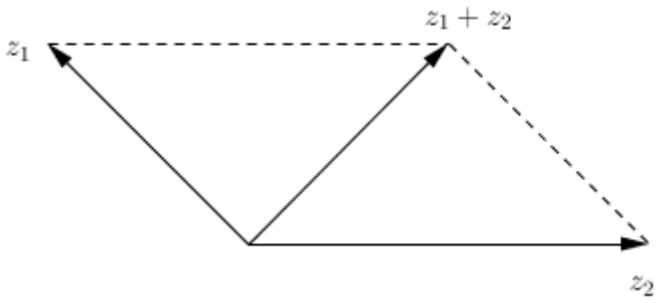


Figura 3.6: Representação geométrica da desigualdade triangular.
Fonte: print screen do software Geogebra.

$$\begin{aligned}
|z_1+z_2|^2 &= (z_1+z_2)(\bar{z_1}+\bar{z_2}) \\
&= z_1\bar{z_1} + z_2\bar{z_2} + (z_1\bar{z_2} + \bar{z_1}z_2) \\
&= |z_1|^2 + |z_2|^2 + z_1\bar{z_2} + \overline{z_1\bar{z_2}} \\
&= |z_1|^2 + |z_2|^2 + 2Re(z_1\bar{z_2}) \\
&\leq |z_1|^2 + |z_2|^2 + 2|Re(z_1\bar{z_2})| \\
&\leq |z_1|^2 + |z_2|^2 + 2|z_1z_2| \\
&= |z_1|^2 + |z_2|^2 + 2|z_1||z_2| \\
&= (|z_1| + |z_2|)^2.
\end{aligned}$$

Daí, extraindo a raiz segue a desigualdade.

Observamos ainda que $|z_1 - z_2| = |z_1 + (-z_2)| \leq |z_1| + |-z_2|$, e como $|-z_2| = |z_2|$, concluímos outra desigualdade:

6-) $|z_1 - z_2| \leq |z_1| + |z_2|$.

Uma terceira desigualdade conhecida é

7-) $|z_1| - |z_2| \leq |z_1 + z_2|$.

Para isto basta observar que

$$|z_1| = |(z_1 + z_2) - z_2| \leq |z_1 + z_2| + |z_2| \tag{3.12}$$

e então subtrair $|z_2|$ do primeiro e último membros.

Por último, uma quarta desigualdade:

8-) $||z_1| - |z_2|| \leq |z_1 + z_2|$.

Para a verificação basta tomar $|z_1| - |z_2| = a$ e do item (7) segue que

$$a \leq |z_1 + z_2| \text{ e } -a \leq |z_1 + z_2|,$$

e daí

$$|a| \leq |z_1 + z_2|,$$

ou seja,

$$||z_1| - |z_2|| \leq |z_1 + z_2|.$$

3.3 Raízes n-ésimas

O problema de extrair a raiz n-ésima, $z^{\frac{1}{n}}$, do número complexo $z \neq 0$ corresponde a resolver a equação:

$$\omega^n = z. \tag{3.13}$$

Tomando

$$\omega = \rho(\cos\phi + i\,\mathrm{sen}\,\phi)$$
$$z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$$

segue da *fórmula de De Moivre* (3.10) que

$$\rho^n(\cos n\phi + i\,\mathrm{sen}\,n\phi) = r(\cos\theta + i\,\mathrm{sen}\,\theta).$$

Consequentemente, da igualdade de números complexos segue:

$$\rho^n \cos n\phi = r\cos\theta \text{ e } \rho^n \,\mathrm{sen}\, n\phi = r\,\mathrm{sen}\,\theta,$$

ou ainda,

$$\rho^n = r \text{ e } n\phi = \theta + 2k\pi,$$

onde k é um número inteiro. Daí segue que ρ é a raiz n-ésima positiva de r e

$$\omega = \sqrt[n]{z} = \sqrt[n]{r}\left(\cos\frac{\theta + 2k\pi}{n} + i\,\mathrm{sen}\,\frac{\theta + 2k\pi}{n}\right). \tag{3.14}$$

Quando $z = 0$, a Equação 3.14 tem apenas uma solução: $\omega = 0$.

Exemplo 3.6. Todo $\omega \in \{-4i, 2\sqrt{3} + 2i, -2\sqrt{3} + 2i\}$ é uma raiz cúbica de $64i$.

De fato, temos $(-4i)^3 = (-4)^3 \cdot i^3 = (-64) \cdot (-i) = 64i$. Para calcular o cubo dos números $2\sqrt{3} + 2i$ e $-2\sqrt{3} + 2i$ escrevemos primeiro sua forma polar:

$$2\sqrt{3} + 2i = 4\left(\cos\tfrac{\pi}{6} + i\,\mathrm{sen}\,\tfrac{\pi}{6}\right) \text{ e } -2\sqrt{3} + 2i = 4\left(\cos\tfrac{5\pi}{6} + i\,\mathrm{sen}\,\tfrac{5\pi}{6}\right).$$

Usando a fórmula de *De Moivre* (3.10), obtemos

$$\begin{aligned}(2\sqrt{3}+2i)^3 &= 4^3\left(\cos\frac{\pi}{2}+i\,\mathrm{sen}\,\frac{\pi}{2}\right)=64i,\\ (-2\sqrt{3}+2i)^3 &= 4^3\left(\cos\frac{5\pi}{2}+i\,\mathrm{sen}\,\frac{5\pi}{2}\right)\\ &= 4^3\left(\cos\left(2\pi+\frac{\pi}{2}\right)+i\,\mathrm{sen}\left(2\pi+\frac{\pi}{2}\right)\right)\\ &= 64\left(\cos\frac{\pi}{2}+i\,\mathrm{sen}\,\frac{\pi}{2}\right)=64i.\end{aligned}$$

Proposição 3.1 ([14], p.37)**.** *Para cada número natural n, um número complexo $z\neq 0$ tem exatamente n raízes complexas n-ésimas, a saber,*

$$z_k=\sqrt[n]{r}\left(\cos\left(\tfrac{\theta+2\pi k}{n}\right)+i\,\mathrm{sen}\left(\tfrac{\theta+2\pi k}{n}\right)\right), k=0,1,\cdots,n-1,$$

onde $r=|z|>0$ e $\theta=arg(z)$.

Demonstração. Seja $n\geq 2$ um número natural dado. Primeiramente, escrevemos z na forma polar $z=r(\cos\theta+\mathrm{sen}\,\theta)$, em que $r=|z|$ e $\theta=arg(z)$. Vamos calcular as raízes n-ésimas também na forma polar. Queremos determinar os números complexos $\omega=\rho(\cos\phi+i\,\mathrm{sen}\,\phi)$ tais que $z=\omega^n$.

Como $\omega^n=\rho^n(\cos(n\phi)+i\,\mathrm{sen}(n\phi))$, temos $\omega^n=z$ se, e somente se,

$$\begin{cases}\rho^n=r\\ n\phi=\theta+2\pi k,\ k\in\mathbb{Z}\end{cases}\Leftrightarrow\begin{cases}\rho=\sqrt[n]{r},\ \rho\in\mathbb{R},\ \rho>0\\ \phi=\frac{\theta+2\pi k}{n},\ k\in\mathbb{Z}.\end{cases}$$

Portanto,

$$z_\lambda=\sqrt[n]{r}\left(\cos\left(\tfrac{\theta+2\pi\lambda}{n}\right)+i\,\mathrm{sen}\left(\tfrac{\theta+2\pi\lambda}{n}\right)\right),\text{ onde }\lambda\in\mathbb{Z}.$$

Sejam $\lambda,\mu\in\mathbb{Z}$. Da igualdade de números complexos na forma polar temos que

$$\begin{aligned}z_\lambda=z_\mu &\iff \frac{\theta+2\pi\lambda}{n}-\frac{\theta+2\pi\mu}{n}=2\pi s,\text{para algum } s\in\mathbb{Z}\\ &\iff \frac{2\pi\lambda}{n}-\frac{2\pi\mu}{n}=2\pi s,\text{para algum } s\in\mathbb{Z}\\ &\iff \frac{\lambda}{n}-\frac{\mu}{n}=s,\text{para algum } s\in\mathbb{Z}\\ &\iff \lambda-\mu=sn,\text{para algum } s\in\mathbb{Z}\\ &\iff \lambda\equiv\mu(mod\ n).\end{aligned}$$

Dessa forma, só interessa o resto que λ deixa na divisão por n. Para cada resto há uma raiz n-ésima de z.

Logo, para cada $k=0,1,\cdots,n-1$ há uma raiz complexa n-ésima de z, determinada pelo argumento principal $\phi_k=\frac{\theta+2\pi k}{n}$, sendo as raízes complexas n-ésimas de z, portanto, dadas por

$$z_k = \sqrt[n]{r}(\cos\phi_k + i\,\mathrm{sen}\,\phi_k), \text{ onde } \phi_k = \tfrac{\theta+2\pi k}{n},\ k = 0, 1, \cdots, n-1.$$

□

Exemplo 3.7. Vamos determinar as raízes cúbicas de $z = -8i$.

Temos $r = 8$ e $\theta = arg(z) = \frac{3\pi}{2}$. Portanto, as raízes complexas cúbicas de z têm como módulo o número real $\rho = \sqrt[3]{r} = \sqrt[3]{8} = 2$ e argumentos principais

$$\phi_k = \tfrac{\theta+2\pi k}{3} = \tfrac{\pi}{2} + \tfrac{2\pi k}{3} \text{ e } k = 0, 1, 2.$$

Assim, as raízes cúbicas z_0, z_1 e z_2 de z são obtidas como segue:

$\phi_0 = \frac{\pi}{2} \Rightarrow z_0 = 2\left(\cos\frac{\pi}{2} + i\,\mathrm{sen}\,\frac{\pi}{2}\right) = 2i;$

$\phi_1 = \frac{7\pi}{6} \Rightarrow z_1 = 2\left(\cos\frac{7\pi}{6} + i\,\mathrm{sen}\,\frac{7\pi}{6}\right) = 2\left(-\frac{\sqrt{3}}{2} - i\frac{1}{2}\right) = -\sqrt{3} - i,$

$\phi_2 = \frac{11\pi}{6} \Rightarrow z_2 = 2\left(\cos\frac{11\pi}{6} + i\,\mathrm{sen}\,\frac{11\pi}{6}\right) = 2\left(\frac{\sqrt{3}}{2} - i\frac{1}{2}\right) = \sqrt{3} - i.$

3.3.1 Raízes da Unidade

As raízes complexas n-ésimas de 1 são chamadas **raízes n-ésimas da unidade**.

A única raiz 1-ésima da unidade é 1. Quando $n \geq 2$, temos

$$\theta = arg(1) = 0 \text{ e } \phi_k = \tfrac{2\pi k}{n}, \text{ onde } k = 0, 1, \cdots, n-1,$$

e as raízes complexas n-ésimas da unidade são os pontos

$$z_k = \cos\tfrac{2\pi k}{n} + i\,\mathrm{sen}\,\tfrac{2\pi k}{n} \text{ e } k = 0, 1, \cdots, n-1,$$

que dividem o círculo em n partes iguais, sendo $z_0 = 1$. Portanto, se $n \geq 3$, as raízes n-ésimas da unidade são vértices de um polígono regular n lados inscrito no círculo de centro na origem e raio 1 em $\mathbb{C}$, tendo um dos vértices no ponto 1. Esta interpretação geométrica das raízes n-ésimas da unidade é devida a *Euler*.

Exemplo 3.8. As raízes quadradas da unidade são $\{1, -1\}$ e as raízes quartas da unidade são $\{1, i, -1, -i\}$. Por outro lado, as raízes cúbicas da unidade são $\{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\}$.

Nas Figuras (3.7) e (3.8) apresentamos a representação geométrica das raízes complexas quartas e cúbicas da unidade no círculo de raio 1, centrado na origem, respectivamente.

Denotando $\zeta_n = z_1 = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$, temos que

$$z_k = \cos\tfrac{2\pi k}{n} + i\,\mathrm{sen}\,\tfrac{2\pi k}{n} = \zeta_n^k,\ k = 0, \cdots, n-1.$$

Portanto, as n raízes complexas da unidade, denotadas por $U_n(\mathbb{C})$, são obtidas como potências de ζ_n, isto é,

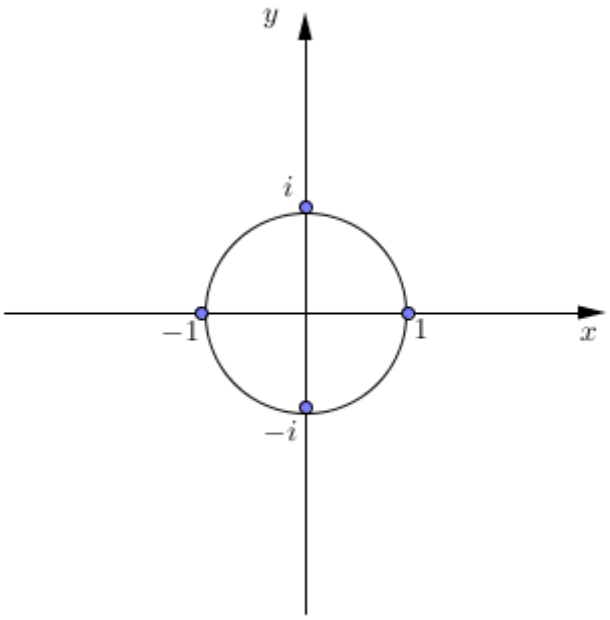


Figura 3.7: Raízes quartas de 1.
Fonte: print screen do software Geogebra.

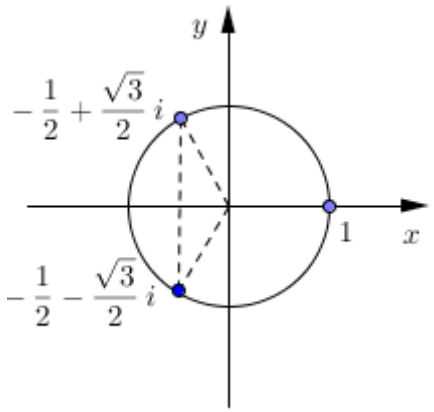


Figura 3.8: Raízes complexas cúbicas de 1.
Fonte: print screen do software Geogebra.

$$U_n(\mathbb{C}) = \{\zeta_n, \cdots, \zeta_n^{n-1}, \zeta_n^n = 1\}.$$

Vimos na Proposição (3.1) que cada número complexo não nulo z tem n raízes n-ésimas. Conhecendo uma das suas raízes n-ésimas, podemos determinar todas as outras raízes n-ésimas através da proposição que se segue.

Proposição 3.2 ([14], p. 45)**.** *Seja z um número complexo não nulo, $\omega \in \mathbb{C}$ uma raiz n-ésima de z e $\zeta_n = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$. Então, as raízes n-ésimas de z são $\omega \cdot \zeta_n^r$, $r = 1, \cdots, n$.*

Demonstração. Observe que $(\omega \cdot \zeta_n^r)^n = \omega^n \cdot (\zeta_n^n)^r = z \cdot 1^r = z$. Logo, $\omega \cdot \zeta_n^r$ é raiz n-ésima de z, para todo $r = 1, \cdots, n$.

Seja $\alpha \in \mathbb{C}$ uma raiz n-ésima de z. Então, $\alpha^n = z = \omega^n$ e $1 = \alpha^n \cdot \omega^{-n} = (\alpha \cdot \omega^{-1})^n$. Portanto, $\alpha \cdot \omega^{-1}$ é uma raiz n-ésima da unidade. Assim, existe $r = 0, \cdots, n-1$ tal que $\alpha \cdot \omega^{-1} = \zeta_n^r$, isto é, $\alpha = \omega \cdot \zeta_n^r$, para algum $r = 1, \cdots, n$. □

Exemplo 3.9. Vamos determinar as raízes quartas de $z = 16$. Temos que $\zeta_4 = \frac{\cos 2\pi}{4} + i\frac{\operatorname{sen} 2\pi}{4} = i$.

Assim, como $\omega = 2$ é uma raiz quarta de 16, segue que as outras raízes são: $2\zeta_4 = 2i,\ 2\zeta_4^2 = 2 \cdot i^2 = -2,\ 2\zeta_4^3 = 2 \cdot i^3 = -2i, 2\zeta_4^4 = 2 \cdot 1 = 2$.

Observamos anteriormente que as potências de expoentes $1, 2, \cdots, n$ de $\zeta_n = \cos\frac{2\pi}{n} + i \operatorname{sen}\frac{2\pi}{n}$ fornecem todas as raízes n-ésimas da unidade. Temos, mais ainda,

$$\{\zeta_n^m |\ m \in \mathbb{Z}\} = U_n(\mathbb{C}).$$

De fato, dado $m \in \mathbb{Z}$, pela divisão de m por n, existem $q, r \in \mathbb{Z}$ tais que $m = nq + r$, onde $0 \leq r \leq n-1$. Assim,

$$\zeta_n^m = \zeta_n^{nq+r} = (\zeta_n^n)^q \cdot \zeta_n^r = 1^q \cdot \zeta_n^r = \zeta_n^r,$$

mostrando que $\zeta_n^m \in U_n(\mathbb{C})$. A outra inclusão é óbvia.

Definição 3.1. *Uma raiz complexa n-ésima da unidade α, isto é, $\alpha \in U_n(\mathbb{C})$, é chamada de uma raiz primitiva n-ésima da unidade se*

$$U_n(\mathbb{C}) = \{\alpha^m |\ m \in \mathbb{Z}\}.$$

Isto é equivalente ao fato das potências de α determinarem todas as raízes n-ésimas da unidade.

Exemplo 3.10. Temos que $U_2(\mathbb{C}) = \{\zeta_2, \zeta_2^2\} = \{1, -1\}$. Observe que:

- $\{1^m |\ m \in \mathbb{Z}\} = \{1\}$ e
- $\{(-1)^m |\ m \in \mathbb{Z}\} = \{1, -1\} = U_2(\mathbb{C})$

Portanto, -1 é a única raiz primitiva quadrada da unidade.

Exemplo 3.11. i e $-i$ são as únicas raízes primitivas quartas da unidade, pois:

- $\{i^m |\ m \in \mathbb{Z}\} = \{1, i, i^2 = -1, i^3 = -i\} = U_4(\mathbb{C})$;
- $\{-i^m |\ m \in \mathbb{Z}\} = \{1, -i, (-i)^2 = -1, (-i)^3 = i\} = U_4(\mathbb{C})$;
- $\{1^m |\ m \in \mathbb{Z}\} = \{1\} \neq U_4(\mathbb{C})$,
- $\{(-1)^m |\ m \in \mathbb{Z}\} = \{1, -1\} \neq U_4(\mathbb{C})$.

Exemplo 3.12. Vamos determinar as raízes primitivas 6-ésimas da unidade.

Temos que $U_6(\mathbb{C}) = \{\zeta_6, \zeta_6^2, \cdots, \zeta_6^5, \zeta_6^6 = 1\}$ são as raízes 6-ésimas da unidade, em que $\zeta_6^k = \cos\frac{2\pi k}{6} + i \operatorname{sen}\frac{2\pi k}{6}$, $k = 1, \cdots, 6$.

- $\{\zeta_6^m |\ m \in \mathbb{Z}\} = \{\zeta_6 = \frac{1}{2} + \frac{\sqrt{3}}{2}i, \zeta_6^2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \zeta_6^3 = -1, \zeta_6^4 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \zeta_6^5 = \frac{1}{2} - \frac{\sqrt{3}}{2}i, \zeta_6^6 = 1\} = U_6(\mathbb{C})$ e, portanto ζ_6 é raiz primitiva da unidade.
- $\{(\zeta_6^2)^m |\ m \in \mathbb{Z}\} = \{\zeta_6^2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, (\zeta_6^2)^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, (\zeta_6^2)^3 = 1\} \neq U_6(\mathbb{C})$ e, portanto ζ_6^2 não é raiz primitiva da unidade.

Continuando dessa forma concluímos que ζ_6^5 é raiz primitiva da unidade, pois $\{(\zeta_6^5)^m |\ m \in \mathbb{Z}\} = \{\zeta_6^5, \cdots, (\zeta_6^5)^6 = 1\} = U_6(\mathbb{C})$. No entanto, ζ_6^3 e ζ_6^4 não são raízes primitivas da unidade, pois $\{(\zeta_6^3)^m |\ m \in \mathbb{Z}\} = \{\zeta_6^3, (\zeta_6^3)^2 = 1\} \neq U_6(\mathbb{C})$ e $\{(\zeta_6^4)^m |\ m \in \mathbb{Z}\} = \{\zeta_6^4, (\zeta_6^4)^2 = 1\} \neq U_6(\mathbb{C})$.

Uma caracterização das raízes primitivas segue do resultado:

Proposição 3.3. *Seja $\zeta_n \in \mathbb{C}$, $n \geq 2$, uma raiz n-ésima da unidade e $k \in \mathbb{Z}$. Assim, ζ_n^k é uma raiz n-ésima primitiva da unidade se, e somente se, $mdc(k, n) = 1$.*

Demonstração. Seja ζ_n^k uma raiz n-ésima primitiva da unidade. Suponhamos que $mdc(k, n) \neq 1$, ou seja, $mdc(k, n) = d$, com $d \neq 1$ e $d \neq n$. Assim, existe $x \in \mathbb{N}$ tal que $n = dx$. Logo,

$$(\zeta_n^k)^d = (\zeta_n)^{k\frac{n}{x}} = (\zeta_n^n)^{\frac{k}{x}} = 1$$

que é um absurdo, tendo em vista que tomamos $1 < d < n$ e ζ_n é uma raiz n-ésima primitiva da unidade. Portanto, $mdc(k, n) = 1$. Por outro lado, se $mdc(k, n) = 1$ e se $m \in \mathbb{N}$ é tal que $(\zeta_n^k)^m = 1$, ou ainda, $\zeta_n^{km} = 1$, implica $n|km$ (n divide km). Por hipótese $mdc(k, n) = 1$ resta que $n|m$. Daí concluímos ζ_n^k é uma raiz n-ésima primitiva da unidade. □

Em consequência, sendo $n > 2$, as raízes primitivas da unidade são sempre em número maior do que 1 e exatamente $n - 1$ se, n for número primo.

No exemplo (3.11) vimos que i e $-i$ são raízes primitivas quartas da unidade. De fato, $mdc(1, 4) = 1 = mdc(3, 4)$. No exemplo (6.2), vimos que ζ_6, ζ_6^5 são raízes primitivas 6-ésimas da unidade. De fato, $mdc(1, 6) = 1 = mdc(5, 6)$.

Como consequência da Proposição (3.3) tem-se que o número de raízes n-ésimas primitivas da unidade é dado por:

$$\varphi(n) = \#\{0 < m < n :\ mdc(m, n) = 1,\ m \in \mathbb{Z}\},$$

onde $\varphi : \mathbb{N} \to \mathbb{N}$ é a função de Euler.

Proposição 3.4 ([16], p.277)**.** *Sejam m e n ambos inteiros tais que $mdc(m, n) = 1$. Temos que $\zeta_m^k \zeta_n^l$, para $0 \leq k \leq m - 1$ e $0 \leq l \leq n - 1$, $mdc(m, n) = 1$, é uma raiz mn-ésima primitiva da unidade se, e somente se, ζ_m^k é uma raiz m-ésima primitiva da unidade e ζ_n^l é uma raiz n-ésima primitiva da unidade.*

Demonstração. Se ζ_m^k não é uma raiz m-ésima primitiva da unidade, então temos que $mdc(k,\, m) = d > 1$. Assim, $(\zeta_m^k \zeta_n^l)^{\frac{mn}{d}} = ((\zeta_m^k \zeta_n^l)^{mn})^{\frac{1}{d}} = 1^{\frac{1}{d}} = 1$, o que é absurdo, pois $\frac{mn}{d} < mn$. Reciprocamente, se ζ_m^k é uma raiz m-ésima primitiva da unidade e ζ_n^l é uma raiz n-ésima primitiva da unidade, então $mdc(k,\, m) = mdc(l,\, n) = 1$. Assim,

$$(\zeta_m^k \zeta_n^l)^a = 1 \iff \zeta_m^{ka} \zeta_n^{la} = 1 \iff \zeta_m^{ka} = \zeta_n^{-la} \iff \zeta_m^{kan} = \zeta_n^{-lan} \iff (\zeta_m^k)^{na} = (\zeta_n^n)^{-la} \iff (\zeta_m^k)^{na} = 1^{-la} \iff (\zeta_m^k)^{na} = 1 \iff m | na.$$

Como $mdc(m,\, n) = 1$ segue que $m|a$. De modo análogo, $n|a$. Ainda, usando o fato de que $mdc(m,\, n) = 1$ segue que $mn|a$. Assim temos que, $(\zeta_m^k \zeta_n^l)^{mn} = (\zeta_m^m)^{kn} (\zeta_n^n)^{lm} = 1$. Assim, mn é a menor potência tal que $(\zeta_m^k \zeta_n^l)^{mn} = 1$. Portanto $\zeta_m^k \zeta_n^l$ é uma raiz mn-ésima primitiva da unidade. □

Seja ζ_n uma raiz n-ésima primitiva da unidade. Um **corpo ciclotômico** $\mathbb{K}$ é uma extensão de $\mathbb{Q}$ gerada por ζ_n, isto é, $\mathbb{K} = \mathbb{Q}(\zeta_n)$.

Os corpos ciclotômicos desempenham um papel importante na teoria de reticulados, que veremos na Seção 6. Veremos que através dos corpos ciclotômicos podemos construir reticulados no $\mathbb{R}^n$.

A seguir apresentamos dois resultados importantes envolvendo corpos ciclotômicos e que não demonstraremos aqui, pelo fato de suas demonstrações utilizarem pré-requisitos que fogem dos objetivos deste trabalho. Faremos o uso desses resultados na Seção 6.

Teorema 3.1. *[16] Se ζ_n é uma raiz n-ésima primitiva da unidade, então* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Proposição 3.5. *[27] Os monomorfismos de $\mathbb{Q}(\zeta_n)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$, são dados por* $\{\sigma_i, mdc(i,n) = 1, i = 1, ..., n-1, \sigma_i(\zeta) = \zeta^i\}$.

3.4 A Função Exponencial

Nesta seção, lembraremos de alguns conceitos estudados nos cursos de cálculo: a constante de Euler e, a função exponencial e^x e as funções trigonométricas seno e cosseno. Os desenvolvimentos dessas funções em séries de potências, válidos para todos os valores reais da variável x, correspondem a:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \cdots \tag{3.15}$$

$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!} = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots \tag{3.16}$$

$$\operatorname{sen} x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{(2n+1)}}{(2n+1)!} = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots \tag{3.17}$$

Em particular, a *constante de Euler* e que é um número irracional compreendido entre 2 e 3 ($e = 2,71828...$), se obtém de (3.15) com $x = 1$. Ou ainda,

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = 1 + 1 + \frac{1}{2} + \frac{1}{3!} + \cdots \tag{3.18}$$

Outro resultado para se retomar é mais uma das contribuições de Leonhard Euler (1707 - 1783) nos vários ramos da matemática em que seu nome é citado. Se a fórmula (3.15) fosse válida para z complexo, teríamos

$$\begin{aligned} e^{iy} &= 1 + iy + \frac{(iy)^2}{2!} + \frac{(iy)^3}{3!} + \frac{(iy)^4}{4!} + \frac{(iy)^5}{5!} + \frac{(iy)^6}{6!} + \frac{(iy)^7}{7!} \cdots & (3.19) \\ &= 1 + iy - \frac{y^2}{2!} - i\frac{y^3}{3!} + \frac{(iy)^4}{4!} + i\frac{y^5}{5!} - \frac{y^6}{6!} - i\frac{y^7}{7!} \cdots & (3.20) \end{aligned}$$

onde y é real.

Organizando a equação acima ainda teríamos

$$e^{iy} = 1 - \tfrac{y^2}{2!} + \tfrac{(iy)^4}{4!} - \tfrac{y^6}{6!} + \cdots + i(y - \tfrac{y^3}{3!} + \tfrac{y^5}{5!} - \tfrac{y^7}{7!} \cdots)$$

ou ainda, de (3.16) e (3.17)

$$e^{iy} = \cos y + i \operatorname{sen} y. \tag{3.21}$$

Estas considerações não estabelecem a relação (3.21) mas, servem como motivação para definirmos a função exponencial. A definição da função exponencial complexa no caso de um expoente qualquer $z = x + yi$ deve manter a propriedade aditiva da exponencial real: $e^{x_1+x_2} = e^{x_1} \cdot e^{x_2}$ [2]. Com isso definimos:

Definição 3.2. *A **função exponencial** $f : \mathbb{C} \to \mathbb{C}$, dada por $f(z) = e^z$, para um número complexo qualquer $z = x + iy$ é definida por $e^z = e^{x+iy} = e^x(\cos y + i \operatorname{sen} y)$.*

A partir da definição e das propriedades das funções reais $\operatorname{sen} x$, $\cos x$ e e^x se verificam facilmente as propriedades para a exponencial complexa:

1-) $e^{z_1} e^{z_2} = e^{z_1+z_2}$;

2-) $e^{-z} = \dfrac{1}{e^z}$;

3-) $(e^z)^n = e^{nz}$;

4-) $e^z \neq 0$ para todo z;

5-) $|e^z| = e^{Re(z)}$,

6-) $e^z = 1$ se, e somente se, $z = 2k\pi i$, k inteiro.

A forma polar de um número complexo $z \neq 0$ pode ser escrita como $z = re^{\theta i}$, $r = |z|$. Nesta representação, podemos usar propriedades da exponencial e obter facilmente que, para quaisquer números complexos $z_1 = r_1 e^{\theta_1 i}$ e $z_2 = r_2 e^{\theta_2 i}$:

- $z_1 \cdot z_2 = r_1 e^{\theta_1 i} r_2 e^{\theta_2 i} = r_1 r_2 e^{\theta_1 i} e^{\theta_2 i} = r_1 r_2 e^{(\theta_1 + \theta_2) i}$,
- $z_1^n = (re^{\theta i})^n = r^n (e^{\theta i})^n = r^n e^{n\theta i}$.

Diz-se que uma função complexa f é **periódica**, de período $w \in \mathbb{C} \setminus \{0\}$, ou que $w \in \mathbb{C} \setminus \{0\}$ é um **período** de f, se $f(z) = f(z+w)$ para todos os pontos z do domínio de f.

Pode-se observar que, ao contrário da função exponencial real, a função exponencial complexa é **periódica**, com período complexo $2\pi i$. De fato, note que $e^{2\pi i} = \cos 2\pi + i \operatorname{sen} 2\pi = 1$ e, em vista que $e^{z+2\pi i} = e^z e^{2\pi i} = e^z$, temos que $f(z + 2\pi i) = f(z)$. Em decorrência dessa periodicidade complexa, todos os valores possíveis de $f(z) = e^z$ são considerados em qualquer faixa horizontal de largura 2π.

4 Resolvendo Equações

Equação polinomial ou *algébrica* é toda equação da forma $p(x) = 0$, em que $p(x)$ é um polinômio (Seção 2.7). As raízes do polinômio constituem o conjunto solução da equação. Para as equações em que o grau é 1 ou 2, o método de resolução é simples e prático e nos casos em que o grau dos polinômios é 3 ou 4, existem expressões para a obtenção da solução e são esses casos que serão estudados no presente capítulo. É curioso notar que a classificação das equações pelo grau permeia os séculos XVI e XVII. Um dos matemáticos da época que contribuíram por esta forma de classificação foi René Descartes (1596 - 1650) em sua única obra matemática *A geometria*, de 1637, mas usava o termo *dimensão* para o que atualmente chamamos de grau. As principais referências utilizadas são [9], [11] e [14].

4.1 Solução por Radicais

Exibir as soluções de uma equação dada por meio de radicais significa encontrar estas soluções por meio da manipulação de seus coeficientes através das quatro operações aritméticas e da extração de raízes.

Essa forma de exibir soluções para uma equação foi desenvolvida na Europa, entre os séculos XVI e XIX. No ano de 1540, após a resolução da equação cúbica (Seção 3.1), o discípulo de Cardano, Ludovico Ferrari, obtém êxito na resolução de equações quárticas. Outras resoluções de quárticas também foram realizadas por outros métodos pelos matemáticos François Viète (século XVI) e por Descartes (1637).

Mostraremos as soluções das equações polinomiais de graus 1, 2, 3 e 4 por meio da seguinte ideia central: trocar a equação dada de grau n para uma equação equivalente, de grau $n - 1$ e, caso soubermos resolver essa nova equação, nosso problema estará resolvido; caso contrário é necessário obter sucessivas reduções dos graus, até onde for necessário.

4.1.1 Equações Lineares

Sejam a, $b \in \mathbb{C}$, com $a \neq 0$. Uma equação linear geral é dada por:

$$ax + b = 0 \tag{4.1}$$

Facilmente obtemos a solução por radicais de (4.1) como sendo:

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

4.1.2 Equações Quadráticas

Sejam a, $b \in \mathbb{C}$, com $a \neq 0$. Uma equação quadrática geral é da forma:

$$ax^2 + bx + c = 0 \tag{4.2}$$

A solução por radicais é obtida efetuando as seguintes operações:

I. Dividindo por a ambos os lados da Equação (4.2),

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \tag{4.3}$$

II. Subtraindo $\frac{c}{a}$ em ambos lados da Equação (4.3),

$$x^2 + \frac{b}{a}x = -\frac{c}{a} \tag{4.4}$$

III. Somando $\left(\frac{b^2}{4a^2}\right)$ em ambos os lados da Equação (4.4),

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = -\frac{c}{a} + \frac{b^2}{4a^2}$$

ou ainda,

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a} \tag{4.5}$$

IV. Como $\mathbb{C}$ é um *corpo*, que contém o corpo dos números reais $\mathbb{R}$, onde se pode extrair uma raiz quadrada de um número real qualquer (inclusive negativo), podemos calcular a raiz quadrada de $\frac{b^2}{4a^2} - \frac{c}{a}$. Logo da Proposição (3.2), segue

$$x + \frac{b}{2a} = \zeta_2^1\sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} \text{ e } x + \frac{b}{2a} = \zeta_2^2\sqrt{\frac{b^2}{4a^2} - \frac{c}{a}}$$

e como $\zeta_2^1 = \cos\frac{2\pi 1}{2} + i\,\mathrm{sen}\,\frac{2\pi 1}{2} = -1$ e $\zeta_2^2 = \cos\frac{2\pi 2}{2} + i\,\mathrm{sen}\,\frac{2\pi 2}{2} = 1$, escrevemos,

$$x + \frac{b}{2a} = \pm\sqrt{\frac{b^2}{4a^2} - \frac{c}{a}}. \tag{4.6}$$

V. Subtraindo $\frac{b}{2a}$ em ambos os lados da Equação (4.6),

$$x = \pm\sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} - \frac{b}{2a} \tag{4.7}$$

apenas organizando a Equação (4.7),

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

e pondo $\Delta = b^2 - 4ac$, concluímos $x = \dfrac{-b \pm \sqrt{\Delta}}{2a}$.

Exemplo 4.1. Quais as raízes da equação $x^2 + 2ix + (-2 - i) = 0$?

Temos que $\Delta = (2i)^2 - 4(-2 - i) = 4 + 4i$.

Calculemos as raízes quadradas de $4 + 4i$. Consideremos

$$4 + 4i = (a + bi)^2 = a^2 - b^2 + 2abi, \text{ com } a, b \in \mathbb{R}.$$

Pela igualdade acima temos que:

$$4 = a^2 - b^2 \Rightarrow 4^2 = (a^2 - b^2)^2 \text{ e } 4 = 2ab \Rightarrow 4^2 = 4a^2b^2,$$
$$\text{ou ainda,}$$
$$4^2 + 4^2 = 32 = a^2 + b^2 + 2a^2b^2 = (a^2 + b^2)^2$$

Portanto, $a^2 + b^2 = \sqrt{32}$. Como também $a^2 - b^2 = 4$, somando e subtraindo essas equações, obtemos, respectivamente,

$$a^2 = \tfrac{\sqrt{32}+4}{2} \text{ e } b^2 = \tfrac{\sqrt{32}-4}{2}.$$

Logo,

$$|a| = \sqrt{\tfrac{\sqrt{32}+4}{2}} \text{ e } |b| = \sqrt{\tfrac{\sqrt{32}-4}{2}}, \text{ ou seja,}$$

$$|a| = \sqrt{2\sqrt{2} + 2} \text{ e } |b| = \sqrt{2\sqrt{2} - 2}. \tag{4.8}$$

Como $4 = 2ab$, ou ainda, $2 = ab > 0$, devemos escolher os números reais a e b, com a propriedade (4.8), de modo que o sinal do seu produto seja positivo.

As soluções da equação proposta são, portanto,

$$x_1 = \tfrac{-2i+\sqrt{\Delta}}{2} \text{ ou } x_2 = \tfrac{-2i-\sqrt{\Delta}}{2}.$$

onde $\sqrt{\Delta} = \sqrt{2\sqrt{2} + 2} + i\sqrt{2\sqrt{2} - 2}$.

4.1.3 Equações Cúbicas

Sejam **a, b, c** e **d** $\in \mathbb{C}$, com **a** $\neq 0$. Uma equação cúbica geral é da forma:

$$\mathbf{a}x^3 + \mathbf{b}x^2 + \mathbf{c}x + \mathbf{d} = 0.$$

Para facilitar nossos cálculos vamos dividir toda equação por **a**. Com isso, temos:

$$x^3 + bx^2 + cx + d = 0. \tag{4.9}$$

Tomemos a mudança de variável $x = y - \frac{b}{3}$. Assim,

$$\begin{aligned}
\left(y - \frac{b}{3}\right)^3 + b\left(y - \frac{b}{3}\right)^2 + c\left(y - \frac{b}{3}\right) + d &= 0 \\
\left(y^3 - y^2 b + y\frac{b^2}{3} - \frac{b^3}{27}\right) + \left(y^2 b - y\frac{2b^2}{3} + \frac{b^3}{9}\right) + \left(yc - \frac{bc}{3}\right) + d &= 0 \\
y^3 + \left(c - \frac{b^2}{3}\right)y + \left(\frac{2b^3}{27} - \frac{bc}{3} + d\right) &= 0.
\end{aligned}$$

Observe que, através dessa mudança de variável, não aparece a incógnita com expoente 2. Ainda, considerando $c - \frac{b^2}{3} = p$ e $\frac{2b^3}{27} - \frac{bc}{3} + d = q$, podemos, assumir, que toda equação cúbica é da forma:

$$y^3 + py + q = 0. \tag{4.10}$$

Vamos agora, concentrar nossa atenção na resolução da Equação (4.10).

Sejam u e v duas novas indeterminadas. Façamos em (4.10) a mudança de variáveis: $y = u + v$. Obtemos, então,

$$0 = (u+v)^3 + p(u+v) + q = (u^3 + v^3 + q) + (u+v)(p + 3uv). \tag{4.11}$$

Segue daí que cada solução (u, v) do sistema

$$\begin{cases} u^3 + v^3 = -q \\ u \cdot v = -\frac{p}{3} \end{cases}$$

nos fornece uma solução (u, v) de (4.11) e, portanto, uma solução da forma $y = u + v$ de (4.10).

Elevando ao cubo a segunda equação do sistema acima, segue-se que se (u, v) é uma solução do sistema, então u^3 e v^3 são soluções da seguinte equação do segundo grau:

$$z^2 + qz - \frac{p^3}{27} = 0. \tag{4.12}$$

Fixando uma das raízes quadradas de $\frac{q^2}{4} + \frac{p^3}{27}$ e denotando-a por $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, temos que as raízes de (4.12) são:

$$z_1 = -\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}} \text{ e } z_2 = -\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}.$$

Pela simetria do papel que desempenham u e v, podemos supor que $u^3 = z_1$ e $v^3 = z_2$.

Escolhendo uma das raízes cúbicas de z_1 e denotando-a por $\sqrt[3]{z_1}$, segue-se que as soluções de $u^3 = z_1$ são $\sqrt[3]{z_1}$, $\zeta_3\sqrt[3]{z_1}$ e $\zeta_3^2\sqrt[3]{z_1}$, em que $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ é uma das raízes cúbicas da unidade.

Agora, denotando por $\sqrt[3]{z_2}$ a raiz cúbica de z_2, tal que $\sqrt[3]{z_1}\sqrt[3]{z_2} = -\frac{p}{3}$, de modo que a segunda equação do sistema acima seja satisfeita, o referido sistema admite as seguintes soluções:

$$\begin{aligned} u_1 = \sqrt[3]{z_1},\ v_1 = \sqrt[3]{z_2};\\ u_2 = \zeta_3\sqrt[3]{z_1},\ v_2 = \zeta_3^2\sqrt[3]{z_2};\\ u_3 = \zeta_3^2\sqrt[3]{z_1},\ v_3 = \zeta_3\sqrt[3]{z_2}. \end{aligned}$$

Finalmente, a equação cúbica(4.10) possui como soluções as chamadas *fórmulas de Cardano*:

$$\begin{aligned} y_1 = u_1 + v_1 = \sqrt[3]{u} + \sqrt[3]{v} &= \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\\ y_2 = u_2 + v_2 = \zeta_3\sqrt[3]{u} + \zeta_3^2\sqrt[3]{v} &= \zeta_3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\\ y_3 = u_3 + v_3 = \zeta_3^2\sqrt[3]{u} + \zeta_3\sqrt[3]{v} &= \zeta_3^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \end{aligned}$$

Exemplo 4.2. Resolvamos a equação $x^3 - 3x - 1 = 0$.

Esta equação é desprovida do seu termo do segundo grau, logo as fórmulas de Cardano nos fornecem imediatamente as seguintes soluções:

$$\begin{aligned} x_1 &= \sqrt[3]{\frac{1}{2} + \frac{\sqrt{3}}{2}i} + \sqrt[3]{\frac{1}{2} - \frac{\sqrt{3}}{2}i};\\ x_2 &= \zeta_3\sqrt[3]{\frac{1}{2} + \frac{\sqrt{3}}{2}i} + \zeta_3^2\sqrt[3]{\frac{1}{2} - \frac{\sqrt{3}}{2}i},\\ x_3 &= \zeta_3^2\sqrt[3]{\frac{1}{2} + \frac{\sqrt{3}}{2}i} + \zeta_3\sqrt[3]{\frac{1}{2} - \frac{\sqrt{3}}{2}i}. \end{aligned}$$

Observe que

$$\sqrt[3]{\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i} = \sqrt[3]{\zeta_3}, \text{ onde } \zeta_3 = \cos\tfrac{\pi}{3} + i\,\mathrm{sen}\,\tfrac{\pi}{3},$$

que pode ser escolhida como sendo $\cos\frac{\pi}{9} + i\,\mathrm{sen}\,\frac{\pi}{9}$.

Portanto, $\sqrt[3]{\frac{1}{2}-\frac{\sqrt{3}}{2}i}=\sqrt[3]{\zeta_3}$ deve ser obrigatoriamente escolhida como sendo $\cos\frac{\pi}{9}-i\,\mathrm{sen}\,\frac{\pi}{9}$, pois devemos ter $\sqrt[3]{\zeta_3}\sqrt[3]{\overline{\zeta_3}}=-\frac{p}{3}=1$. Temos, então, que

$$\begin{aligned}
x_1 &= \left(\cos\frac{\pi}{9}+i\,\mathrm{sen}\,\frac{\pi}{9}\right)+\overline{\left(\cos\frac{\pi}{9}+i\,\mathrm{sen}\,\frac{\pi}{9}\right)}=2\cos\frac{\pi}{9};\\
x_2 &= \zeta_3\left(\cos\frac{\pi}{9}+i\,\mathrm{sen}\,\frac{\pi}{9}\right)+\overline{\zeta_3\left(\cos\frac{\pi}{9}+i\,\mathrm{sen}\,\frac{\pi}{9}\right)}=2\cos\frac{7\pi}{9},\\
x_3 &= \overline{\zeta_3}\left(\cos\frac{\pi}{9}+i\,\mathrm{sen}\,\frac{\pi}{9}\right)+\overline{\overline{\zeta_3}\left(\cos\frac{\pi}{9}+i\,\mathrm{sen}\,\frac{\pi}{9}\right)}=2\cos\frac{5\pi}{9}.
\end{aligned}$$

Exemplo 4.3. Resolvamos a equação $x^3-3x-18=0$.

Pelas fórmulas de Cardano, esta equação possui as seguintes raízes:

$$\begin{aligned}
x_1 &= \sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}};\\
x_2 &= -\frac{1}{2}\left(\sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}\right)+\frac{i\sqrt{3}}{2}\left(\sqrt[3]{9+4\sqrt{5}}-\sqrt[3]{9-4\sqrt{5}}\right),\\
x_3 &= -\frac{1}{2}\left(\sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}\right)-\frac{i\sqrt{3}}{2}\left(\sqrt[3]{9+4\sqrt{5}}-\sqrt[3]{9-4\sqrt{5}}\right).
\end{aligned}$$

A equação tem portanto uma raiz real e duas raízes complexas (conjugadas). Por inspeção, vê-se que 3 é raiz da equação, daí extraímos a seguinte igualdade curiosa:

$$3=\sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}.$$

Exemplo 4.4. Resolvamos a equação $x^3+6x^2+21x+14=0$.

Para eliminar o termo do segundo grau, efetuamos a substituição $x=y-2$, obtendo a equação $y^3+9y-12=0$, cujas raízes são:

$$\begin{aligned}
y_1 &= \sqrt[3]{6+\sqrt{63}}+\sqrt[3]{6-\sqrt{63}};\\
y_2 &= \zeta_3\sqrt[3]{6+\sqrt{63}}+\zeta_3^2\sqrt[3]{6-\sqrt{63}},\\
y_3 &= \zeta_3^2\sqrt[3]{6+\sqrt{63}}+\zeta_3\sqrt[3]{6-\sqrt{63}}.
\end{aligned}$$

Portanto, as raízes da equação original são:

$$x_1=y_1-2,\ x_2=y_2-2 \text{ ou } x_3=y_3-2.$$

4.1.4 Equações Quárticas

Sejam **a, b, c, d** e **e** $\in\mathbb{C}$, com **a** $\neq 0$. Uma equação quártica (ou biquadrada) geral é da forma:

$$\mathbf{a}x^4+\mathbf{b}x^3+\mathbf{c}x^2+\mathbf{d}x+\mathbf{e}=0. \tag{4.13}$$

Para facilitar nossos cálculos, sem perda de generalidade, dividimos (4.13) por **a** e obtemos:

$$x^4 + ax^3 + bx^2 + cx + d = 0. \tag{4.14}$$

Temos que $x^4 + ax^3 = -(bx^2 + cx + d)$. Completando o quadrado no primeiro membro desta equação e ajustando o segundo membro, temos:

$$\left(x^2 + \frac{1}{2}ax\right)^2 = \left(\frac{1}{4}a^2 - b\right)x^2 - cx - d. \tag{4.15}$$

Se o segundo membro desta equação fosse um quadrado perfeito, a resolução da equação recairia na resolução de duas equações do segundo grau. O nosso objetivo será, agora, transformar o segundo membro de (4.15) em um quadrado perfeito, sem destruir o quadrado perfeito do primeiro membro.

Somando a expressão $y^2 + 2y(x^2 + \frac{1}{2}ax)$ a ambos os membros de (4.15), obtemos

$$\left[\left(x^2 + \frac{1}{2}ax\right) + y\right]^2 = \left(2y + \frac{1}{4}a^2 - b\right)x^2 + (ya - c)x + (y^2 - d). \tag{4.16}$$

Vamos agora determinar os valores de y que transformarão o segundo membro de (4.16) em um quadrado perfeito. Para que isto ocorra, devemos ter o discriminante do segundo membro de (4.16), como trinômio do segundo grau em x, nulo. Ou seja,

$$(ya - c)^2 - 4\left(2y + \frac{1}{4}a^2 - b\right)(y^2 - d) = 0. \tag{4.17}$$

Daí, segue-se que

$$8y^3 - 4by^2 + (2ca - 8d)y + (4db - da^2 - c^2) = 0. \tag{4.18}$$

Escolhendo y como sendo uma das raízes da Equação (4.18), a Equação (4.16) nos fornece

$$\left[\left(x^2 + \frac{1}{2}ax\right) + y\right]^2 = (\alpha x + \beta)^2, \tag{4.19}$$

com α e β convenientes. Esta equação se resolve mediante a resolução das duas seguintes equações do segundo grau:

$$\left(x^2 + \tfrac{1}{2}ax\right) + y = (\alpha x + \beta) \text{ e } \left(x^2 + \tfrac{1}{2}ax\right) + y = -(\alpha x + \beta).$$

Como a Equação (4.14) é equivalente à Equação (4.19), temos que a resolução de uma equação do quarto grau pode ser reduzida à resolução de equações de graus dois e três.

Exemplo 4.5. Resolvamos a equação $x^4 - 2x^3 - x^2 - 2x - 2 = 0$.

Determinemos y satisfazendo a Equação (4.18), que, no nosso caso, toma a forma $2y^3 + y^2 + 6y + 3 = 0$. É fácil verificar que $y = -\frac{1}{2}$ é solução desta equação. Para este valor de y, a Equação (4.16) passa a ser

$$\left(x^2 - x - \tfrac{1}{2}\right)^2 = x^2 + 3x + \tfrac{9}{4} = \left(x + \tfrac{3}{2}\right)^2.$$

Obtemos, assim, as seguintes equações do segundo grau:

$$x^2 - x - \tfrac{1}{2} = x + \tfrac{3}{2} \text{ e } x^2 - x - \tfrac{1}{2} = -\left(x + \tfrac{3}{2}\right),$$

cujas raízes são as raízes da equação proposta. Assim, a equação proposta possui raízes:

$$1 + \sqrt{3}, 1 - \sqrt{3}, i \text{ ou } -i.$$

4.1.5 Equações de grau $n \geq 5$

Resolvidas as equações polinomiais, com coeficientes complexos, até o grau quarto, uma pergunta natural que se coloca é se as equações de grau maior do que 4 possuem sempre raízes complexas e, em tal caso, se há fórmulas algébricas para expressá-las em função dos coeficientes da equação.

A primeira pergunta é respondida afirmativamente pelo Teorema Fundamental da Álgebra que abordaremos adiante. A segunda pergunta foi respondida pela negativa pelo matemático norueguês Niels Henrik Abel (1802-1829), em um artigo publicado em 1829, para as equações gerais de graus maiores ou iguais do que cinco.

No entanto, algumas equações admitem fórmulas resolventes algébricas em termos dos seus coeficientes. Coube ao jovem matemático francês Évariste Galois (1811-1832) caracterizar tais equações, através de um estudo conhecido hoje como Teoria de Galois.

A insolubilidade da equação geral de grau $n \geq 5$ é provada nos cursos de álgebra sobre a teoria dos corpos, podendo ser encontrada em [10]. Parte deles é dedicada às extensões algébricas de corpos, culminando com o chamado Teorema Fundamental da Teoria de Galois.

Teorema 4.1 (Teorema Fundamental da Álgebra, [20], p.199)**.** *Todo polinômio complexo não constante possui pelo menos uma raiz.*

Através do *Teorema Fundamental da Álgebra* podemos provar um importante resultado que é dado na próxima proposição. Para a demonstração deste será necessário o *Teorema do Resto*, a saber:

Teorema 4.2 (Teorema do Resto, [18])**.** *Seja $p(x) \in \mathbb{C}[x]$ com $\partial p \geq 1$, e seja $\alpha \in \mathbb{C}$.*

1. *Existe $q(x) \in \mathbb{C}[x]$ e $r \in \mathbb{C}$ tal que $p(x) = (x - \alpha)q(x) + r$,*
2. *A constante r satisfaz $r = p(\alpha)$.*

Proposição 4.1. *([20]) Seja $p(x) \in \mathbb{C}[x]$ com $\partial p = n \geq 1$. Então existe $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ e $0 \neq a \in \mathbb{C}$, tal que,*

$$p(x) = a(x - \alpha_1).\cdots.(x - \alpha_n). \tag{4.20}$$

Demonstração. Usemos indução sobre n. Para o caso $n = 1$ é imediato. Se $n > 1$, sabemos do *Teorema Fundamental da Álgebra* (4.1), que $p(x)$ tem ao menos uma raiz em $\mathbb{C}$, chamemos tal de α_n. Pelo *Teorema do Resto*, existe $q(x) \in C[x]$ tal que

$$p(x) = (x - \alpha_n)q(x). \tag{4.21}$$

(Notemos que $r = p(\alpha_n) = 0$). Então, $\partial q = n - 1$, assim por indução,

$$q(x) = a(x - \alpha_1).\cdots.(x - \alpha_{n-1}) \tag{4.22}$$

para alguns números complexos $a, \alpha_1, \cdots, \alpha_{n-1}$. Substituindo (4.21) em (4.22), e o passo de indução está completo.

Segue imediatamente que os complexos α_j são os únicos zeros de $p(x)$.

Os zeros α_j não precisam ser distintos. Agrupando aqueles que são iguais, reescrevemos (4.20) como,

$$p(x) = a(x - \beta_1)^{m_1}.\cdots.(x - \beta_l)^{m_l}$$

onde β_j são distintos, e m_j são inteiros maiores do que, ou iguais a 1, e ainda, $m_1 + \cdots + m_l = n$. Chamamos m_j de multiplicidade do zero β_j de $p(x)$. □

Em particular, provamos que todo polinômio complexo de grau n tem precisamente n raízes complexas, contadas a partir da multiplicidade.

5 Teorema de Dirichlet

A partir do conceito de cálculo da raiz da unidade discutido no Capítulo 2, tomaremos $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. O objetivo agora será apresentar uma conexão entre raízes da unidade e um caso particular do Teorema de *Dirichlet* para progressões aritméticas. Para isso, apresentamos conceitos e propriedades de polinômios ciclotômicos. As principais referências usadas para o desenvolvimento deste capítulo foram [1], [5], [12], [22] e [23].

5.1 Polinômios Ciclotômicos

A teoria de polinômios nos permite apresentar algumas das propriedades elementares de uma classe muito importante de polinômios, conhecidos como *ciclotômicos*. Como subproduto do estudo que aqui faremos, mostraremos que os polinômios ciclotômicos são exatamente os polinômios minimais das raízes complexas da unidade.

Definição 5.1. *Seja ζ_n uma raiz n-ésima primitiva da unidade. O polinômio $\phi_n(x) = \prod_{j=1,\, mdc(j,n)=1}^{n} (x - \zeta_n^j)$ é chamado de **n-ésimo polinômio ciclotômico**.*

Lema 5.1 ([19], p. 196)**.** *Se n é um inteiro positivo, então $x^n - 1 = \prod_{d|n} \phi_d(x)$.*

Demonstração. Sendo $f(x) = x^n - 1$, temos que as raízes de $f(x)$ são $1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}$. Logo $x^n - 1 = (x-1)(x-\zeta_n).\cdots.(x-\zeta_n^{n-1})$. Analisando os períodos de cada raiz de $f(x)$, e escrevendo todas as raízes de mesmo período como um polinômio da forma $\phi_d = \prod_{\text{período de } \zeta_n = d} (x - \zeta_n)$, segue que $x^n - 1 = \prod_{d|n} \phi_d(x)$.

□

Como consequência do Lema (5.1) temos que

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\, d<n} \phi_d(x)}. \tag{5.1}$$

Assim, $\phi_1(x) = x - 1$, $\phi_2(x) = \dfrac{x^2-1}{\phi_1(x)} = \frac{x^2-1}{x-1} = x + 1$, $\phi_3(x) = \dfrac{x^3-1}{\phi_1(x)} = \dfrac{x^3-1}{x-1} = x^2 + x + 1$, $\phi_4(x) = \dfrac{x^4-1}{\phi_1(x)\phi_2(x)} = \dfrac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = x^2 + 1$. Quando $n = p$, onde p é

um número primo, segue que

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1. \tag{5.2}$$

que é chamado de p**-ésimo polinômio ciclotômico**.

Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo, de acordo com o Lema (5.1), temos que

$$x^{p^r} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x)\cdots\phi_{p^{r-1}}(x)\phi_{p^r}(x) \ \ e$$
$$x^{p^{r-1}} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x)\cdots\phi_{p^{r-1}}(x).$$

Logo, $\phi_{p^r}(x) = \dfrac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1$. Este polinômio é chamado de p^r**-ésimo polinômio ciclotômico**.

Exemplo 5.1. Considere o polinômio $f(x) = x^6 - 1$. Temos que as raízes de $f(x)$ são ζ_6, ζ_6^2, ζ_6^3, ζ_6^4, ζ_6^5, ζ_6^6. Deste modo, ζ_6, ζ_6^2, ζ_6^3, ζ_6^4 e ζ_6^5 tem período 6, 3, 2, 3 e 6 respectivamente. De fato, efetuando os cálculos vemos que $\zeta_6^6 = 1, (\zeta_6^2)^3 = 1, (\zeta_6^3)^2 = 1, (\zeta_6^4)^3 = 1$ e $(\zeta_6^5)^6 = 1$. Assim, $\phi_1(x) = (x - \zeta_6^6) = (x - 1)$, $\phi_2(x) = (x - \zeta_6^3)$, $\phi_3(x) = (x - \zeta_6^2)(x - \zeta_6^4)$, $\phi_6(x) = (x - \zeta_6)(x - \zeta_6^5)$. Como os divisores de 6 são 1, 2, 3, 6, temos que $x^6 - 1 = \prod_{d|6} \phi_d(x)$, ou seja, $x^6 - 1 = \phi_1(x)\phi_2(x)\phi_3(x)\phi_6(x) = (x-1)(x-\zeta_6^3)$ $(x - \zeta_6^2)(x - \zeta_6^4)(x - \zeta_6)(x - \zeta_6^5)$.

Proposição 5.1 ([19], p. 197)**.** *Para cada $n \in \mathbb{N}$, seja*

$$\phi_n(x) = \prod_{1 \leqslant k \leqslant n,\, mdc(k,n)=1} (x - \zeta_n^k),$$

onde $\zeta_n = e^{\frac{2\pi i}{n}}$. Então: $\phi_n(0) = 1$ para $n > 1$.

Demonstração. Por indução sobre $n \in \mathbb{N}$, temos primeiramente

$$x^2 - 1 = \phi_1(x)\phi_2(x) = (x - 1)\phi_2(x),$$

de modo que $\phi_2(x) = x + 1$ e $\phi_2(0) = 1$. Seja agora $n > 1$ e suponha, por hipótese de indução, que $\phi_m(0) = 1$ para todo inteiro $2 \leq m < n$. Então, se $g(x) = \prod_{1 \leq d < n, d|n} \phi_d(x)$, daí

$$g(0) = (-1) \prod_{1 < d < n, d|n} \phi_d(0) = -1,$$

Pelo Lema (5.1), segue $x^n - 1 = \phi_n(x)g(x)$. Daí

$$-1 = \phi_n(0)g(0) = -\phi_n(0),$$

como desejado. □

Observe que o corpo das raízes de $x^n - 1$ sobre $\mathbb{Q}$ é dado por $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade.

Teorema 5.1 ([16], p. 204)**.** *Se ζ_n é uma raiz n-ésima primitiva da unidade, então* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Demonstração. Seja $f(x)$ polinômio mônico, irredutível e de menor grau de ζ_n sobre $\mathbb{Q}$. Logo $x^n - 1 = f(x)h(x)$, com $h(x) \in \mathbb{Q}[x]$. Pelo Lema de Gauss segue que $f(x)$, $h(x) \in \mathbb{Z}[x]$. Seja p um número primo tal que $p \nmid n$. Assim, ζ_n^p é raiz n-ésima primitiva da unidade. Logo $(\zeta_n^p)^n - 1 = f(\zeta_n^p)h(\zeta_n^p)$, ou seja, $0 = f(\zeta_n^p)h(\zeta_n^p)$. Assim, se ζ_n^p não for raiz de $f(x)$, então ζ_n^p é raiz de $h(x)$, e portanto ζ_n é raiz de $h(x^p)$. Portanto, pelo modo como tomamos $f(x)$, segue que, $f(x) \,|\, h(x^p)$, ou seja, $h(x^p) = f(x)g(x)$, com $g(x) \in \mathbb{Z}[x]$ pelo lema de Gauss.

Como consequência do pequeno Teorema de Fermat (2.2), temos que $a^p \equiv a(mod\, p)$ e daí $h(x^p) \equiv h(x)^p(mod\, p)$. Assim, $f(x)g(x) \equiv h(x)^p(mod\, p)$, e portanto $h(x)^p \equiv f(x)g(x)(mod\, p)$. Logo, $\overline{h(\zeta_n)^p} = \overline{0}$, pois ζ_n é raiz de $f(x)$. E recursivamente chegamos que $\overline{h}(\zeta_n) = 0$. Portanto $\overline{f}$ e $\overline{h}$ tem uma raiz em comum. Assim $x^n - \overline{1} = \overline{f}(x)\overline{h}(x)$, e portanto $x^n - \overline{1}$ tem raízes múltiplas. Logo $nx^{n-1} = \overline{0}$ e assim, para qualquer $\alpha \in \mathbb{Z}_p$, $n\alpha^{n-1} = \overline{0}$. Como a característica de $\mathbb{Z}_p$ é p segue que $p|n$, o que contradiz o fato de termos suposto que $p \nmid n$. Portanto ζ_n^p é raiz de $f(x)$ $\forall\ p \nmid n$ e $mdc(p, n) = 1$. Logo $\partial(f(x)) \geq \partial(\phi_n(x))$, pois toda raiz de $\phi_n(x)$ é raiz de $f(x)$, e como $f(x)|\phi_n(x)$, segue que $\partial(\phi_n(x)) \geq \partial(f(x))$. Portanto, $\partial(f(x)) = \partial(\phi_n(x)) = \varphi(n)$. □

Observação 5.1. Existe um único polinômio minimal $f(x)$ tal que $f(\zeta_n) = 0$. Pelo Teorema (5.1) temos que $\partial(f(x)) = \partial(\phi_n(x))$, e que $\phi_n(\zeta_n) = 0$. Assim, $f(x) = \phi_n(x)$ e, portanto $\phi_n(x)$ é irredutível.

Teorema 5.2. *([17]) O anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \cdots, \zeta_n^{\varphi(n)-1}\}$ é uma base integral de $\mathcal{O}_\mathbb{K}$.*

A demonstração do Teorema 5.2 divide-se nos casos em que n é primo, n não é uma potência de primo e n não é primo e nem uma potência de primo. Devido a sua complexidade optamos por omiti-la.

5.2 Caso Particular do Teorema de Dirichlet

Nesta seção apresentamos um caso particular do Teorema de Dirichlet para progressões aritméticas, cuja demonstração apresentada em [20] foi adaptada por nós. Lembremos que uma progressão aritmética é um tipo de sequência numérica onde cada termo (elemento) é determinado pela soma do seu antecessor por uma constante (razão).

Agora, a função de Euler, definida no Capítulo 3, pode também ser considerada como:

$$\varphi(n) := |(\mathbb{Z}_n)^\times|,$$

sendo $(\mathbb{Z}_n)^\times$ o **sistema completo de invertíveis módulo** n, ou ainda, $(\mathbb{Z}_n)^\times = \{b_1, b_2, \cdots, b_{\varphi(n)}\}$, onde $mdc(b_i, n) = 1$, para todo i, e $b_i \equiv b_j (mod\ n)$ implica $i = j$.

Definição 5.2. *Dado $\bar{a} \in (\mathbb{Z}_n)^\times$, definimos a* ***ordem de*** *$\bar{a}$, denotada por ord $\bar{a}$, como o menor inteiro $t > 0$ tal que $\bar{a}^t = \bar{1}$ em $\mathbb{Z}_n$.*

Definição 5.3. *Se $a, n \in \mathbb{Z}$, com $mdc(a, n) = 1$, definimos a* ***ordem de*** *a* ***módulo*** *n, denotado por $ord_n a$, como a ordem de $\bar{a} \in (\mathbb{Z}_n)^\times$.*

Se $ord_n a = \varphi(n)$, dizemos que a é raiz primitiva módulo n. Por exemplo, 2 é raiz primitiva módulo 5, pois $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16$ que é a primeira potência de 2 congruente a 1 módulo 5 e $4 = \varphi(5)$.

Teorema 5.3 (Dirichlet - caso particular, [19], p. 200)**.** *Se $n > 1$ é um inteiro então a progressão aritmética $1, 1+n, 1+2n, \cdots$ contém infinitos números primos.*

Demonstração. Sejam $p_1, \cdots, p_k$ primos quaisquer e ϕ_n o n-ésimo polinômio ciclotômico. Como ϕ_n é mônico, podemos escolher um inteiro y tal que $\phi_n(ynp_1 \cdots p_k) > 1$.

De fato,

$$\begin{aligned} \phi_n(x) &= \prod_{1 \le k \le n; mdc(k,n)=1} (x - \zeta^k) \\ &= (x - \zeta) \cdots (x - \zeta^{n-1}) \end{aligned}$$

$$= x^{\phi(n)} + x(\cdots) + 1. \tag{5.3}$$

Agora, fazendo $a = ynp_1 \cdots p_k$ temos, módulo $ynp_1 \cdots p_k$, que

$$\phi_n(a) \equiv \phi_n(0) = 1\,(mod\ a).$$

Daí,

$$a|(\phi_n(a) - 1) \Rightarrow \phi_n(a) - 1 = qa \Rightarrow \phi_n(a) = qa + 1 = ynp_1 \cdots p_k q + 1,$$

onde $q \in \mathbb{Z}$.

Se p for um fator primo de $\phi_n(a)$, isto é, $\phi_n(a) = pf$, temos que

$$ynp_1 \cdots p_k q + 1 = pf,$$

$f \in \mathbb{Z}$.

Daí, $p \neq p_1, \cdots, p_k$, pois se $p = p_i$, para algum $i = 1, \cdots, k$, teremos $ynp_1 \cdots p \cdots p_k q + 1 = pf$, o que implicaria no absurdo: $p(ynp_1 \cdots p_k q) + 1 = pf$. Resulta ainda que $mdc(p,\ n) = 1$, pois $mdc(p, n) = d \neq 1$, então $d|p$ e $d|n$ implica

$$p = dl_1 \text{ e } n = dl_2, \quad l_1, l_2 \in \mathbb{Z},$$
$$ydl_2 p_1 \cdots p_k q + 1 = dl_2 \text{ e } d(ydl_2 p_1 \cdots p_k q) + 1 = dl_2,$$

que é absurdo.

Se provarmos que $p \equiv 1(mod\ n)$ seguirá que p é um primo em nossa progressão aritmética, diferente de $p_1, \cdots, p_k$. De fato, já vimos que $p \neq p_1, \cdots, p_k$ e se $p \equiv 1(mod\ n)$, então

$$n|(p-1) \Rightarrow p-1 = hn \Rightarrow p = hn+1,\ h \in \mathbb{Z},$$

ou seja, p é um dos termos da progressão aritmética: $1, 1+n, 1+2n+\cdots$.

Para o que falta, note que $mdc(p,a) = 1$.

Com efeito, temos

$$\begin{cases} mdc(p,n) = 1 \\ p \neq p_1, \cdots p_k \\ a = ynp_1 \cdots p_k q + 1. \end{cases}$$

Daí, se $mdc(p,y) = d \neq 1$, então, $d|p$ e $d|y$, ou ainda, $p = l_1 d$ e $y = l_2 d$. Logo, $l_2 dnp1 \cdots p_k q + 1 = l_1 df$, ou ainda, $d(l_2 dnp1 \cdots p_k q) + 1 = d(l_1 f)$ o que é absurdo. Logo, $mdc(p,y) = 1$, ou seja, $mdc(p,a) = 1$.

Como $mdc(p,a) = 1$, podemos considerar $t := ord_p(a)$, isto é, t é o menor inteiro tal que $a^t \equiv 1(mod\ p)$. Como $p|\phi_n(a)$ (pois p é um fator primo de $\phi_n(a)$) e $\phi_n(a)|(a^n-1)$ (pois $x^n - 1 = \prod_{0<d|n} \phi_d(x) = \phi_n(x) \prod_{0<d|n;d<n} \phi_l(x)$ implica $\phi_n(x)|(x^n-1)$ em $\mathbb{Z}[x]$), vem que

$$a^n - 1 = k\phi_n(a).$$

Como $p|\phi_n(a)$, segue que $a^n - 1 = kpl \equiv 0(mod\ p)$, ou ainda, $a^n \equiv 1(mod\ p)$ e, daí, $t = ord_p(a)$ e, portanto, $t|n$ $(t < n)$.

Se mostrarmos que $t = n$ teremos, das propriedades da ordem e de $a^{p-1} \equiv 1(mod\ p)$ (Pequeno Teorema de Fermat), que $n|(p-1)$ ou, o que é o mesmo que, $p \equiv 1(mod\ n)$.

Se $c \in \{a, a+p\}$, segue de $a^t \equiv 1(mod\ p)$ que

- $c = a \Rightarrow c^t \equiv 1(mod\ p)$
- $c = a+p \Rightarrow (a+p)^t \equiv a^t \equiv 1(mod\ p)$.

Portanto, em qualquer um dos casos $c^t \equiv 1(mod\ p)$.

Suponha, por contradição, que $t < n$. O Lema 5.1, juntamente com o fato de que $t|n$, nos dá

$$\begin{aligned} c^n - 1 = \prod_{0<d|n} \phi_d(c) &= \phi_n(c) \prod_{0<d|n,\, d<n} \phi_d(c) = \phi_n(c)h(c) \prod_{0<d|t} \phi_d(c) \\ &= \phi_n(c)h(c)(c^t - 1), \end{aligned}$$

onde $h \in \mathbb{Z}[x]$ é algum polinômio apropriado. Mas, como $c = a$ ou $c = a+p$, segue que $a \equiv a(mod\ p)$ e $a+p \equiv a(mod\ p)$. Daí, segue que $c \equiv a(mod\ p)$, $c \in \{a, a+p\}$.

Assim, $\phi_n(c) = \phi_n(a) \equiv 0(mod\ p) \Rightarrow p|\phi_n(c) \Rightarrow \phi_n(c) = k_1 p$. Como $c^t \equiv 1(mod\ p)$, segue que $p|(c^t - 1)$, isto é, $c^t - 1 = k_2 p$. Daí,

$$c^n - 1 = \phi_n(c)h(c)(c^t - 1) = k_1 p h(c) k_2 p = k_1 k_2 h(c) p^2 \equiv 0(mod\ p^2).$$

Por outro lado, como

$$\begin{aligned}(a+p)^n - 1 &= a^n - 1 + \sum_{j=1}^{n-1} a^j p^{n-j} \begin{pmatrix} n \\ j \end{pmatrix} \\ &= a^n - 1 + nap^{n-1} + \cdots + na^{n-1}p.\end{aligned}$$

Se $c = a + p$ e, como $c^n - 1 \equiv 0(mod\ p^2)$, então $(a+p)^n - 1 \equiv 0(mod\ p^2)$. Se $c = a$, então $a^n - 1 \equiv 0(mod\ p^2)$, pois $c^n - 1 \equiv 0(mod\ p^2)$.

Logo,

$$\begin{aligned}(a+p)^n - 1 = a^n - 1 + \cdots + na^{n-1}p \ &\Rightarrow\ 0 \equiv na^{n-1}p(mod\ p^2) \\ &\Rightarrow\ p^2 | na^{n-1}p \\ &\Rightarrow\ na^{n-1}p = kp^2 \\ &\Rightarrow\ na^{n-1} = kp \\ &\Rightarrow\ p | na^{n-1} \\ &\Rightarrow\ p|n \ \text{ ou } \ p|a^{n-1}.\end{aligned}$$

Se $p|a^{n-1} \Rightarrow p|aa^{n-2} \Rightarrow p|a^{n-2} \Rightarrow p|aa^{n-3} \Rightarrow p|a^{n-3} \Rightarrow \cdots \Rightarrow p|aa^2 \Rightarrow p|a^2 \Rightarrow p|aa \Rightarrow p|a$, que é absurdo, pois $mdc(p, a) = 1$.

Logo, $p|n$, o que é absurdo, pois $mdc(p, n) = 1$. Portanto, $p \equiv 1(mod\ n)$. □

Os números primos ostentam uma longa história, desde a Grécia antiga até o presente. O *Teorema Fundamental da Aritmética* diz que os números primos são tijolos de construção a partir dos quais os outros inteiros são formados multiplicativamente. Por conseguinte, os números primos foram muito estudados e se fizeram esforços consideráveis no sentido de determinar a natureza de sua distribuição na sequência dos inteiros positivos. Um dos principais resultados obtidos na antiguidade foi a prova da infinitude dos primos pelo matemático alemão Lejeune-Dirichlet (Peter Gustav Lejeune Dirichlet (1805-1859)) ao conseguir mostrar que toda progressão aritmética

$$a, a + d, a + 2d, a + 3d, \cdots$$

contém infinitos números primos, com a e d primos entre si.

Como a demonstração desse resultado exige instrumentos complicados da análise focamos num caso especial deste teorema: quando o termo inicial da progressão for igual a 1. O nome de Dirichlet surge ainda em muitos outros contextos em matemática pura e aplicada [4].

6 Raízes da Unidade e a Construção de Reticulados

Além da aplicação de raiz da unidade num caso particular do Teorema de Dirichlet, as raízes da unidade possuem várias outras aplicações. Uma delas é a que apresentamos neste capítulo.

Através da associação de uma raiz da unidade com um corpo, isto é, um corpo ciclotômico, é possível construir reticulados.

Uma maneira econômica, em número de palavras, de definirmos um reticulado é: como um subgrupo aditivo e discreto do $\mathbb{R}^n$. Os pontos de um reticulado posicionam-se de maneira bastante regular e simétrica no espaço. Uma boa parte da pesquisa de reticulados é impulsionada pela busca por uma resposta da seguinte pergunta: qual a maneira de dispormos esferas de mesmo raio em $\mathbb{R}^n$, sem sobreposição, de modo a cobrir a maior parte possível do espaço? A solução no plano e no espaço tridimensional é bastante intuitiva: a maneira com que as abelhas fazem as suas colmeias provém a maior eficiência no plano, enquanto em $\mathbb{R}^3$ o reticulado conhecido como cúbico de face centrada (ou "pilha de laranjas") nos diz onde devem estar posicionados os centros das esferas de modo a minimizar os espaços vazios. Para dimensões maiores, o problema torna-se significativamente mais complexo.

Neste capítulo apresentamos alguns conceitos da teoria de reticulados e um método para a gerá-lo no $\mathbb{R}^n$. A vantagem de obter reticulados por este método é que podemos identificar os pontos do reticulado no $\mathbb{R}^n$ como os elementos de um corpo de números.

6.1 Reticulados

Além das utilizações mais comuns da sua estrutura, como o empacotamento de compras na feira ou a fabricação de colmeias por abelhas, reticulados são importantes por desempenharem um papel significativo na Teoria da Informação.

Definição 6.1. *Sejam $\{v_1, v_2, ..., v_m\}$ vetores linearmente independentes do $\mathbb{R}^n$ (logo, $m \leq n$). O conjunto de pontos $\Lambda = \left\{ \mathbf{x} = \sum_{\mathbf{i=1}}^{\mathbf{m}} \lambda_\mathbf{i} \mathbf{v_i}, \lambda_\mathbf{i} \in \mathbb{Z} \right\}$ é chamado **reticulado** de dimensão m e $\{v_1, v_2, ..., v_m\}$ é chamado de **base** do reticulado.*

Definição 6.2. *O paralelepípedo formado pelos pontos* $\theta_1 v_1 + \cdots + \theta_m v_m,\ 0 \leq \theta_i < 1$ *é chamado um* **paralelepípedo fundamental** *ou* **região fundamental** *do reticulado.*

Exemplo 6.1. $\Lambda = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na figura abaixo.

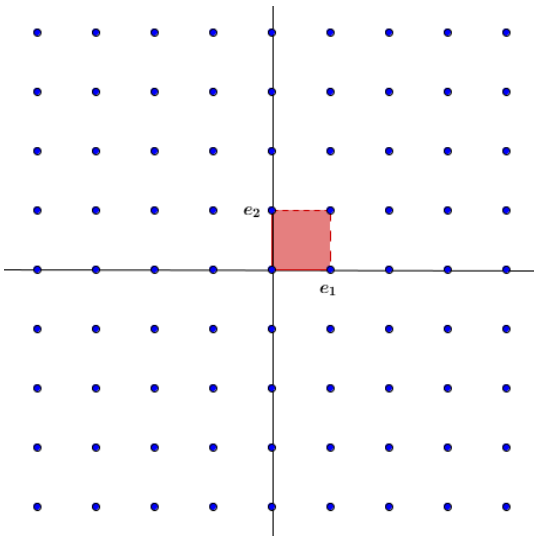


Figura 6.1: Representação de $\mathbb{Z}^2$.
Fonte: print screen do software Geogebra.

Definição 6.3. *Seja* $\{v_1, \ldots, v_m\}$ *uma base de um reticulado* Λ. *Se* $v_i = (v_{i1}, \ldots, v_{in})$, *para* $i = 1, \cdots, m$, *a matriz* $M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ & & \ddots & \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$ *é chamada uma* ***matriz geradora*** *para o reticulado. A matriz* $G = MM^t$ *é chamada uma* ***matriz de Gram*** *para o reticulado, onde* t *denota a transposição.*

Assim, os pontos do reticulado são formados por $\Lambda = \{\mathbf{x} = \lambda \mathbf{M} | \lambda \in \mathbb{Z}^{\mathbf{m}}\}$.

Definição 6.4. *O* ***determinante do reticulado*** Λ *é definido como sendo o determinante da matriz geradora* G, *isto é,* $det(\Lambda) = det(G)$.

Um reticulado é dito ter **posto máximo** se $m = n$, e neste caso M é uma matriz quadrada. Assim, $det(\Lambda) = (det(M))^2$.

É importante observar que o mesmo reticulado pode ser representado de diferentes maneiras e como uma consequência, dado uma matriz de Gram (ou geradora), não é fácil determinar qual é o reticulado correspondente. Invariantes tais como a dimensão e o determinante poderão ajudar, mas um dos cuidados que temos que ter é que tendo o mesmo determinante não é suficiente para garantir que dois reticulados sejam equivalentes, isto é, que um deles pode ser obtido do outro por rotação ou por translação.

Definição 6.5. *a) Um* **empacotamento esférico**, *ou simplesmente um empacotamento no* $\mathbb{R}^n$, *é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

b) Um ***empacotamento reticulado*** *é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* Λ *de* $\mathbb{R}^n$.

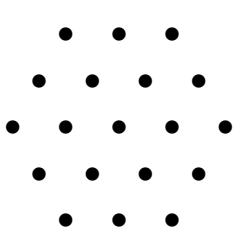
Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a **densidade de empacotamento** de Λ é igual a

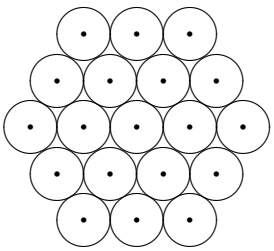
$$\Delta(\Lambda) = \frac{\text{Volume da região coberta pelas esferas}}{\text{Volume da região fundamental}} = \frac{\mathcal{V}ol(\mathcal{B}(\rho))}{\mathcal{V}ol(\Lambda)} = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Um dos problemas de empacotamento esférico de um reticulado no $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade. A seguir, daremos exemplos em dimensões $1, 2$ e 3. Para maiores detalhes, consultar [6].

Em dimensão um, temos que os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$-reticulado cuja a densidade de empacotamento é a melhor possível, dada por $\Delta = 1$. Neste caso, as "esferas" são intervalos da reta.

Para dimensão dois o reticulado hexagonal A_2 (favo de mel) é o de maior densidade, dada por $\Delta = \frac{\pi}{\sqrt{12}} \approx 0,9069$. O empacotamento deste reticulado com base $\beta = \left\{(1,0), (-\frac{1}{2}, \frac{\sqrt{3}}{2})\right\}$ é dado por





Em dimensão o reticulado conhecido como fcc (*face centered cubic*) é o empacotamento com maior densidade (pirâmides de laranjas), sendo essa $\Delta = \frac{\pi}{\sqrt{18}} \approx 0,7405$.

6.2 Reticulados via Corpos de Números

Nesta seção veremos que a definição de mergulho canônico estabelece uma correspondência um a um entre os elementos do corpo de números algébrico de grau n e os vetores do espaço euclidiano n-dimensional. Uma de suas aplicações é a geração

Figura 6.2: Favo de mel.
Fonte: google imagens.

Figura 6.3: Pirâmide de laranjas.
Fonte: google imagens.

de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria dos números algébricos, através de propriedades herdadas de $\mathbb{K}$.

Sejam $\mathbb{K}$ um corpo de números e n seu grau. Temos que existem n monomorfismos distintos $\sigma_j : \mathbb{K} \to \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$ diz-se que σ_j é **real**, caso contrário, σ_j é dito **imaginário**. Quando todos os monomorfismos são reais diz-se que $\mathbb{K}$ é um **corpo totalmente real** e quando os monomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um **corpo totalmente complexo**.

Se $\overline{\alpha} : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$, temos que $\overline{\alpha} \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$, e que $\overline{\alpha} \circ \sigma_j = \sigma_j$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Desta forma, temos que os monomorfismos imaginários aparecem aos pares, isto é, se σ_j é imaginário, existe k tal que $\overline{\alpha} \circ \sigma_j = \sigma_k$,. Assim, usando r_1 para denotar o número de monomorfismos reais e r_2 o número de pares de monomorfismos imaginários, podemos reordenar os monomorfismos $\sigma_1, \cdots, \sigma_n$, de modo que $\sigma_1, \cdots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+1}, \cdots, \sigma_{r_1+2r_2}$ sejam os monomorfismos imaginários com $\sigma_{r_1+r_2+i} = \overline{\alpha} \circ \sigma_{r_1+i}$ para $i = 1, \cdots, r_2$. Notemos que $n = r_1 + 2r_2$.

Assim, usando r_1 para denotar o número de índices, tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, podemos

ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de tal modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$. Então $n - r_1$ é um número par, assim podemos escrever $r_1 + 2r_2 = n$. Daí, para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), Re(\sigma_{r_1+1}(x)), Im(\sigma_{r_1+1}(x)), \ldots, Re(\sigma_{r_1+r_2}(x)), Im(\sigma_{r_1+r_2}(x))),$$

onde as notações $Re(x)$ e $Im(x)$ representam as partes real e imaginária do número complexo x, respectivamente, é chamado **mergulho canônico** de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$.

Exemplo 6.2. Considere o ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_5)$, onde $\zeta_5 = e^{\frac{2\pi i}{5}}$ e $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Como $\mathbb{K}$ é um corpo totalmente complexo, temos que $r_1 = 0$ e $r_2 = 2$. Pela Proposiçao 3.5 os quatro monomorfismos são dados por

$$\sigma_1(\zeta_5), \sigma_2(\zeta_5) = \zeta_5^2, \sigma_3(\zeta_5) = \zeta_5^3, \sigma_4(\zeta_5) = \zeta_5^4.$$

Se $x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 \in \mathbb{K}$, com $a, b, c, d, e \in \mathbb{Q}$, temos

$$\sigma_{\mathbb{K}}(x) = (Re(\sigma_1(x)), Im(\sigma_1(x)), Re(\sigma_2(x)), Im(\sigma_2(x))).$$

Os próximos resultados, cujas demonstrações podem ser ecntradas em [24], nos dizem como obter um reticulado no $\mathbb{R}^n$.

Teorema 6.1. *Sejam $\{w_1, \cdots, w_n\}$ uma base integral de $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{C}$ o mergulho canônico. Os n vetores $\mathbf{v_i} = \sigma_{\mathbb{K}}(w_i) \in \mathbb{R}^n$, $i = 1, \cdots, n$ são linearmente independentes e definem um reticulado em $\mathbb{R}^n$, denominado* **reticulado algébrico** *de posto máximo, $\Lambda = \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.*

Proposição 6.1. *Seja $\mathbb{K}$ um corpo de números de grau n e B um $\mathbb{Z}$-submódulo livre de $\mathbb{K}$ de posto n. Se $(x_i)_{1 \leq i \leq n}$ é uma $\mathbb{Z}$-base de B, então $\sigma_{\mathbb{K}}(B)$ é um reticulado em $\mathbb{R}^n$.*

Concluímos assim, que o ingrediente chave para a construção de reticulados algébricos tem sido a existência de uma $\mathbb{Z}$-base livre em $\mathbb{K}$. Como $\mathcal{O}_{\mathbb{K}}$ e seus ideais são $\mathbb{Z}$-módulos livres de posto n, podemos mergulhá-los em $\mathbb{R}^n$ para obter um reticulado algébrico.

A matriz geradora M de um reticulado algébrico, isto é, de um reticulado construído usando o mergulho canônico de $\mathbb{K}$, é dada por

$$\begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_{r_1}(w_1) & Re(\sigma_{r_1+1}(w_1)) & \cdots & Im(\sigma_{r_1+r_2}(w_1)) \\ \vdots & & & & \vdots & \\ \sigma_1(w_n) & \cdots & \sigma_{r_1}(w_n) & Re(\sigma_{r_1+1}(w_n)) & \cdots & Im(\sigma_{r_1+r_2}(w_n)) \end{pmatrix},$$

onde $\{w_1, \cdots, w_n\}$ é aqui uma base de $\mathcal{O}_{\mathbb{K}}$.

Exemplo 6.3. Seja $\mathbb{K} = \mathbb{Q}(\zeta_3)$. Uma base integral de $\mathbb{K}$ é $\{1, \zeta_3\}$ e $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_3]$. Pelo Teorema (6.1), $\Lambda = \sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ é um reticulado no $\mathbb{R}^2$. Os dois mergulhos são $\sigma_1(\zeta_3) = \zeta_3$ e $\sigma_2(\zeta_3) = \zeta_3^2$. Neste caso, $r_1 = 0$ e $r_2 = 1$, assim, a matriz geradora do reticulado é

$$M = \begin{pmatrix} Re(\sigma_1(1)) & Im(\sigma_1(1)) \\ Re(\sigma_1(\zeta_3)) & Im(\sigma_1(\zeta_3)) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

É possível verificar que com essa estrutura algébrica obtêm-se o reticulado hexagonal $\Lambda = A_2$, com base $\{(1,0), (-\frac{1}{2}, \frac{\sqrt{3}}{2})\}$. Para maiores detalhes consultar [6]. Este reticulado pode ser representado graficamente da seguinte forma:

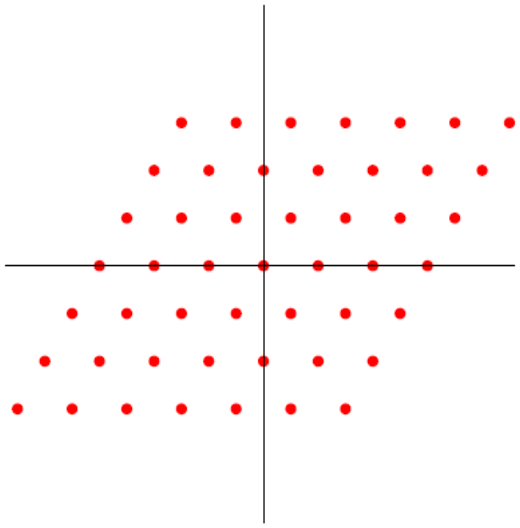


Tabela 6.1: Reticulado $\Lambda = A_2$.

7 Fatos Históricos Sobre o Último Teorema de Fermat e a Raiz n-ésima da Unidade

Neste Capítulo abordamos fatos históricos relacionados ao Último Teorema de Fermat e como a raiz n-ésima se inseriu neste contexto. As principais referências utilizadas nesse capítulo foram [4], [11] e [25].

7.1 Apresentação Geral

Pierre De Fermat (1601?-1665) é considerado o maior matemático francês do século XVII. A sua maior contribuição, na qual toma relevância neste trabalho, é a fundação da moderna teoria dos números. Em uma tradução latina do livro *Aritmética* de Diofanto, feita por Bachet de Méziriac em 1621, Fermat anotava suas contribuições em forma de notas e enunciados nas margens do próprio exemplar e muitos desses teoremas posteriormente mostrariam-se verdadeiros. Essas anotações se incorporaram numa nova impressão da edição de *Aritmética* publicada por um dos filhos de Fermat, Clément - Samuel.

A anotação de Fermat encontrada ao lado do Problema 8 do Livro II corresponde ao famoso *Último teorema de Fermat (UTF)*: "Dado um número quadrado, dividi-lo em dois quadrados", e na nota marginal completava sua conjectura, "Dividir um cubo em dois cubos, uma quarta potência ou, em geral uma potência qualquer em duas potências da mesma denominação acima da segunda é impossível, e eu seguramente encontrei uma prova admirável desse fato, mas a margem é demasiado estreita para contê-la".

É desconhecido tal demonstração por Fermat, mas é fato que muitos dos mais brilhantes matemáticos se empenharam na resolução do problema.

Dentre os grandes matemáticos ao longo dos tempos que tentaram solucionar o problema podemos citar: Euler, Dirichlet (1828), Legendre (1830), Gabriel Lamé (1839), Sophie Germain, Kummer e mais recentemente, Wagstaff (1980). Um fato interessante

é que Kummer, em 1847, ao tentar demonstrar o teorema, criou o método dos divisores complexos, a que chamou números complexos ideais, contribuindo para o desenvolvimento da teoria dos números.

O último teorema de Fermat destaca-se ainda por ser o problema matemático com maior número de demonstrações incorretas publicadas. Apenas em 1995 o UTF foi resolvido corretamente pelo matemático britânico Andrew Wiles (1953 -).

O desenvolvimento de uma conejctura pelos dois matemáticos Yutaka Taniyama e Goro Shimura não tinha como objetivo solucionar o UTF, mas foi a primeira contribuição (mesmo que não intencional) para a resolução do teorema. A conjectura feita pelos dois matemáticos diz que para cada equação elíptica há uma forma modular correspondente; a relevância dessa conjectura reside no fato de que se a mesma estiver correta ela poderia ser aplicada ao Último Teorema de Fermat provando a sua veracidade. Ou seja, para provar se o Último Teorema de Fermat era ou não verdadeiro, deveria se provar primeiro a conjectura Taniyama-Shimura, e foi exatamente isso que Andrew Wiles fez.

7.2 Contribuições de Matemáticos no Último Teorema de Fermat

Quem fez o primeiro avanço em direção à prova do Último Teorema de Fermat, foi Leonard Euler, com sua memória e intuição incríveis.

Ao deparar-se com o Último Teorema de Fermat, Euler imaginou se não poderia provar que uma das equações não tinha solução e então extrapolar o resultado para todas as infinitas equações restantes. Inicialmente, Euler provou o caso por contradição para $n = 3$. Durante seus estudos, Euler teve que incorporar os números imaginários, o que acrescentaria uma nova dimensão à matemática naqueles tempos. Entretanto, todas as tentativas de Euler de fazer seu argumento valer para outros valores de n terminaram em fracasso.

Sophie Germain adotou uma nova estratégia: a partir de um tipo especial de número primo p, de modo que $2p + 1$ também fosse primo, desenvolveu um argumento que provavelmente não existem soluções para $x^n + y^n = z^n$ para valores de n iguais a esses primos de Germain. Assim a lista de Germain incluía, por exemplo, o 5 porque $11 = 2 \cdot 5 + 1$ também é primo, mas não incluía 13, porque $27 = 2 \cdot 13 + 1$ não é primo. Em 1825, com Gustav Lejeune-Dirichlet e Adrien-Marie Legendre o método de Germain teve o primeiro sucesso na prova que o caso $n = 5$ não tinha solução.

Quatorze anos depois, Gabriel Lamé fez alguns acréscimos engenhosos ao método de Germain e conseguiu a demonstração para o número primo $n = 7$. Em março de 1847, tanto Gabriel Lamé como Augustin Louis Cauchy anunciaram que estavam prestes a publicar a demonstração completa para o Último Teorema de Fermat.

Em sua suposta demonstração, Lamé utilizou uma fatoração no espaço dos números complexos sem provar que a fatoração em irredutíveis nesse espaço é única. Apesar disso, a ideia de fatoração feita por Lamé é a mesma utilizada na demonstração de Ernst Kummer para os chamados primos regulares. Lamé introduziu, em sua fatoração, raízes complexas da unidade, iniciando a análise do corpo $\mathbb{Q}(\zeta_n)$ que apresenta, de certa forma, a incorporação ao corpo dos racionais do elemento ζ_n, que é uma raiz da unidade dependendo de n, sem perder as propriedades de corpo de $\mathbb{Q}$.

Antes que Lamé e Cauchy publicassem a demonstração tão esperada, Ernest Kummer percebeu que as demonstrações de ambos dependiam do uso de propriedade dos números conhecida como fatoração única, verdadeira dentro dos reais, porém trabalhavam dentro dos imaginários.

E embora a fatoração única seja verdadeira para os números reais, ela pode se tornar falsa quando introduzimos os números imaginários. Por exemplo, se nos restringirmos aos números reais, então o número 12 pode ser fatorado apenas como $2 \cdot 2 \cdot 3$. Contudo, se permitirmos a entrada de números imaginários nesta demonstração, então 12 pode ser fatorizado do seguinte modo:

$$12 = (1 + \sqrt{-11}) \cdot (1 - \sqrt{-11}).$$

Aqui $(1+\sqrt{-11})$ é um número complexo, uma combinação de um número real com um número imaginário. E embora o processo de multiplicação seja mais complicado do que para os números comuns, a existência dos números complexos leva a modos adicionais de se fatorar 12. Outro modo é $(2 + \sqrt{-8}) \cdot (2 - \sqrt{-8})$. Não existe mais fatoração única e sim uma escolha de fatorações.

Para resolver essa questão Kummer criou o conceito de *números ideais*. Assim, se o domínio a ser trabalhado não apresentasse a unicidade da fatoração de seus elementos, então existiriam números, os números ideais, que quando "adicionados" ao conjunto, o tornariam um domínio fatorial. Foi com essa teoria de números ideais que Kummer, cerca de três anos após o anúncio da "prova" de Lamé, provou o Último Teorema de Fermat para expoentes n que atendessem a uma condição especial, que são os chamados primos regulares. A prova de Kummer era o maior avanço realizado na busca pela solução do Último Teorema de Fermat até a demonstração completa, finalizada por Wiles.

O tratamento do UTF por Kummer considera que se existirem inteiros $a, b, c \in \mathbb{Z}$ que é solução de $x^n + y^n = z^n$ para um determinado n, e p for um irredutível ímpar que divide n, então, escrevendo $n = pm$, tem-se que

$$(a^m)^p + (b^m)^p = a^n + b^n = c^n = (c^m)^p,$$

e assim, a equação terá solução inteira para o expoente p. Logo, se demonstrasse que a equação não tem solução para todo irredutível ímpar p, então $x^n + y^n = z^n$ só poderia ter solução quando n fosse uma potência de 2. Mas, adicionalmente, se soubesse que a

equação não tem solução para $n = 4$ poderia concluir também que a equação não tem solução para $n = 2^r$, para todo $r \geq 2$.

Para lidar com essa equação, os matemáticos pensaram em usar a seguinte decomposição

$$\prod_{i=1}^{n}(x + \zeta_n^i y) = z^n,$$

onde $\zeta_n = \cos\left(\frac{2\pi}{n}\right) + \text{sen}\left(\frac{2\pi}{n}\right)$ é uma raiz primitiva n-ésima da unidade, conforme vimos no Capítulo 3. Essa decomposição ocorre em $\mathbb{Z}[\zeta_n]$ que é o anel dos inteiros de $\mathbb{Z}$ em $\mathbb{Q}(\zeta_n)$. Usando essa fatoração e assumindo que $\mathbb{Z}[\zeta_n]$ é um anel de fatoração única, onde $n = p$ é um primo regular ímpar, Kummer demonstrou o UTF.

Para provar o UTF Andrew Wiles decide se isolar por sete anos até apresentar uma solução ao problema, levou dezoito meses estudando os elementos matemáticos que foram usados, ou que derivam das equações elípticas e das formas modulares. Ele abandonou todos os trabalhos que não fossem relevantes para a demonstração do Último Teorema de Fermat, inclusive deixou de participar de conferências. Neste período Wiles resolveu trabalhar em completo isolamento e segredo na sua demonstração, a única pessoa que sabia de seu segredo era sua esposa.

Para demonstrar O Último Teorema de Fermat, Wiles tinha que provar a conjectura de Taniyama-Shimura, onde cada equação elíptica teria que ser relacionada com uma forma modular. Wiles utiliza os trabalhos de Évarist Galóis para demonstrar a conjectura, sendo uma brilhante demonstração.

Depois de seis anos de isolamento Wiles partilhara seu segredo com Katz, quando o mesmo o ajudou a analisar sua demonstração, num curso sobre curvas elípticas que Wiles ministrou na Universidade de Princeton. Neste período do curso, Katz assistia as aulas para ver se tinha algum erro. Segundo Katz, nada precisava ser alterado e Wiles poderia publicar sua demonstração.

Depois de sete anos de estudo, Wiles tinha completado a demonstração da conjectura de Taniyama-Shimura, e como consequência, a demonstração do Último Teorema de Fermat e então poderia anunciar o mesmo.

Em maio de 1993 Wiles acreditava que estava provado o teorema, então no final do mês de junho em uma conferência na cidade de Cambridge (sua terra natal), no Instituto Isaac Newton, ele anunciou sua demonstração. Nesta conferência, Wiles realizou várias palestras até terminar sua demonstração, quando Wiles concluiu sua última palestra, sua demonstração tinha que ser submetida a um exame de avaliação, onde foram distribuídas partes da demonstração para que os matemáticos avaliassem.

Na parte que Katz tinha para analisar ocorreu um erro, então ele comunicou Wiles, mas em segredo do resto da comissão, para que Wiles a corrigisse. Ele tinha que corrigir o erro antes que a comunidade percebesse. Seis meses passados, Wiles ainda não tinha conseguido corrigir o erro, mas continuou persistindo. E disse a comunidade que precisava de mais tempo para aprontar seus manuscritos. Como o tempo ia passando,

Peter Sarnak sugeriu que Wiles conseguisse um auxiliar, então pensou em Richard Taylor um dos avaliadores e ex-aluno.

Wiles e Taylor dedicaram quatorze meses de trabalho, após Wiles ter anunciado a demonstração, para corrigir o erro e então a demonstração estava pronta. Wiles presenteou o aniversário de sua esposa com a prova do Último Teorema de Fermat, pois foi ela a única que sabia de seu maior sonho. Andrew Wiles levou oito anos de total estudo para demonstrar o Último Teorema de Fermat, publicado em 1995.

Referências

[1] ALVES, C. **Reticulados via Corpos Ciclotômicos**. 2005. 140f. Dissertação (Mestre em Matemática) - IBILCE, UNESP, São José do Rio Preto, 2005.

[2] AVILA, Geraldo. **Variáveis complexas e aplicações**. Rio de Janeiro: LCT, 2000.

[3] BASTOS, G. G. **Notas de Álgebra**. Edições Livro Técnico: Fortaleza, 2002.

[4] BOYER, C. B. **História da matemática**.Blucher: 2010.

[5] CAMINHA, A. **Polinômios Ciclotômicos e o Teorema dos Primos de Dirichlet**. 2003. Disponível em:<http://cyshine.webs.com/ciclotomico.pdf>. Acesso em: 03 jan. 2017.

[6] CONWAY, J.H.; SLOANE, N.J.A. **Sphere Packings, Lattices and Groups**. Springer, New York, 1999.

[7] COOKE, R.**The history of mathematics**: a brief course. WILEY, 2013.

[8] DOMINGUES, H. H. **Síntese da História das Equações Algébricas**. São José do Rio Preto: SBEM, 2000.

[9] EDWARDS, H. M. **Galois Theory**. New York: Springer, 1998.

[10] ENDLER, O. **Teoria dos Corpos**, Monog. de Matemática $n.44$. Rio de Janeiro: IMPA: 1987.

[11] EVES, H. **Introdução à história da matemática**. Campinas: Unicamp, 2004.

[12] GONÇALVES, A. **Introdução à álgebra**. Rio de Janeiro: IMPA, 2006.

[13] GUERREIRO, J. **Número de Classe e o Teorema de Dirichlet**. Disponível em: <http://guests.mpim−$bonn$.mpg.de/guerreiro/$class_number$.pdf>. Acesso em: 02 jan. 2017.

[14] HEFEZ, A., VILLELA, M. L. T. **POLONÔMIOS E EQUAÇÕES ALGÉBRICAS**. v.6. Rio de Janeiro: SBM, 2012.

[15] JACINTO, J. F. **O ÚLTIMO TEOREMA DE FERMAT** Disponível em: <http://www.ensino.eb.br/portaledu/conteudo/artigo8953.pdf> Acesso em: 02 jan. 2017.

[16] LANG, S. **Álgebra**. Addison-Wesley Publishing Company, 1972.

[17] MARCUS, D. A. **Numbers Fields**. Springer - Verlag, New York, 1977.

[18] MONTEIRO, L. H. J. **Elementos de Álgebra**.Rio de Janeiro: IMPA, 1969.

[19] NETO, A. C. M. **Tópicos de Matemática Elementar**: polinômios. Rio de Janeiro: SBM, 2012.

[20] NETO, A. L. **Funções de uma variável complexa**. Rio de Janeiro: IMPA, 2005.

[21] NIETO, J. H. **Sobre la Divisibilidad de Polinomios con Coeficientes Enteros**. Disponível em: <https://www.emis.de/journals/DM/vXI2/art7.pdf>. Acesso em: 02 jan. 2017.

[22] SANTOS, E. L. F. dos. **Unidades em Corpos Abelianos**. 2013. 80f. Dissertação (Mestre em Matemática) - IBILCE, UNESP, São José do Rio Preto, 2013.

[23] SANTOS, J. P. de O. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 2000.

[24] SAMUEL, P. **Algebraic Theory of Numbers** . Hermana, Paris, 1967.

[25] SINGH, S. **O ÚLTIMO TEOREMA DE FERMAT**. Rio de Janeiro: RECORD, 2000.

[26] STEWART, I.; TALL, D. **Algebraic Number Theory.** Chapman & Hall, New York, 1987.

[27] WASHINGTON, L. C. *Introduction to cyclotomic fiels.* New York: Springer-Verlag, 1982.

[28] **A Matemática Pura:** Um blog para gostar de matemática. Disponível em: <http://amatematicapura.blogspot.com.br/2012/07/numeros-complexos-e-unidade-imaginaria.html>. Acesso em: 02 jan. 2017.